UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

"Implementación de los Sistemas de Gestión de Riesgo Operacional, Seguridad de Información y Continuidad de Negocios para la Autorización del Método Estándar Alternativo por la SBS en un Banco"

INFORME DE SUFICIENCIA

Para optar por el título profesional de Ingeniero Industrial

Martín Mesía Vásquez

LIMA - PERU

2012

DEDICATORIA

Dedico esta documento al único ser supremo, mi Dios que me cuida y brinda fortaleza para seguir adelante, a mis queridos padres Nicolás y Esperanza por su constante aliento, a mis hermanos, a mi familia, amigos que me apoyan siempre en las buenas y en las malas circunstancias.

AGRADECIMIENTO

Mediante este documento quiero agradecer a todos los colegas que me apoyaron para crecer profesionalmente y personalmente, brindándome los conocimientos necesarios, su confianza y grandes enseñanzas que ahora me han servido para realizar este informe.

INDICE

DESCRIPTORES TEMÁTICOS

RESUMEN

INTRODUCCIÓN

CAPÍTULO I: PENSAMIENTO ESTRATÉGICO.....1

1.1. DIAGNÓSTICO FUNCIONAL.....1

1.1.1. Organización 1

1.1.1.1. Misión.....2

1.1.1.2. Visión.....2

1.1.1.3. Valores corporativos.....2

1.1.1.4. Organigrama de la Organización.....3

1.1.1.5. Organigrama del área de Trabajo.....5

1.1.2. Clientes.....6

1.1.2.1. Productos y Servicios.....6

1.1.3. Proveedores 7

1.1.4. Cadena de Valor del Banco……..……...9

1.1.4.1. Procesos de Dirección……10

1.1.4.2. Procesos Core……10

1.1.4.3. Procesos de Apoyo……....11

1.2. DIAGNÓSTICO ESTRATÉGICO……12

1.2.1. Análisis de las 5 Fuerzas de Porter……..13

1.2.1.1. Amenaza de Entrada de Nuevos Competidores……13

1.2.1.2. Rivalidad entre competidores existentes……13

1.2.1.3. Poder de negociación de los clientes……14

1.2.1.4. Poder de negociación de los proveedores……14

1.2.1.5. Amenazas Posibles de productos sustitutos……14

1.2.2. Análisis Externo……15

1.2.2.1. Oportunidades……15

1.2.2.2. Amenazas……17

1.2.3. Análisis Interno…..……....18

1.2.3.1. Fortalezas……18

1.2.3.2. Debilidades……19

1.2.4. Matriz FODA……..20

CAPÍTULO II: MARCO TEÓRICO Y METODOLOGÍA……...…22

2.1. ANTECEDENTES BIBLIOGRÁFICOS……22

2.2. BASES TEÓRICAS……23

2.2.1. Visión Global de los Riesgos Bancarios.....23

2.2.1.1. La Administración de Riesgos.....23

2.2.1.2. Riesgos Bancarios y la Macroeconomía.....26

2.2.1.3. Comité Basilea II.....29

2.2.1.4. Objetivos del Comité.....29

2.2.1.5. Funciones del Comité de Basilea.....30

2.2.1.6. Los 3 pilares importantes de Basilea II.....30

2.2.2. Riesgo Crediticio.....34

2.2.2.1. Introducción al Riesgo de Crédito.....34

2.2.2.2. Principales Factores que determinan el Riesgo en Banca.....34

2.2.2.3. Análisis de Riesgo de Crédito.....35

2.2.2.4. Aspectos Necesarios en la Evaluación de Crédito...36

2.2.2.5. Gestión de Riesgo Crediticio del banco en estudio.37

2.2.3. Riesgo de Mercado.....38

2.2.3.1. Introducción al Riesgos de Mercado.....38

2.2.3.2. Definición del Riesgo de Mercado.....39

2.2.3.3. Factores de Riesgo de Mercado.....39

2.2.3.4. Concepto del VaR (Value at Risk).....40

2.2.3.5. Requerimiento de Patrimonio por Riesgo de Mercado.....40

2.2.4. Riesgo operacional 41

2.2.4.1. Método del Indicador Básico.....42

2.2.4.2. Método del Estándar Alternativo.....44

2.2.4.3. Métodos Avanzados.....62

CAPÍTULO III: PROBLEMA Y SOLUCION..... 64

3.1. IDENTIFICACIÓN DEL PROBLEMA.....64

3.2. PLANTEAMIENTO DE ALTERNATIVAS DE SOLUCIÓN.....65

3.2.1. Aumentar el patrimonio del banco mediante una inyección de liquidez.....65

3.2.2. Implementación de Sistemas de Gestión para reducir el requerimiento de Patrimonio solicitado por la SBS.....66

3.3. SELECCIÓN DE UNA ALTERNATIVA DE SOLUCIÓN.....66

3.4. PLANES DE ACCIÓN PARA DESAROLLAR LA SOLUCIÓN PLANTEADA.....66

3.4.1. Implementación del Sistema de Riesgo Operacional.....66

3.4.1.1. Participación activa del Directorio y la Gerencia General en la Gestión de Riesgo operacional.....66

3.4.1.2. Función de la Gestión del Riesgo operacional.....67

3.4.1.3. Programa de Capacitación al Personal.....71

3.4.1.4. Metodología para la gestión de Riesgo Operacional...72

3.4.1.5. Recursos Suficientes……89

3.4.1.6. Remisión de información periódica a interesados internos e externos…….....90

3.4.1.7. Procedimientos para asegurar cumplimiento de metodología para gestión del riesgo operacional……..91

3.4.1.8. Incentivos para mejorar la gestión de riesgo operacional…….……...91

3.4.1.9. Gestión de la base de datos de pérdida de eventos de pérdida por riesgo operacional…… ……92

3.4.1.10. Revisión periódica independiente de la gestión de riesgo operacional por parte de Auditoría Interna …….93

3.4.1.11. Revisión periódica independiente de la gestión del riesgo operacional por parte de una sociedad de Auditoría Externa…… ……93

3.4.2. Implementación del Sistema de Gestión de Seguridad de Información…… ……..94

3.4.2.1. Política y Organización del SGSI…… ……94

3.4.2.2. Mecánica Operativa del Sistema de gestión de seguridad de Información…….....95

3.4.2.3. Gestión de Servicios Externos……98

3.4.2.4. Gestión de Activos…….....98

3.4.2.5. Seguridad del Personal…….....99

3.4.2.6. Seguridad Física y Ambiental……....99

3.4.2.7. Seguridad de las Operaciones y Comunicaciones…101

3.4.2.8. Norma de Control de Accesos……103

3.4.2.9. Seguridad en la adquisición y Desarrollo de Software……..……..104

3.4.2.10. Gestión de Incidentes……..…...105

3.4.2.11. Gestión de Cumplimiento…….……106

3.4.2.12. Gestión de Riesgos de Seguridad de Información….106

3.4.3. Implementación del Sistema de Continuidad de Negocios..111

3.4.3.1. Entendimiento Estratégico y operativo del negocio…….……...113

3.4.3.2. Análisis de Impacto y Evaluación……...114

3.4.3.3. Plan de Gestión de Crisis…….……127

3.4.3.4. Plan de Gestión de Continuidad……128

3.4.3.5. Plan de Emergencia…….……128

3.4.3.6. Plan de recuperación de Servicios TI……...129

3.4.3.7. Capacitación y despliegue de Pruebas de Continuidad de Negocios……129

3.4.3.8. Modelo y Evaluación del Sistema……..……130

CAPÍTULO IV: ANALISIS BENEFICIO COSTO.....132

4.1. SELECCIÓN DE CRITERIOS DE EVALUACIÓN…….132

4.2. INFORMACIÓN DE LA SITUACIÓN ECONÓMICA ACTUAL DE IMPLEMENTACIÓN DE LOS SISTEMAS DE GESTIÓN……..137

4.2.1. Costos de Implementación del Sistema de Gestión de Riesgo Operacional……137

4.2.2. Costos de Implementación del Sistema de Gestión de Seguridad de la Información……...142

4.2.3. Costos de Implementación del Sistema de Gestión de Continuidad del Negocio……..146

4.3. RESULTADOS DE LA SOLUCIÓN PLANTEADA…...149

CONCLUSIONES Y RECOMENDACIONES……..…151

CONCLUSIONES……..…151

Sistema de Gestión de riesgo operacional……..152

Sistema de Gestión de Seguridad de la Información …..……153

Sistema de Gestión de Continuidad de Negocios……155

RECOMENDACIONES……155

BIBLIOGRAFÍA……..…157

GLOSARIO DE TERMINOS……159

ANEXOS……...161

Estándar Australiano Neozelandés AS/NZS 4309-2009

Examinando los riesgos Macroeconómico en Basilea II: Propuestas de supervisión para economías emergentes.

DESCRIPTORES TEMÁTICOS

Diagnóstico de la Situación del banco

Sistema Integral de Riesgos

Sistema de Gestión Riesgo Operacional

Sistema de Gestión de Seguridad de la Información

Sistema de Gestión de Continuidad de Negocios

Requerimiento de patrimonio por Riesgo operacional

RESUMEN

El principal problema presentado para el Banco en Estudio es la implementación de los Sistemas de Gestión de Riesgo Operacional, Seguridad de Información y continuidad de Negocios, ya que los accionistas no están dispuestos a inyectar más patrimonio en el Banco lo cual reflejaría una mala gestión de la Gerencia General.

Para poder Solucionar el problema de la mejor manera hemos diseñado este documento de tal manera que el lector pueda tener una referencia y guía del paso a paso para la implementación.

En el Primer capítulo podremos encontrar el pensamiento estratégico del Banco, toda implementación parte de una estrategia; para esto se analizar las 5 fuerzas de Porter, se identifica las fortaleza, debilidades, oportunidades y amenazas para luego poder generar estrategias que se convertirán en acciones concretas.

En el segundo capítulo podemos ver un marco teórico de los tipos de riesgos y sólidas teorías que permitirán brindar información al lector sobre los

tipos de Riesgos orientándose a la Gestión de Riesgo Operacional, Seguridad de información y Continuidad de Negocios.

En el siguiente capítulo podemos encontrar el Problema principal que tiene la empresa, las alternativas de solución con su respectiva selección y los planes de acción que permitan eliminar el problema implementando los tres sistemas de gestión detallados, de tal manera que el lector tenga una visión global de todas las actividades.

En el cuarto capítulo mostramos los análisis beneficio costo que se realiza en toda la implementación; todas las inversiones que deberán estar justificadas y determinaremos que el proyecto agrega valor a la organización, aquí mostraremos los análisis que llevarán a interesantes conclusiones.

En el último capítulo tenemos las conclusiones y recomendaciones en donde se mencionan ciertos puntos que son parte de la experiencia adquirida al implementar estos sistemas de Gestión.

Finalmente este documento refleja 3 años de experiencia implementando sistemas de gestión para obtener la autorización del método estándar alternativo para el cálculo del requerimiento de patrimonio de riesgo operacional; así como también la investigación a diferentes autores que permiten un entendimiento claro.

INTRODUCCIÓN

Podemos apreciar que el mundo de los negocios son dinámicos y flexibles y buscan obtener rentabilidad; sin embargo es muy necesario conocer los Riesgos de cada uno de los negocios, riesgos que pueden conllevar a generar grandes pérdidas en las empresas por no tener una adecuada Gestión de Riesgos. En el Negocio Bancario también sucede lo mismo y las repercusiones pueden ser muy críticas, llegando hasta a desestabilizar una nación. En este sentido las naciones empezaron a preocuparse por los clientes de los Bancos implementando medidas de control que puedan minimizar dichos riesgos. Muchos países europeos se unieron para atender esta preocupación formando el Comité de Basilea en la cual buscaron definir buenas prácticas para el manejo de los riesgos en Banca.

El Perú no es ajeno a la implementación de las mejores prácticas; con el fin de proteger a los ahorristas de los Bancos, la Superintendencia de Banca y Seguros promulgó un Resolución SBS N° 2115-2009 del 02 de abril del 2009, exigiendo de esta manera a que los bancos implementen sistemas de Gestión de Riesgo Operacional, Seguridad de Información y Continuidad de Negocios para disminuir el requerimiento de Patrimonio por riesgo operacional.

El Banco en estudio, es un banco que tiene 4,5 Billones de soles en activos y 379 MM de soles en patrimonio; actualmente se encuentra en el Método Básico de Cálculo de Requerimiento de Capital y está interesado en postular para la autorización al uso del Método Estándar alternativo de requerimiento de patrimonio por Riesgo Operacional. El principal problema presentado es que si se implementa los sistemas de Gestión y no se obtiene la autorización, el Banco tendrá que inyectar mayor Patrimonio a la Empresa, lo cual será un dinero que no agregue Valor a la organización porque estará inmovilizado.

En tal Sentido, El banco en estudio con el involucramiento de su directorio y las Gerencias empezaron a implementar los requisitos para obtener la autorización por parte de la Superintendencia de Seguros, Pensiones y AFP.

Esta implementación de estos sistemas de gestión tienen costos asociados, no sólo en la implementación de los sistemas, sino en inversión en tecnología para garantizar que el Banco pueda funcionar con escenarios críticos, con seguridad y sin pérdidas (o con pérdidas mínimas) de riesgo operacional.

Esta fuerte inversión permitirá reducir las pérdidas por Riesgo operacional, Pérdidas de disponibilidad de los sistemas de información y garantizar la continuidad de las operaciones del Banco.

Este documento muestra las actividades que se realizan para poder obtener la autorización del Método estándar Alternativo de la Superintendencia

de Banca y Seguros para reducir el requerimiento de patrimonio, el cual es importante para la SBS para poder asegurar a los Superavitarios.

CAPÍTULO I

PENSAMIENTO ESTRATÉGICO

1.1. DIAGNÓSTICO FUNCIONAL

1.1.1. Organización

El Banco se inicia en Julio de 1964, como Financiera y Promotora de la Construcción S.A. Luego en enero de 1982, se modificó su denominación a FINANPRO Empresa Financiera. Es el 21 de Noviembre de 1986 cuando se constituyó como el Banco comercial.

El principal accionista es el Banco Pichincha de Ecuador, quien dio inicio al diseño del Plan Estratégico de Desarrollo Institucional desde el año 1997 con presencia en la región andina en Perú; Panamá, Estados Unidos y España.

En el 2001, el Banco adquiere el NBK Bank consolidando su crecimiento y diversificación de sus líneas de negocio, ya que en años anteriores estuvo enfocado en el sector empresarial.

A partir del 2004 desarrollamos operaciones bancarias de consumo, microcrédito y expandimos la colocación de créditos vía descuento de rol de pagos y casas comerciales a través de los

llamados convenios. Es así que durante el 2006 lanzamos la tarjeta de crédito Máxima Banco con tasas muy atractivas para los consumos de nuestros clientes.

En el 2008, nuestro Banco firmó una Alianza Estratégica con las tiendas de electrodomésticos Carsa, la cual nos permitió duplicar nuestro número de oficinas a casi 100 y contar con oficinas del Banco a nivel nacional.

En el 2012 el Banco anunció la compra del 100% de las acciones de Amerika Financiera, institución especializada en leasing y soluciones financieras ágiles y personalizadas para sus clientes, con lo cual apunta a fortalecer sus planes de crecimiento.

El Banco lleva 25 años operando en el mercado Peruano y con la adquisición última consolida sus activos de 4,781 millones de soles y un patrimonio de 458 millones de soles.[1]

1.1.1.1. Misión

Impulsar el crecimiento sostenible de nuestros clientes, colaboradores, accionistas y del país.

1.1.1.2. Visión

Ser el Banco líder en ofrecer soluciones financieras a nuestro mercado objetivo, brindando calidad de servicio, eficiencia y oportunidad.

1.1.1.3. Valores corporativos

a) Orientación al cliente:

Conocer y satisfacer sus necesidades

Simplicidad y transparencia

Disponibilidad y cercanía

[1] Diario Gestión: http://gestion.pe/noticia/1344881/banco-financiero-completa-compra-total-amerika-financiera

- Amabilidad

b) Orientación a las Personas

- Confianza
- Equidad
- Reconocimiento y desarrollo
- Trabajo en equipo

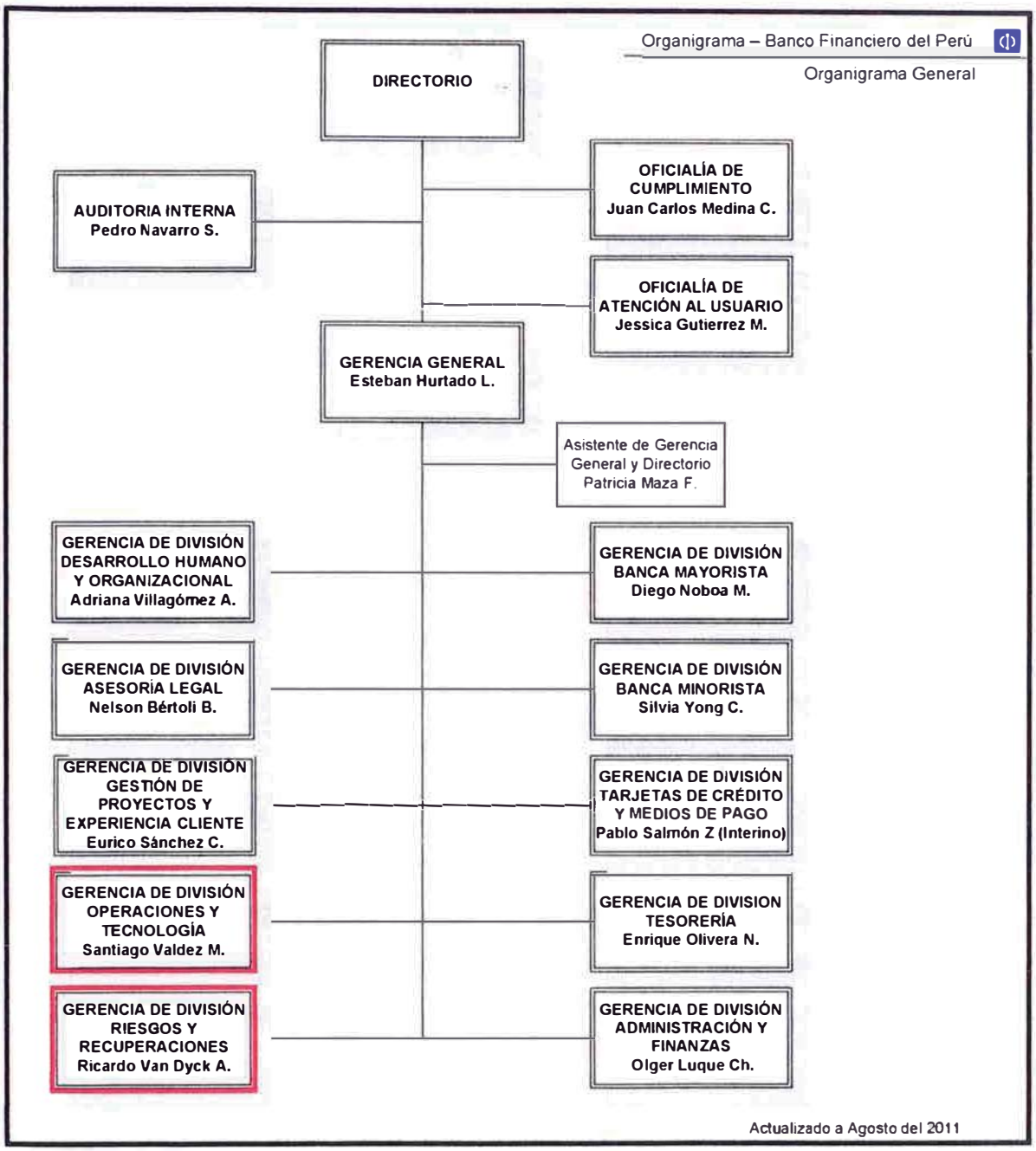
c) Orientación al Logro

- Visión global
- Integridad
- Pro actividad
- Responsabilidad y compromiso

1.1.1.4. Organigrama de la Organización

A continuación se muestra el organigrama del Banco

ESQUEMA N° 01: Organigrama del Banco



Fuente: Empresa Bancaria

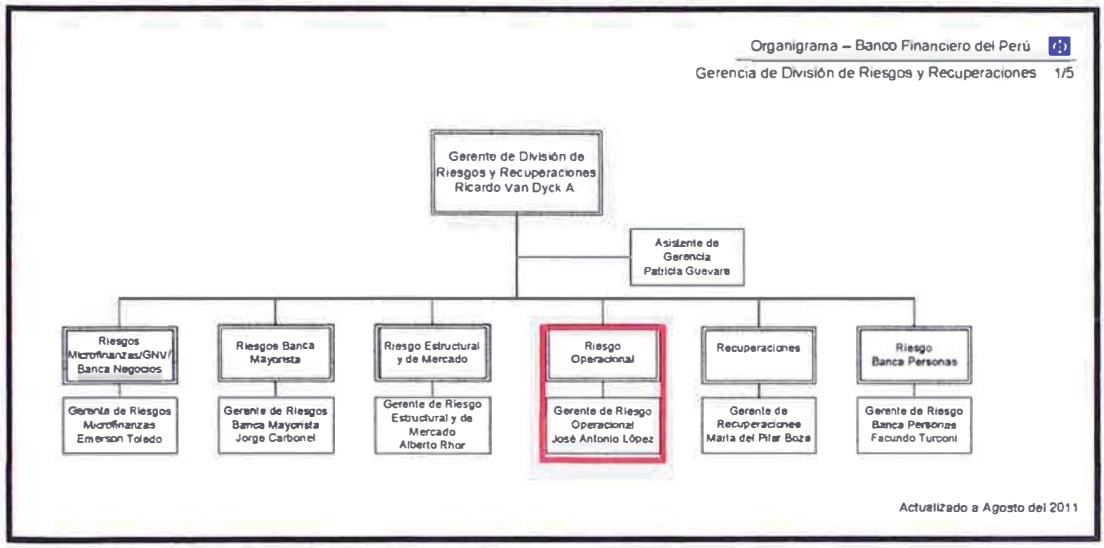
Elaboración: Empresa Bancaria

Las Gerencias en donde se centra nuestro estudio son en las áreas de **Gerencia de División de Riesgo y recuperaciones junto con la Gerencia de División de Operaciones y Tecnología.**

1.1.1.5. Organigrama del área de Trabajo

A continuación mostramos el detalle de la Gerencia de División de Riesgos y Recuperaciones. Lo sombrado con rojo es el área en la cual se ha realizado el trabajo.

ESQUEMA N° 02: Organigrama del área de trabajo 01

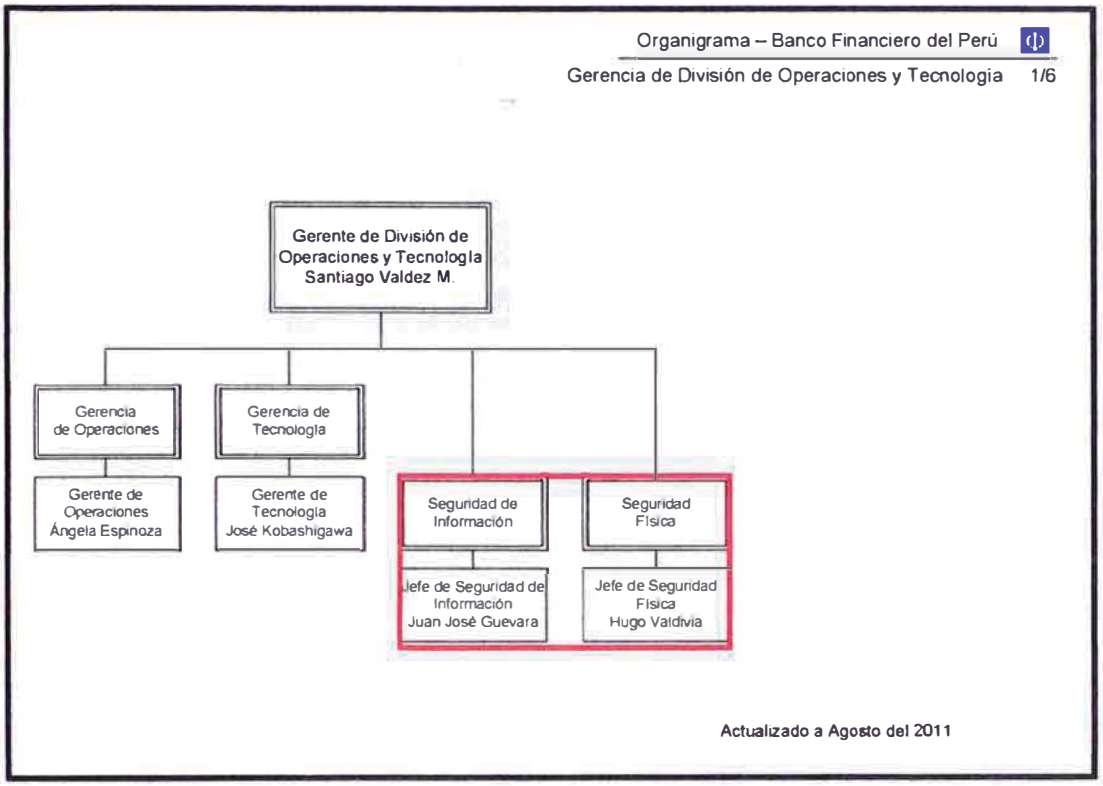


Fuente: Empresa Bancaria

Elaboración: Empresa Bancaria

Con respecto a la Gerencia de División de Operaciones y Tecnología. Lo sombrado con rojo es el área en la cual se ha realizado el trabajo.

ESQUEMA N° 03: Organigrama del área de trabajo 02



Fuente: Empresa Bancaria

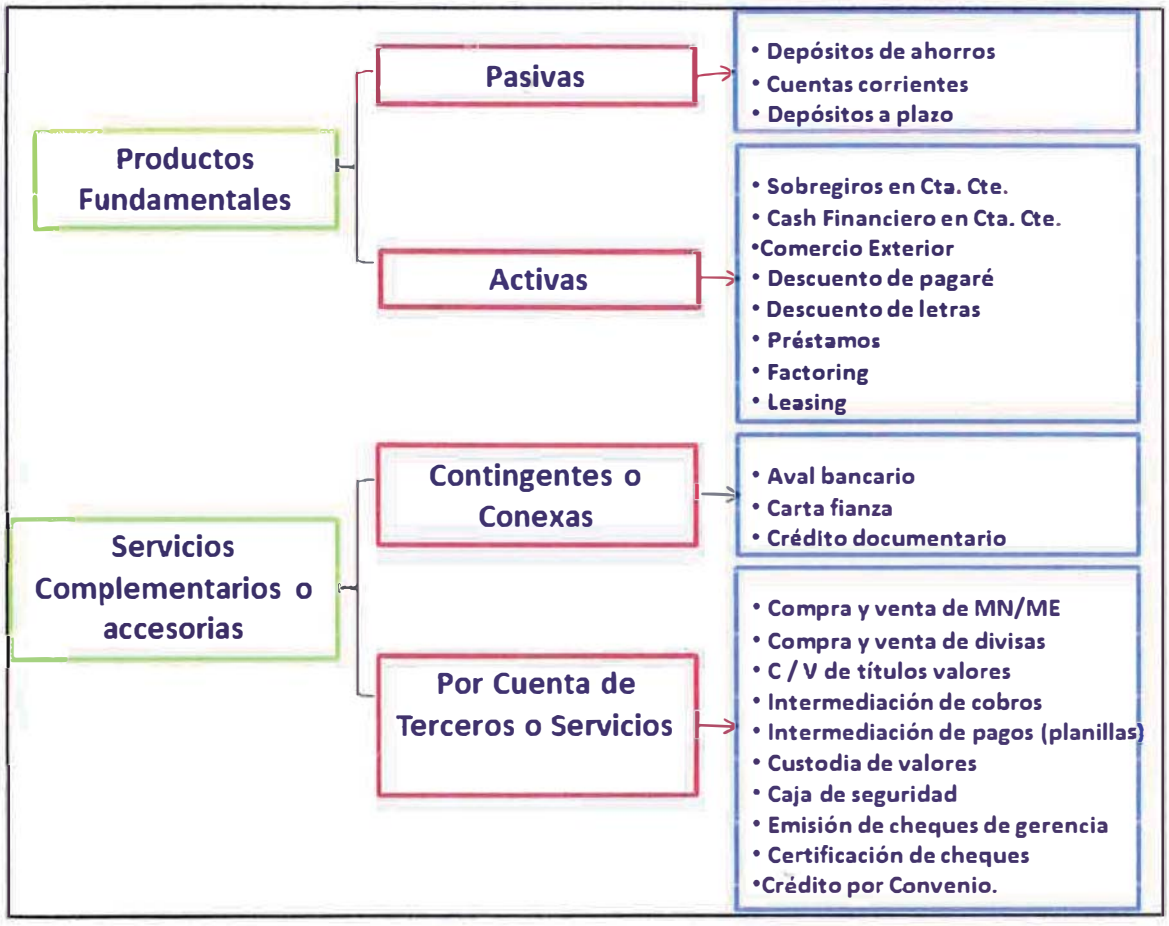
Elaboración: Empresa Bancaria

1.1.2. Clientes

1.1.2.1. Productos y Servicios

Los productos y servicios que el Banco Proporciona a los clientes están orientados a la clase B y C; orientándose al mercado microempresario. Mostramos el cuadro en el cual se puede apreciar todos los productos y servicios que el Banco Ofrece.

GRÁFICO N° 01: Productos y Servicios del Banco



Fuente: Empresa Bancaria

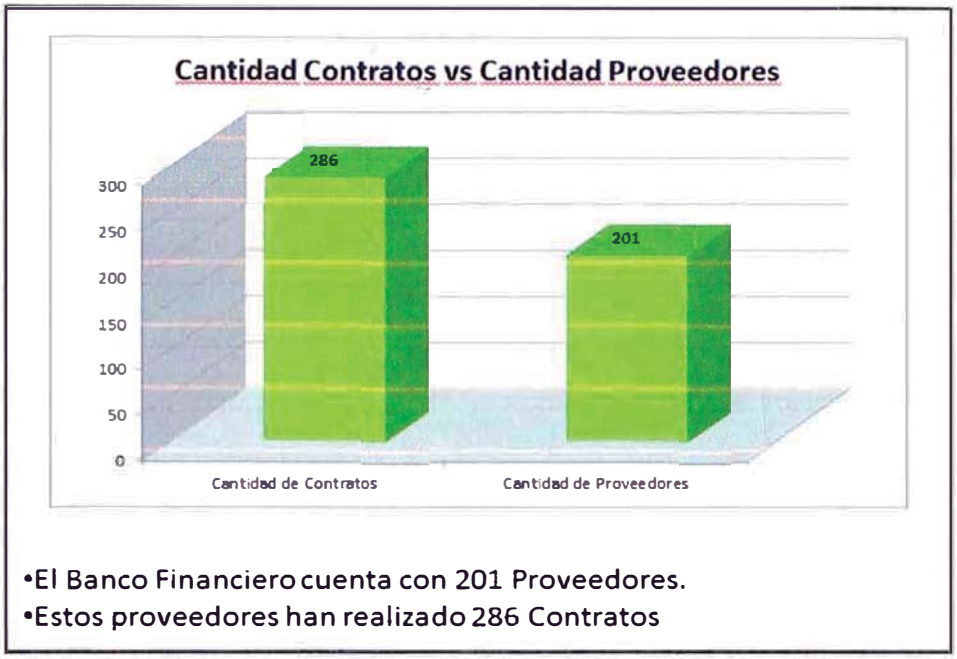
Elaboración: Propia

1.1.3. Proveedores

El Banco cuenta con proveedores, los cuales se clasifican por la información que manejan y el riesgo que podría existir en el cumplimiento del servicio solicitado.

Aquí mostramos la cantidad de los contratos y proveedores:

GRÁFICO N° 02: Contratos y Proveedores

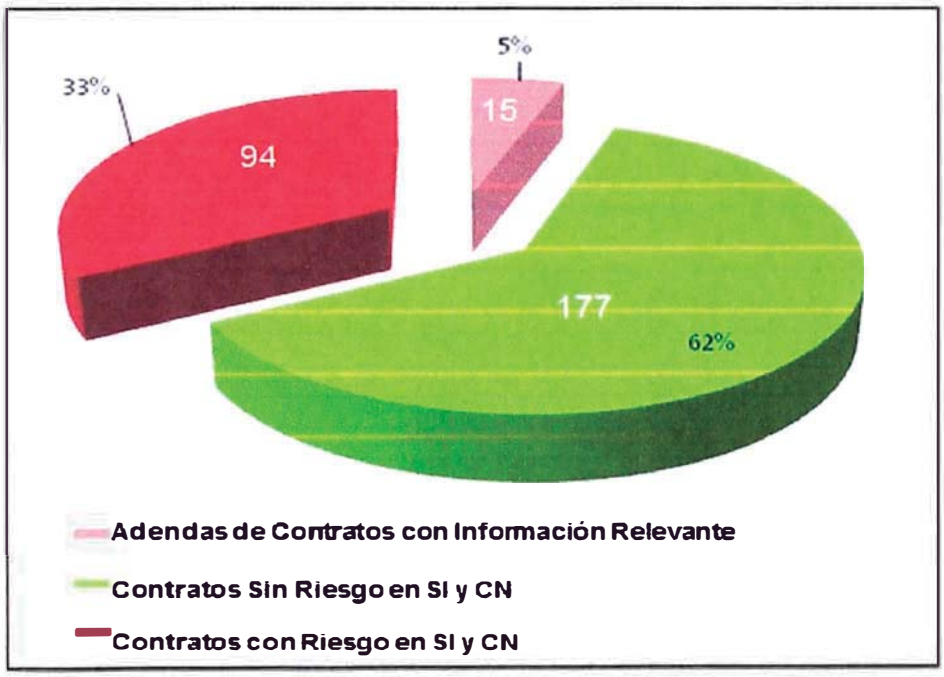


Fuente: Empresa Bancaria

Elaboración: Propia

Aquí mostramos la clasificación de los contratos y proveedores según el riesgo de representa, esta clasificación fue realizada por un grupo de expertos.

GRÁFICO N° 03: Riesgo de Contratos



Fuente: Empresa Bancaria

Elaboración: Propia

El siguiente cuadro muestra a los proveedores más representativos y críticos del Banco los cuales deben ser monitoreados permanentemente para reducir cualquier riesgo. La criticidad de los proveedores fue clasificada por el nivel de información confidencial que manejan y la importancia frente al negocio (monto en $)

CUADRO N° 01: Proveedores más críticos

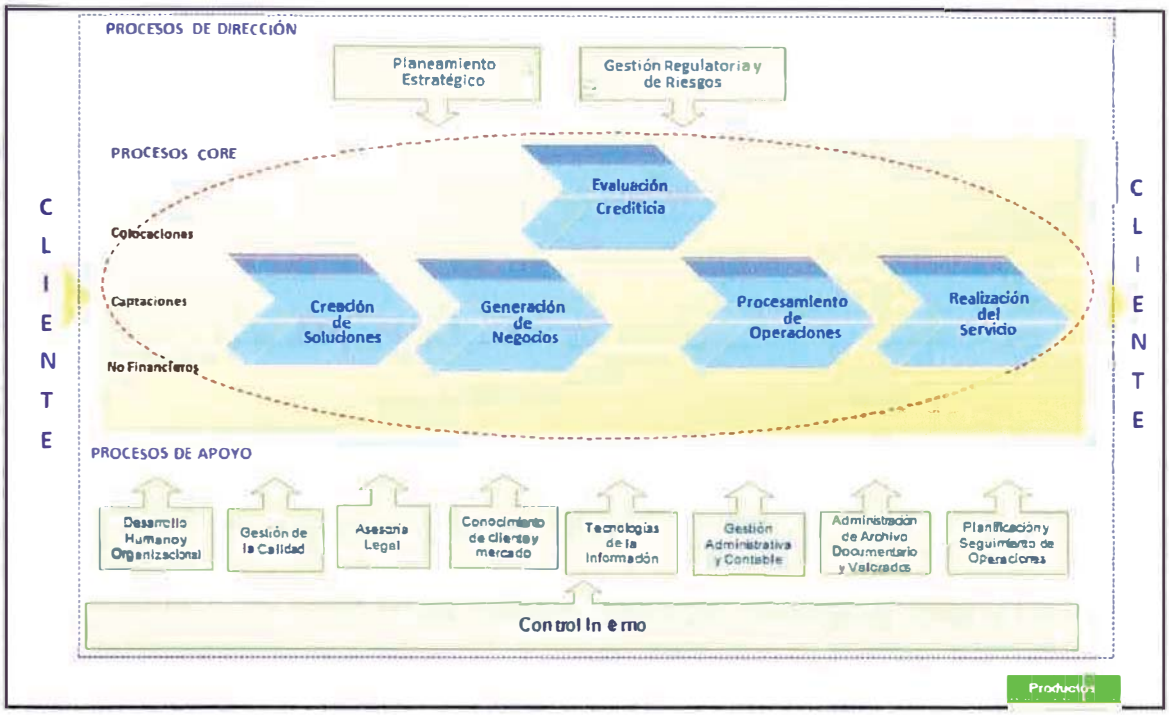
Fuente: Empresa Bancaria

Elaboración: Empresa Bancaria

1.1.4. Cadena de Valor del Banco

Es necesario definir y describir a la Empresa mediante procesos, por lo que me muestra el siguiente gráfico con los macro procesos del Banco.

SQUEMA N° 04: Cadena de Valor del Banco



Fuente: Empresa Bancaria

Elaboración: Propia

1.1.4.1. Procesos de Dirección

a) Planeamiento Estratégico. Son los procesos en donde se realizan la planificación estratégica anual, que determinan el rumbo de la empresa.

b) Gestión Regulatoria y de Riesgos. Son aquellos procesos que reducen los riesgos del negocio y cumplen con los pedidos solicitados por los entes reguladores.

1.1.4.2. Procesos Core

a) Captaciones. Se encargan de captar dinero (pasivos) los cuales brindan una tasa de interés a los clientes por el dinero que dejan los clientes (depósitos)

b) Colocaciones. Son los procesos que se encargan de prestar el dinero a los clientes que lo requieren (prestamos) para diversas actividades.

c) Recuperación. Son los procesos de cobranzas orientados a colocaciones, aquí tenemos cobranza prejudical, judicial, etc.

d) Negocios No financieros. Son aquellos servicios que el banco brinda tales como el Servicio de Bóvedas; pago a la planilla de los clientes, cheques de gerencia, etc.

1.1.4.3. Procesos de Apoyo

a) Desarrollo Humano y Organizacional. Proceso orientado al personal de la empresa Reclutamiento, selección, remuneraciones, etc.

b) Gestión de Calidad. Proceso orientado a reducir los costos y aumentar la productividad, para esto despliega metodologías que permiten su mejora continua; además de gestionar proyectos.

c) Asesoría Legal. Proceso orientado a la parte legal del Banco.

d) Conocimiento de cliente y Mercado. Proceso orientado a la satisfacción del cliente y análisis de mercado para orientar esfuerzos a aumentar las colocaciones y captaciones.

e) Tecnología de Información. Soporte de información y tecnología para un manejo normal de la organización.

f) Gestión Administrativa contable. Proceso orientado a mantener la contabilidad de la mejor forma.

g) Administración de archivos documentarios y valorados. Proceso orientado a administrar los documentos valorados del banco.

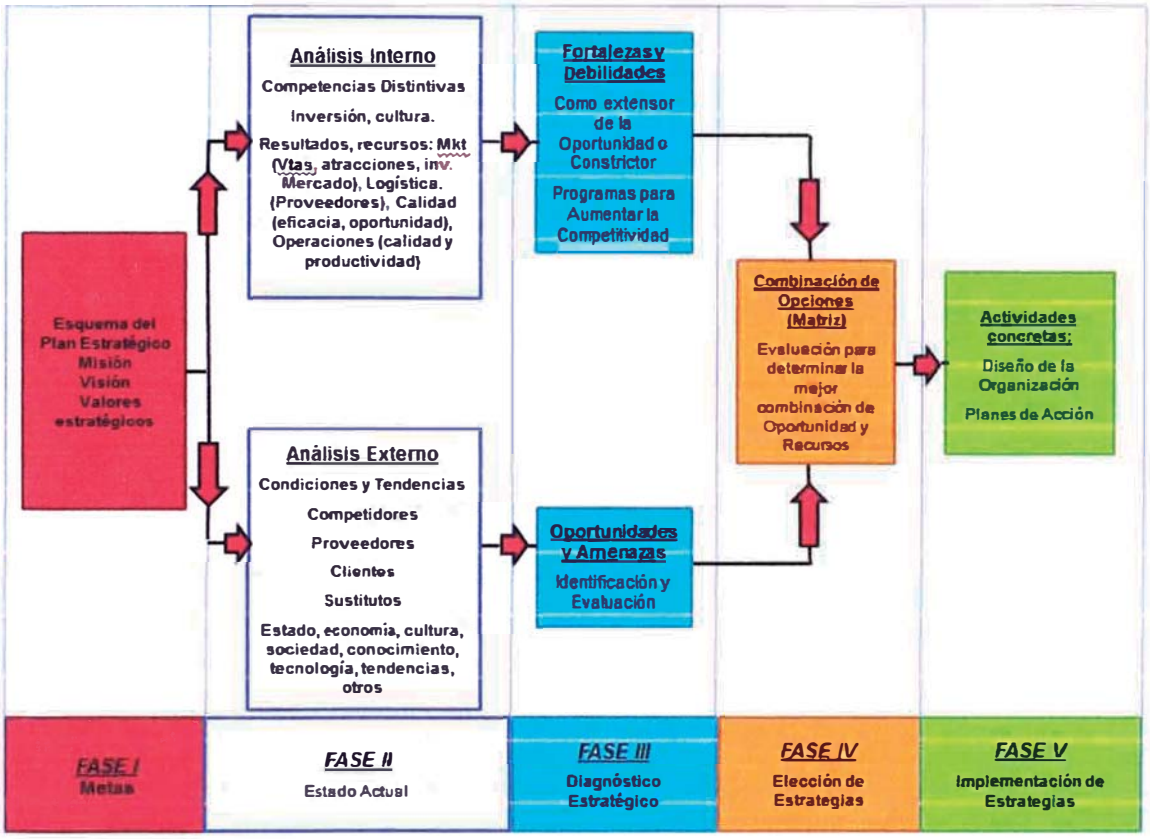
h) Planificación y seguimiento de Operaciones. Procesos orientados a reducir cualquier error en la parte de operaciones.

i) Control Interno. Proceso de auditoría interna que tiene el fin de identificar hallazgos en la organización con el fin de mejorar los procesos y sus resutlados.

1.2. DIAGNÓSTICO ESTRATÉGICO

Para realizar el Diagnóstico Estratégico del Banco hemos utilizado el siguiente esquema, el cual nos proporcionará un rumbo para lograr un adecuado diagnóstico estratégico.

ESQUEMA N° 05: Fases del Plan Estratégico



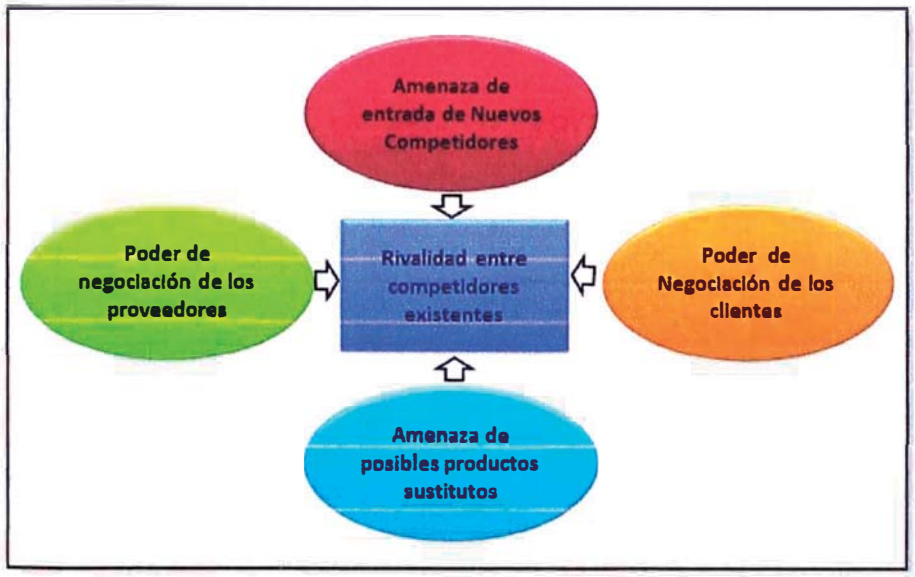
Fuente: Elaboración del Plan estratégico y Su implementación a través del cuadro de mando Integral

Elaboración: Propia

1.2.1. Análisis de las 5 Fuerzas de Porter

A continuación mostramos el esquema del estudio de las 5 fuerzas de Porter.

ESQUEMA N° 06: Las 5 fuerzas que Moldean la competencia de un sector



Fuente: Ser Competitivo – Michael E. Porter 2009 Ediciones Deusdo

Elaboración: Propia

1.2.1.1. Amenaza de Entrada de Nuevos Competidores

Con respecto a nuevos competidores es complicado el ingreso de un nuevo banco en el Perú, las leyes del Perú hacen complicado el ingreso de un nuevo banco; por lo tanto el ingreso de un nuevo competidor al Perú es difícil en este negocio por la cantidad de capital que hay que inyectar a la empresa, sin embargo cabe también la posibilidad de que los bancos mundiales puedan enfocar su interés en el Perú por el crecimiento que se viene teniendo por las inversiones extranjeras.

1.2.1.2. Rivalidad entre competidores existentes

Con respecto a la rivalidad entre los competidores podemos apreciar en el cuadro siguiente, donde mostramos las utilidades acumuladas y la participación de mercado.

CUADRO N° 02: Análisis de Participación de Mercado

#	En miles de nuevos soles	Utilidades Acumuladas			Variación Dic 2010 - 2011		Participación de Mercado		
		Utilidad Dic 2009	Utilidad Dic 2010	Utilidad Dic 2011	Δ	Δ %	A Dic 2009	A Dic 2010	A Dic 2011
1	Banco de Crédito del Perú	924.501	1.209.341	1.438.994	229.654	19%	28,48%	31,83%	33,22%
2	Banco Continental	927.611	1.007.247	1.128.963	121.717	12%	28,57%	26,51%	26,06%
3	Scotiabank Perú	637.053	680.197	788.493	108.296	16%	19,62%	17,90%	18,20%
4	Interbank	429.366	534.218	540.928	6.710	1%	13,23%	14,06%	12,49%
5	Mibanco	97.089	97.143	109.423	12.280	13%	2,99%	2,56%	2,53%
6	Banco Falabella Perú	82.548	112.302	104.779	(7.523)	-7%	2,54%	2,96%	2,42%
7	Banco Interamericano de Finanzas	50.474	54.107	66.777	12.670	23%	1,55%	1,42%	1,54%
8	Citibank	43.290	41.048	57.671	16.623	40%	1,33%	1,08%	1,33%
9	Banco Ripley	49.468	51.734	52.818	1.085	2%	1,52%	1,36%	1,22%
10	Banco Financiero	17.734	32.973	33.842	870	3%	0,55%	0,87%	0,78%
11	Banco de Comercio	14.659	14.964	16.582	1.619	11%	0,45%	0,39%	0,38%
12	Deutsche Bank Perú	15.821	10.362	16.068	5.716	55%	0,49%	0,27%	0,37%
13	Banco Azteca Perú	1.948	13.426	16.057	2.631	20%	0,06%	0,35%	0,37%
14	Banco Santander Perú	(1.769)	6.419	14.241	7.822	122%	-0,05%	0,17%	0,33%
15	HSBC Bank Perú	(43.132)	(65.511)	(53.386)	12.125	-19%	-1,33%	-1,72%	-1,23%
	SISTEMA	3.246.571	3.789.958	4.332.251	532.293	312%	100%	100%	100%

Fuente: Superintendencia de Banca, Seguros y AFP

Elaboración: Propia

1.2.1.3. Poder de negociación de los clientes

Desde el punto de vista empresarial y corporativo, definitivamente los clientes son los que tienen el poder de Negociación con respecto al banco; ya que la participación de mercado es baja con respecto a los demás bancos

Desde el punto de vista microempresario y personas naturales; el Banco tiene el poder de negociación ante las microempresas.

1.2.1.4. Poder de negociación de los proveedores

El Banco cuenta con diversos tipos de proveedores, el Banco tiene el poder de negociación; sin embargo es necesario mencionar que con algunos proveedores como Telefónica, Procesos Master Card, etc.; hay un poder compartido, ya que el banco no podría operar sin la red tecnológica, sin tarjeta de crédito o cheques.

1.2.1.5. Amenazas Posibles de productos sustitutos.

El producto sustituto para este tipo de negocios, es directamente la competencia entre los bancos, en estos casos el poder de negociación es compartida, ya que los clientes

pueden elegir diversas entidades financieras y obtener el mismo beneficio.

1.2.2. Análisis Externo

1.2.2.1. Oportunidades

- El Perú sube posiciones en ranking de Riesgo país, se encuentra en el cuarto mejor país ubicado en América Latina luego de Chile, Brasil y México. Esto fomenta a que las inversiones en el Perú se consoliden y sea más atractivo.[2]

- Algunos indicadores actuales y adelantados de actividad muestran que el crecimiento de la economía se ha estabilizado alrededor de su nivel sostenible de largo plazo. A continuación mostramos algunos indicadores.

CUADRO N° 03: Expectativas Macroeconómicas

ENCUESTA DE EXPECTATIVAS MACROECONÓMICAS: CRECIMIENTO DEL PBI (%)

	Encuesta realizada al:		
	29 de Feb.	31 de Mar.	30 de Abr.
SISTEMA FINANCIERO 1/			
2012	5,3	5,5	6,0
2013	5,6	5,7	6,0
2014	6,0	6,0	6,0
ANALISTAS ECONÓMICOS 2/			
2012	5,0	5,5	5,8
2013	5,6	6,0	6,2
2014	6,0	6,0	6,0
EMPRESAS NO FINANCIERAS 3/			
2012	5,5	5,8	6,0
2013	6,0	6,0	6,0
2014	6,0	6,0	6,0

1/ 22 empresas financieras en febrero, 24 en marzo y 22 en abril del 2012.
2/ 23 analistas en febrero, 21 en marzo y 19 en abril del 2012.
3/ Muestra representativa de empresas de los diversos sectores económicos.

Fuente: Superintendencia de Banca, Seguros y AFP

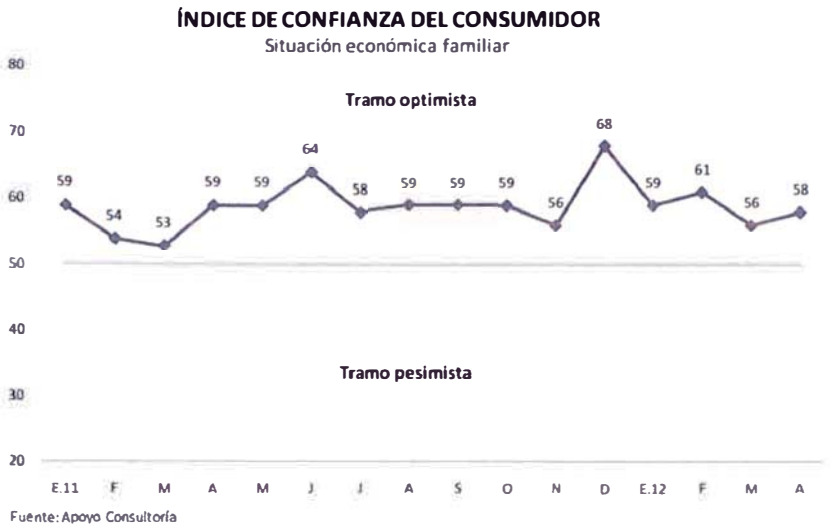
Elaboración: Informe de Situación Económica Actual

- La Confianza empresarial y del consumidor se mantienen en el tramo optimista. Esto crea el dinamismo económico el cual el Banco debe aprovechar para obtener mayores

[2] Diario Gestión: http://gestion.pe/noticia/350753/peru-sube-posiciones-ranking-riesgo-pais

clientes. A continuación mostramos los gráficos acreditan lo dicho anteriormente.

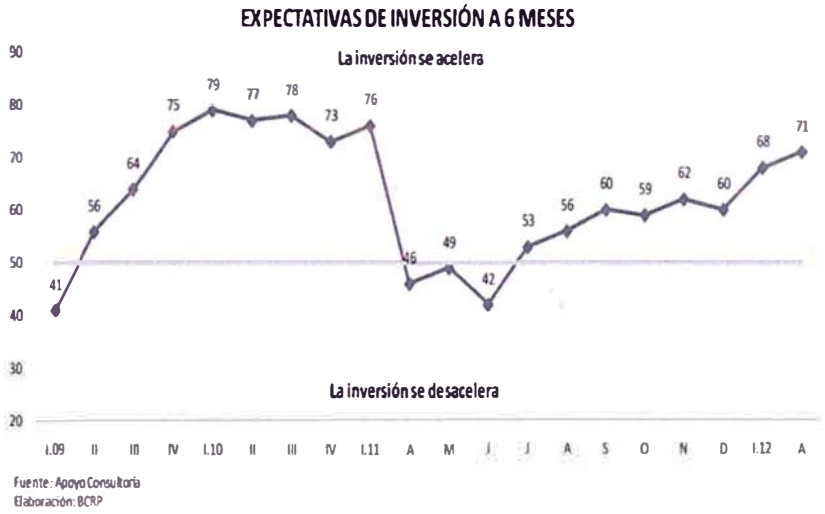
CUADRO N° 04: Confianza del Consumidor



Fuente: Superintendencia de Banca, Seguros y AFP

Elaboración: Informe de Situación Económica Actual

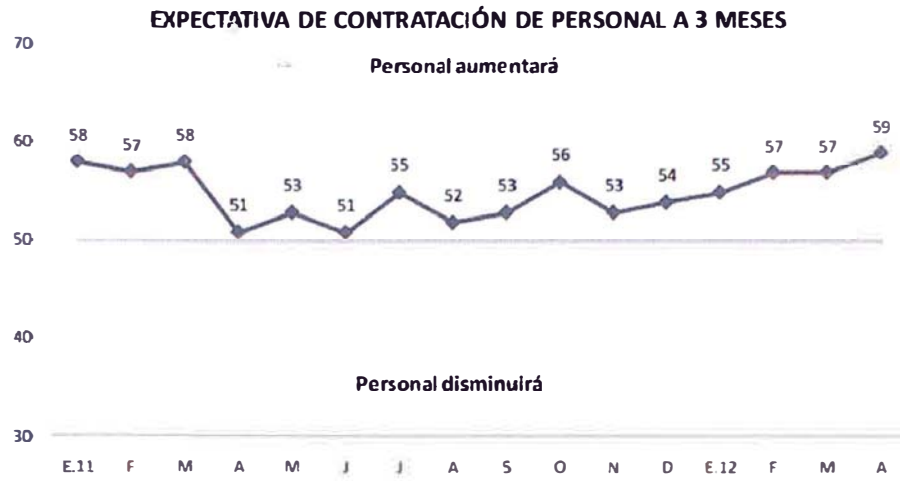
CUADRO N° 05: Inversión a 6 meses



Fuente: Superintendencia de Banca, Seguros y AFP

Elaboración: Informe de Situación Económica Actual

CUADRO N° 06: Contratación a 3 meses



Fuente: Superintendencia de Banca, Seguros y AFP

Elaboración: Informe de Situación Económica Actual

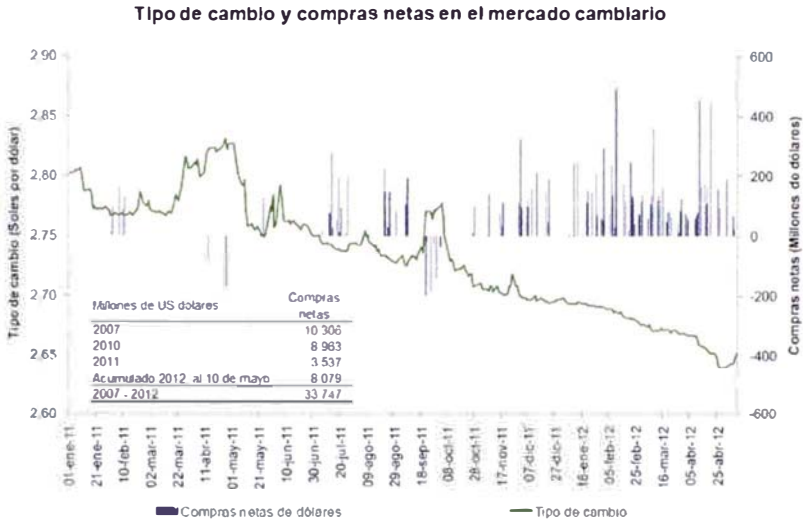
1.2.2.2. Amenazas

- La falta de liquidez que se podría generar al no tener una gestión eficiente de los recursos, para minimizar este riesgo, el banco tiene un área del control financiero y operacional, incluyendo el plan de contingencia de liquidez.
- La Superintendencia de banca, seguros y pensiones solicita la implementación de una adecuada gestión de riesgos crediticios y de mercado.
- La superintendencia de Banca, Seguros y pensiones; ha solicitado que los Bancos tengan una adecuada Gestión de Riesgos Operacionales, clasificándolos en tres niveles de Madurez: Básico, Intermedio y Avanzado. Cada nivel de madurez indica una reducción Requerimiento de Patrimonio por Riesgo Operacional.
- Los competidores de la banca tienen la mayor parte de la participación de mercado que el Banco, por lo que tiene que

mejorar las colocaciones, captaciones y gestionar mejor los riesgos para poder hace eficiente su gestión.

El capital del Banco es del Grupo Pichincha por lo que las inyecciones de capital se realizan en Dólares americanos. Actualmente la tendencia es que el sol se está apreciando; por lo que los dólares pierden su valor. A continuación mostramos el análisis.

CUADRO N° 07: Tipo de Cambio.



Fuente: Superintendencia de Banca, Seguros y AFP

Elaboración: Informe de Situación Económica Actual

1.2.3. Análisis Interno

1.2.3.1. Fortalezas

- El Banco tiene una red de agencias en todo el Perú (con más de 100 Agencias-Banco y Carsa), para los cuales tiene un contrato con Global Net operar en todos los cajeros en Perú.
- El Banco ha absorbido a la financiera Amerika; ampliando y mejorando su cartera de clientes.
- Tiene una Gestión por proyectos, todos los proyectos se Canalizan con el área de Gestión de Proyectos y cada

inversión debe sustentarse en el Tiempo. Optimizando los recursos.

1.2.3.2. Debilidades

- La marca del Banco no tiene la fuerza suficiente para mantenerse en la mente de las personas y empresas.
- El banco no busca brindar una experiencia del Cliente que lo diferencia de los demás
- La potencia comercial mediante la red de agencias del Banco no está consolidada.
- La participación de mercado del banco es muy bajo, es necesario hacerlo crecer, especialmente en provincias.
- El banco cuenta con el Método Básico de requerimiento de capital es mucho más alto, para esto deben implementar metodologías que permitan reducir en Riesgo operacional.

1.2.4. Matriz FODA

- La Matriz FODA, nos ayuda a identificar nuestras estrategias a seguir mediante el análisis de la Fortaleza, Oportunidad, debilidad y amenaza, con esto tenemos 4 tipos de estrategias que son: explotar, buscar, confrontar y evitar.

- A continuación mostramos la matriz FODA realizada para poder determinar las estrategias a seguir.

Estrategias	Fortalezas 1. Red de agencias en todo el Perú (100 Agencias) 2. Compra a AMERIKA FINANCIERA 3. Creación de Oficina de Gestión de Proyectos	Debilidades 1. La marca del Banco no tiene la fuerza suficiente 2. El banco no busca brindar una experiencia del Cliente que lo diferencia de los demás 3. La potencia comercial mediante la red de agencias del Banco no está consolidada. 4. La participación de mercado del banco es muy bajo. 5. El Banco no Gestiona bien los Riesgos.
Oportunidades 1. Reducción del Riesgo País a Perú 2. Crecimiento de la Economía peruana 3. La Confianza empresarial y del consumidor optimistas	FO: Explorar 1.1. Marketing Agresivo en Provincias para captar más clientes 2.2. Explotar la cartera de clientes de AMERIKA y generar más negocios 3.2 Optimización de inversiones en el BFP para generar mayor valor en la organización	DO: Buscar 1.1 Tomar acciones de incrementar la marca del banco en personas y empresas, proponer soluciones a la industria creciente. 3.2. Invertir en capacitación a los ejecutivos de cuenta para fidelizar a clientes, proponer productos a la medida. 2.3 Medir constantemente el ROA de cada agencia y desplegar fuerza de ventas industriales. 2.4 Es necesario brindar productos a la medida a las empresa para lograr aumentar la participación de mercado. 2.5 El crecimiento trae consigo riesgo crediticio, de mercado y operacional. Implementar los sistemas de Gestión que minimicen los riesgos para tener una cartera sana

Amenazas	FA: Confrontar	DA: Evitar
1. Falta de Liquidez 2. Riesgo de Crédito y Riesgo de mercado 3. Riesgo Operacional. (SBS) 4. Competidores agresivos 5. Reducción del Tipo de Cambio perjudicando inversiones en dólares	1.1 Crear un plan de contingencia de Liquidez para poder minimizar cualquier riesgo que pudiese presentarse. 2.1 Necesitamos implementar políticas claras para reducir el riesgo de Crédito principalmente. 3.1 Necesitamos implementar 3 sistemas integrados de gestión: Sistema de Gestión de Riesgo Operacional, Sistema de Gestión de Sistema de Seguridad de Información y Sistema de Gestión de Continuidad de Negocios para reducir los riesgos y obtener la autorización del Método estándar alternativo por parte de la SBS. 4.2 Debemos ganar más participación de mercado con la adquisición de Amerika Financiera, esto a su vez debe reforzar los negocios generados. 5.1 Las colocaciones y captaciones deben orientarse reduciendo el riesgo de mercado por tipo de cambio.	1.1 La Marca del BFP y la percepción debe ser de una Banco Sólido, con ello el Banco de Pichincha apoyará en caso de liquidez. 2.5 No se puede evitar por ser una regulación 3.5 No se puede evitar por ser una regulación 4.4 Debemos invertir en la fuerza generadora negocio 5.5 Políticas claras para inversiones que tengan riesgo de mercado.

De todas las estrategias del banco que mencionamos aquí; nuestro propósito de este documento es desplegar la estrategia **FA 3,1**; la cual es implementar 3 sistemas integrados de Gestión con el fin de Reducir los Riesgos Operacionales, tecnológicos y de catástrofe a su vez obtener el Método estándar alternativo por parte de la SBS; esto permitirá aumentar la imagen corporativa de la organización, reducir el requerimiento patrimonial y obtener mejores resultados con las clasificadoras de riesgos.

CAPÍTULO II

MARCO TEÓRICO Y METODOLOGÍA

2.1. ANTECEDENTES BIBLIOGRÁFICOS

Para desarrollar este informe se investigaron tesis e informes de suficiencia a fin de ilustrarnos con conceptos ya realizados y aprovechar los conocimientos desarrollados. A continuación se muestran los siguientes informes de suficiencia y tesis:

- Tesis: Metodología de análisis de riesgos en los sistemas de información de una empresa bancaria. Antonio Alejandro Cordero Rosado.
- Informe de Suficiencia: Adecuación de un banco de un sistema de gestión integral de riesgos – Miguel Ángel Loayza rojas
- Informe de Suficiencia: Administración de riesgos de tecnología de información en una institución financiera. – Oswaldo Manuel Cohaila Bravo
- Informe de Suficiencia: Modelo para la gestión de riesgo operacional en las empresas del sector financiero – Carlos Alejandro Bobadilla Guerrero.

2.2. BASES TEÓRICAS

2.2.1. VISIÓN GLOBAL DE LOS RIESGOS BANCARIOS

Al hablar de Riesgos Bancarios, primero debemos saber que es el riesgo, la relación de los riesgos operacionales bancarios con la macroeconomía, definir los pasos que se sigue para una administración de riesgos eficiente y finalmente nos enfocamos al COMITÉ BASILEA II, las cuales son estándares internacionales para Riesgos, por lo que a continuación damos un alcance de estos temas

2.2.1.1. La Administración de Riesgos

Según el Estándar Australiano Neozelandés 4360: 1999 Administración de Riesgo, define al riesgo como: "La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos, el cual se mide en términos de consecuencias o probabilidades.[3]

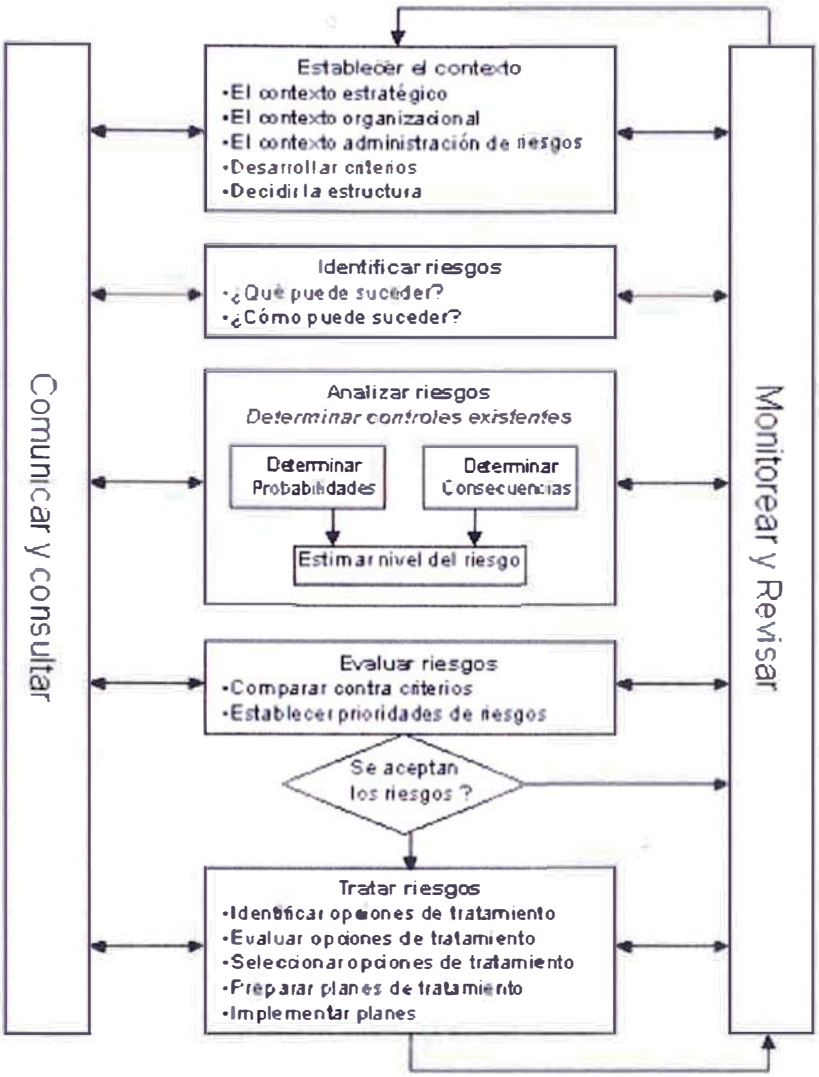
La administración de riesgos es reconocida como un parte integral de las prácticas gerenciales, es un proceso de interactivo que consta de pasos, los cuales cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones.

La administración de Riesgos es un método lógico y sistemático que establece el contexto, identifica, analiza, evalúa, trata, monitorea y comunica los riesgos asociados de una actividad, función o proceso, de tal forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. La administración de riesgos es identificar oportunidades, como evitar y mitigar pérdidas.

A continuación se muestran los elementos principales de la administración de riesgos, los cuales son utilizados para la implementación del Sistema de gestión de Riesgo operacional, Riesgos asociados a Seguridad de Información y Riesgos de Continuidad de negocios.

[3] Estándar australiano AS/NZS 4360_1999 – Administración de Riesgos - Definiciones

ESQUEMA N° 07: Procesos de la Administración de Riesgos



Fuente: Estándar Australiano Neozelandés AS/NZ 4360 : 1999

Elaboración: Estándar Australiano Neozelandés AS/NZ 4360 : 1999

Dentro de los procesos de análisis de riesgos, vamos a describir 3 tipos de análisis de riesgos:[4]

a) Análisis Cualitativo

[4] Estandar australiano Neozelandez AS/NZS 4360:1999 – Administración de riesgos

El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran. Estas escalas se pueden modificar o ajustar para adaptarlas a las circunstancias, y se pueden utilizar distintas descripciones para riesgos diferentes.

b) Análisis Semi-cuantitativo

En el análisis semi-cuantitativo, a las escalas cualitativas, tales como las descriptas arriba, se les asignan valores. El número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades. Los números pueden ser combinados en cualquier rango de fórmula dado que el sistema utilizado para priorizar confronta el sistema seleccionado para asignar números y combinarlos. El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo, y no sugerir valores realistas para los riesgos tales como los que se procuran en el análisis cuantitativo.

c) Análisis cuantitativo

El análisis cuantitativo utiliza valores numéricos para las consecuencias y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos y semi-cuantitativos) utilizando datos de distintas fuentes. La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados.

Estos procesos son utilizados para desplegar el sistema de gestión de Riesgo operacional, Riesgos

asociados a Seguridad de Información y Riesgos de Continuidad de negocios.

2.2.1.2. Riesgos bancarios y la Macroeconomía

El Nuevo acuerdo de capital (NAC – New Capital Committee) recomienda que los requerimientos de capital sean más sensibles a los riesgos bancarios que se enfrentan en el negocio bancario. Uno de los pilares del NAC reconoce la importancia del riesgo de mercado, crediticio y operacional.[5]

Pero además existen Riesgos materiales adicionales de impacto global, tales como el aumento del riesgo sistémico derivado de la concentración de mercados financieros; con respecto a la excesiva concentración. Y es aquí donde nos enfocaremos.

El sistema financiero mundial ha experimentado un proceso de concentración, producido por diversas causas entre las que destacan la salida del mercado de muchas instituciones financieras a nivel mundial y los proceso de fusión debido al crecimiento de las empresas o al redimensionamiento de los mercados internacionales. Como se puede apreciar en el cuadro, los 5 primeros bancos al nivel internacional agrupan el 10,55% de los activos de los 1000 grupos bancarios más grandes del mundo mientras que . Estos altos niveles de concentración justifican la magnitud del problema a discutir, así como la relevancia del problema de definir medidas regulatorias preventivas y de supervisión en un contexto de alta concentración en los mercados financieros y en una dimensión global.

[5] Examinando Riesgos Macroeconómicos en Basilea II: Propuesta de Supervisión para economías emergentes. Juan José Marthans

CUADRO N° 08: 25 Grupos Bancarios Más Grandes Según Activos

Orden actual	Nombre del grupo bancario	Activos (Millones de US $)	Participación en los 1000 primeros grupos (%)
1	Mizuho Financial Group, Tokio, Japon	1,285,471	2.33%
2	Citigroup, New York, EEUU.	1,264,032	2.29%
3	UBS Zurich, Suiza.	1,120,543	2.03%
4	Crédit Agricole Groupe, Paris, Francia.	1,105,378	2.01%
5	HSBC Holdings	1,034,216	1.88%
6	Deutsche Bank, Frankfurt, Alemania.	1,014,845	1.84%
7	BNP Paribas, Paris, Francia.	986,962	1.79%
8	Mitsubishi Tokyo Financial Group, Tokio, Japón.	974,950	1.77%
9	Sumitomo Mitsui Banking Corporation, Tokio, Japón.	950,446	1.73%
10	The Royal Bank of Scotland Group, Edinburgo, Reino Unido.	806,207	1.46%
11	Barclays, Londres, Reino Unido.	791,292	1.44%
12	Credit Suisse Group, Zurich, Suiza.	777,848	1.41%
13	JP Morgan Chase Bank, New York, EEUU.	770,912	1.40%
14	UFJ Bank, Tokio, Japón.	735,631	1.34%
15	Bank of America, Charlotte, EEUU.	736,445	1.34%
16	ING Bank , Amsterdam, Holanda.	684,004	1.24%
17	Société Générale, Paris, Francia.	681,218	1.24%
18	ABN AMRO Holding, Amsterdam, Holanda.	667,636	1.21%
19	HBOS, Londres, Reino Unido.	650,721	1.18%
20	Industrial & Commercial Bank of China, Beijing, China.	637,828	1.16%
21	Hypovereinsbank, Alemania.	605,525	1.10%
22	Dresdner Bank Group, Frankfurt, Alemania.	605,461	1.10%
23	Fortis Bank, Bélgica.	535,462	0.97%
24	Rabobank Group, Holanda.	509,352	0.92%
25	Commerzbank, Alemania.	481,921	0.87%
	Activos de los primeros 25	**20,414,330**	**37.06%**
	Activos de los primeros 1000	**55.084.539**	**100.00%**

Fuente: Ranking "Top 1000 World Banks" de la Revista "The Banker"

Fuente: Ranking "Top 1000 World Bank" de la revista "The Banker"

Elaboración: Ranking "Top 1000 World Bank" de la revista "The Banker"

En el Contexto Latinoamericano, el fenómeno de concentración de mercados financieros es evidente, y el Perú no es ajeno a ello, desde 1997 hasta el 2012, el sistema bancario peruano pasó de tener 24 bancos a sólo 15.

Pero ¿en qué repercute la concentración?, hay dos teorías: El enfoque de la "concentración y fragilidad" y el enfoque de "concentración y estabilidad".

El enfoque de concentración y fragilidad[6], propone que mientras más grande sea un banco, mayores serán sus incentivos a tomar riesgos, ya que se considera "demasiado grande para quebrar", así mismo su mayor tamaño deriva una mayor complejidad en sus negocios y un incremento de Riesgo Operacional[7].

En contraste, el enfoque de concentración y estabilidad enfatiza la hipótesis de que una mayor concentración deriva en una mayor estabilidad del sistema financiero, debido al mayor nivel de diversificación que se alcanza al aumentar la escala del banco, o porque los banco concentrados generan mayores ganancias, las cuales pueden constituir una reserva contra futuros adversos y es mucho más fácil supervisar y monitorear a pocos bancos en los mercados.

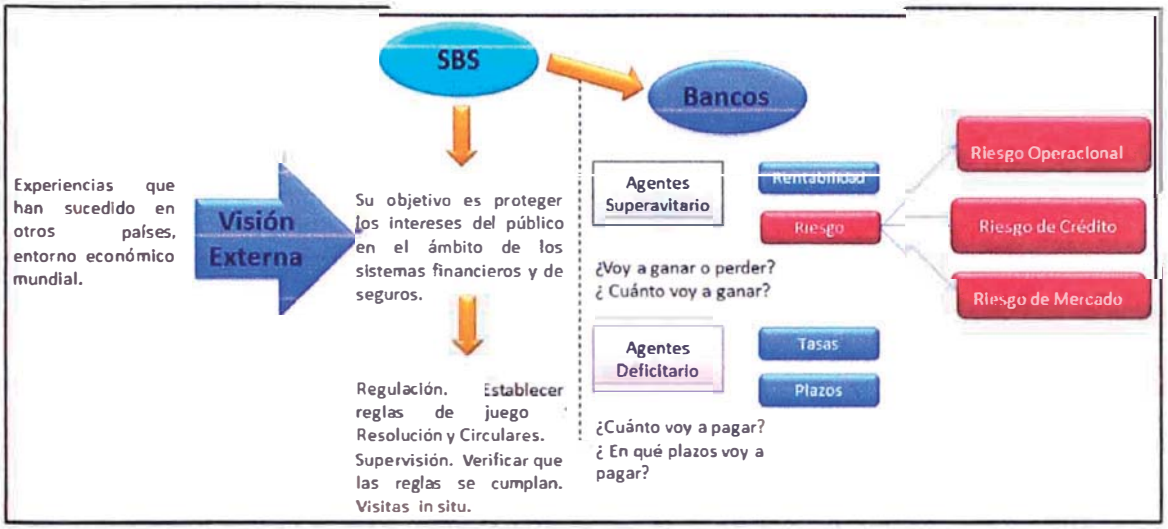
Estos contextos macroeconómicos son tomados por Basilea, los cuales buscan reducir los riesgos que se generan.

A continuación mostramos el siguiente cuadro, en el que se muestra la relación entre el ambiente económico externo junto con el objetivo del ente regulador.

[6] Examinando los riesgos Macroeconómicos en Basilea II: Propuestas de supervisión para economías emergentes. Juan José Marthan.

[7] Existen varios casos que muestran la relevancia de este tipo de riesgo. Desde los casos de ENRON y World Trade Center, que afectaron a numerosas empresas financieras y no financieras; o los famosos casos de fraude de Bank of credit and commerce International (BCCI) en 1991 y el Long Term Capital Management en 1998, hasta casos de sobre exposición en operaciones de trading como el caso de la corporación Sumitomo en 1996, las empresas del Grupo Prudential en 1994 o Baring en 1995.

CUADRO N° 09: 25 Visión Macroeconómico



Fuente: Banca Comercial – Roxana Escoto Leiva

Elaboración: Propia

Además podemos apreciar que las regulaciones van orientadas hacia los 3 tipos de riesgos.

2.2.1.3. Comité Basilea II

Fue establecido como comité de regulación bancaria y practicas supervisoras por los Bancos Centrales del Grupo de los 10 (G-10) a finales de 1974 como resultado de la turbulencia monetaria y bancaria internacional.

Los países miembros del Comité son Japón, Canadá, estados Unidos, Reino Unido, Francia, Alemania, Italia, Holanda, Bélgica, Luxemburgo, Suecia, Suiza y desde 2001 España.

2.2.1.4. Objetivos del Comité

El Objetivo principal del Comité es mejorar el entendimiento y la calidad de la supervisión bancaria en el Mundo. Para lograrlo, el Comité se basa en:

d) El intercambio de información a través de acuerdos nacionales de supervisión

e) El desarrollo de una mayor efectividad de las técnicas de supervisión para bancos internacionalmente activos

f) Establecimiento de estándares mínimos de supervisión.

2.2.1.5. Funciones del Comité de Basilea

Formular estándares y pautas generales de supervisión bancaria

Emitir declaraciones de mejores prácticas a fin que las autoridades individuales tomen las medidas necesarias para aplicarlas de la forma que mejor convenga a sus propios sistemas nacionales

Fomentar la convergencia hacia enfoques y estándares comunes sin procurar la amortización detallada de técnicas de supervisión de los países miembros.

2.2.1.6. Los 3 pilares importantes de Basilea II

a) Pilar I. El cálculo de los requisitos mínimos de Patrimonio

Constituye el núcleo del acuerdo e incluye una serie de novedades con respecto al anterior: tiene en cuenta la calidad crediticia de los prestatarios (utilizando ratings externos o internos) y añade requisitos de capital por el riesgo operacional.

La norma de Basilea I, que exige fondos propios > 8% de activos de riesgo, considerando: (riesgo de crédito + riesgo de negociación+ riesgo de tipo de cambio) mientras que ahora considera: (riesgo de crédito + riesgo de

negociación+ riesgo de tipo de cambio + riesgo operacional)

Dentro del riesgo de crédito se otorga un tratamiento especial a las titulizaciones, para las cuales se debe analizar si existe una transferencia efectiva y significativa del riesgo, y si son operaciones originadas por la entidad o generados por otras.

El riesgo operacional se calcula multiplicando los ingresos por un porcentaje que puede ir desde el 12% hasta el 18%. Existen 3 métodos alternativos para calcularlo dependiendo del grado de sofisticación de la entidad bancaria.

b) Pilar II. El proceso de supervisión de la gestión de los fondos propios

Los organismos supervisores nacionales están capacitados para incrementar el nivel de prudencia exigido a los bancos bajo su jurisdicción. Además, deben validar tanto los métodos estadísticos empleados para calcular los parámetros exigidos en el primer pilar como la suficiencia de los niveles de fondos propios para hacer frente a una crisis económica, pudiendo obligar a las entidades a incrementarlos en función de los resultados.

Para poder validar los métodos estadísticos, los bancos estarán obligados a almacenar datos de información crediticia durante periodos largos, de 5 a 7 años, a garantizar su adecuada auditoría y a superar pruebas de "stress testing".

Además se exige que la alta dirección del banco se involucre activamente en el control de riesgos y en la planificación futura de las necesidades de capital. Esta autoevaluación de las necesidades de capital debe ser discutida entre la alta dirección y el supervisor bancario. Como el banco es libre para elegir la metodología para su

autoevaluación, se pueden considerar otros riesgos que no se contemplan en el cálculo regulatorio, tales como el riesgo de concentración y/o diversificación, el riesgo de liquidez, el riesgo reputaciones, el riesgo de pensiones, etc.

c) Pilar III. La disciplina del Mercado

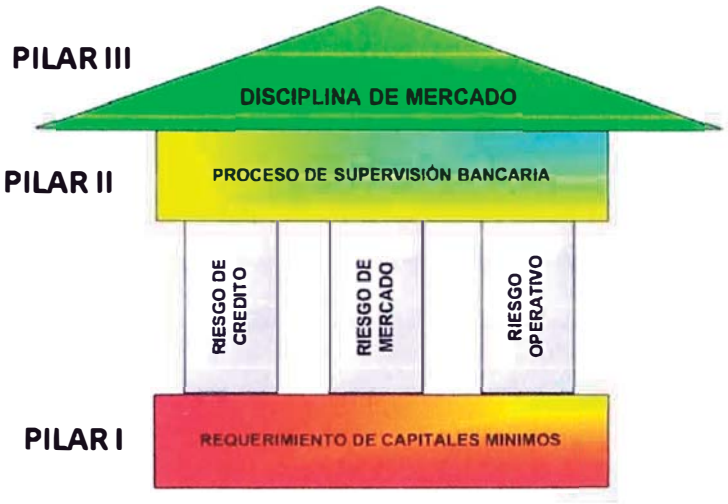
El acuerdo establece normas de transparencia y define la publicación periódica de información acerca de su exposición a los diferentes riesgos y la suficiencia de sus fondos propios. El objetivo es:

- La generalización de las buenas prácticas bancarias y su homogeneización internacional.
- La reconciliación de los puntos de vista financiero, contable y de la gestión del riesgo sobre la base de la información acumulada por las entidades.
- La transparencia financiera a través de la homogeneización de los informes de riesgo publicados por los bancos.
- Descripción de la gestión de riesgos: objetivos, políticas, estructura. organización, alcance, políticas de cobertura y mitigación de riesgos.
- Aspectos técnicos del cálculo del patrimonio: diferencias en la consolidación financiera y regulatoria.
- Descripción de la gestión de capital.
- Composición detallada de los elementos del patrimonio regulatorio disponible.
- Requerimientos de patrimonio por cada tipo de riesgo, indicando el método de cálculo utilizado.

El requisito inicial es que se publique al menos anualmente, aunque es previsible que la frecuencia será mayor (al menos resumida) y a sus contenidos mínimos se irá añadiendo la información que el mercado exija en cada momento.

A continuación mostramos el esquema de los pilares de la gestión de riesgo bancaria, donde se muestra el requerimiento de patrimonio mínimo; los 3 tipos de riesgo que exigen los entes reguladores, el proceso de supervisión bancaria y al final la disciplina del mercado.

ESQUEMA N° 09: Los Pilares de la Gestión de Riesgo Bancaria

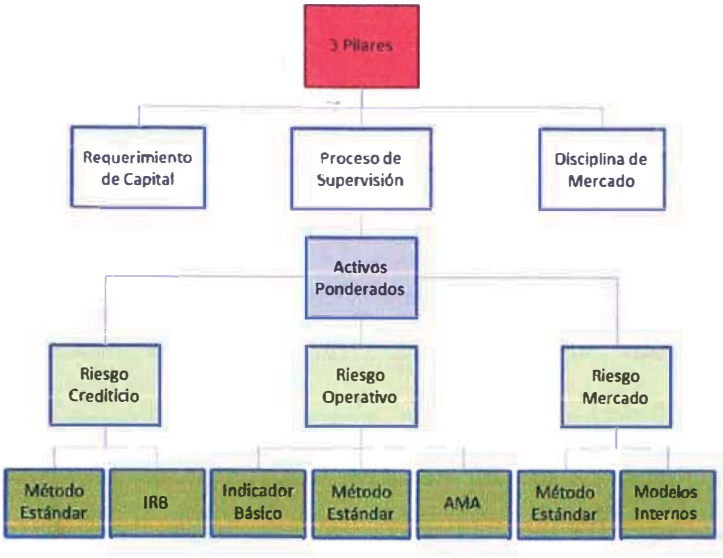


Fuente: El Banco en la Gestión de Riesgo (Die Bank im Risikomanagement) – Thomas Reicks

Elaboración: Propia

A continuación mostramos el organigrama en que se soporta los 3 pilares del riesgo bancario.

ESQUEMA N° 10: Basilea II – Estructura Básica



Fuente: El nuevo Acuerdo de Capital- Basilea II

Elaboración: Propia

2.2.2. RIESGO DE CRÉDITO

2.2.2.1. Introducción al Riesgo de Crédito

Antes de querer hacer cualquier comentario al respecto es necesario conocer la variable y el concepto de riesgo con la cual convivimos en el día a día en una institución financiera

En términos muy simples existe riesgo en cualquier situación en que no sabemos con exactitud lo que ocurrirá al futuro. En otros lugares Riesgo es sinónimo de Incertidumbre, es a la dificultad de poder predecir lo que ocurrirá.

No siempre el riesgo es malo se puede convivir con él a través de un incentivo. Es decir aceptaremos más Riesgo en la medida que haya recompensa. Es por ello que existe una relación muy estrecha entre riesgo y rentabilidad.

2.2.2.2. Principales Factores que determinan el Riesgo en Banca

Factores internos, que dependen directamente de la administración propia y/o capacidad de los ejecutivos de cada empresa

Factores externos, que no dependen de la administración, tales como inflación, depreciaciones no previstas de la moneda local, desastres climáticos, etc. aquí aparecen como importante el estado de los equilibrios básicos macroeconómicos que comprometan la capacidad de pago de los prestatarios

Frecuentemente, este riesgo se mide por las pérdidas netas de créditos entre los

Factores. Entre los factores internos están:

- **Volumen de crédito:** a mayor volumen de créditos, mayores serán las pérdidas por los mismos
- **Políticas de créditos:** cuento más agresivo es la política crediticia, mayor es el riesgo crediticio
- **Mezcla de créditos:** cuanta más concentración crediticia existe por empresas o sectores, mayor es el riesgo que se está asumiendo.
- **Concentración** geográfica, económica, por número de deudores, por grupos económicos y por grupo accionario: por ello no hay duda que cualquier tipo de concentración de cartera aumenta el riesgo de una institución financiera

2.2.2.3. Análisis de Riesgo de Crédito

Un aspecto de extraordinaria importancia en la gestión de los riesgos crediticios, es el relativo al análisis y evaluación del riesgo, así como la clasificación de los clientes. Estos procesos de análisis de riesgos precisan de

fuentes de información, tanto internas como externas y de unos sistemas específicos.

En una fase de análisis previo se debe medir y calificar el riesgo, esto es, analizar y valorar las contingencias, cuantificando cuál se va a asumir con el cliente y qué valoración tiene el mismo, asignándose límites de riesgos. Para ello se aplicarán sistemas de gestión y modelos de análisis de riesgos, que van alcanzando cada vez mayor grado de automatización. En este proceso de análisis de la solvencia, el credit manager debe estar en permanente contacto no sólo con el departamento financiero sino también con el departamento comercial, pues debe tenerse presente que una venta no se perfecciona hasta el momento de su cobro, lo que implica una coordinación entre ambos departamentos que procure acuerdos con los clientes, coberturas adecuadas, cumplimiento de los límites de riesgo asignados, autorizaciones de excedidos, etc. La gestión del riesgo precisa también de información externa que se obtendrá tanto de los registros oficiales como de empresas especializadas y bureaus de crédito.

Una vez debidamente valoradas y ponderadas estas variables según el modelo de análisis tomado, y efectuadas las oportunas correcciones en coordinación con el departamento comercial, se fijará el límite de riesgo del cliente que vendrá dado por el máximo quebrando económico que puede ocasionar en la empresa.

Las nuevas tecnologías aplicadas a este campo facilitan enormemente la actividad del gestor, permitiendo la automatización de procesos repetitivos y posibilitando la asignación de límites de riesgo por cliente de una forma fiable.

2.2.2.4. Aspecto Necesarios en la Evaluación de Crédito

El análisis de crédito debe contemplar un análisis los aspectos cualitativos (honorabilidad, administración, mercado de producción, competencia, etc.) y cuantitativos (balances, estado de pérdidas y ganancia, flujo de caja)

- El comportamiento del pasado de un cliente con una institución es un elemento muy importante para la decisión de futuros crédito, sin embargo es un elemento o necesario pero no suficiente, ya que hay que verlos aspectos cualitativos y cuantitativos
- La decisión de crédito definitiva es prever si un cliente podrá pagar o no en determinadas condiciones. Por consiguiente una decisión de crédito tomada exclusivamente tomada en base a antecedentes históricos presentes, sin contemplar el futuro está mal concedida

2.2.2.5. Gestión de Riesgo Crediticio del banco en estudio

Como consecuencia de la implementación de su Plan estratégico, el Banco ha efectuado importantes cambios con respecto al manejo y criterios de riesgo crediticio.

Antes del Plan estratégico, la determinación de la exposición máxima de cada cliente se hacía caso por caso, ahora existen criterios establecidos de riesgo máximo por cliente, por grupo económico y riesgo máximo total, que incluye créditos directos, indirectos y responsabilidad individual (avales y aceptaciones de letras).

Se establecieron límites por sector económico, además de haber identificado sectores de mayor riesgo a los que se les exige un esquema de garantías.

Los créditos se evalúan bajo dos modalidades: "***Caso por caso"*** y ***"Enlatados***", buscando una mayor eficiencia en la utilización de los recursos del Banco. Anteriormente todas las operaciones se evaluaban caso por caso, independientemente del importe en evaluación.

Se estableció una relación de préstamos prohibidos y límites a los sobregiros en cuenta corriente, que antes no existían.

Se asignaron responsabilidades a los funcionarios de negocio para el seguimiento y evaluación permanente del riesgo del cliente, utilizando las herramientas de Detección Temprana de Riesgo.

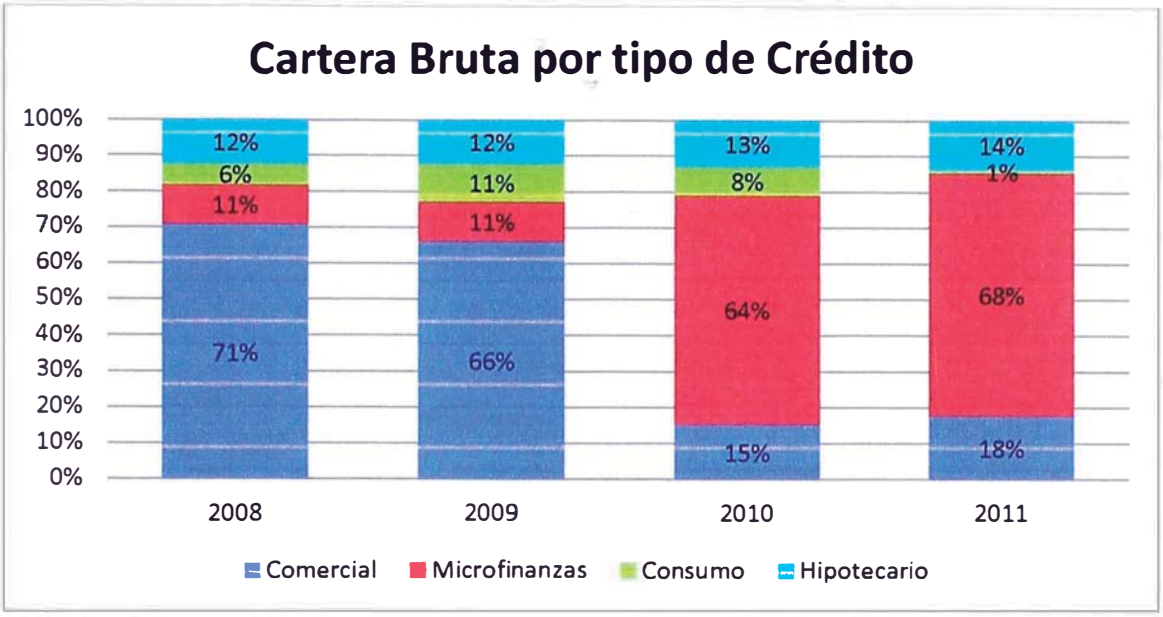
Para la evaluación de los créditos a microempresas cada funcionario elabora los estados financieros del cliente en caso estos no existan. Anteriormente dichos créditos se evaluaban bajo el sistema "Caso por caso", lo que generaba muchas ineficiencias debido a la naturaleza de los importes de dichos créditos. Actualmente se utiliza un sistema especializado.

Se ha incentivado el otorgamiento de microcréditos en moneda nacional. Anteriormente estos se desembolsaban en dólares, lo que carecía de sentido en vista que cerca del 100% de este tipo de clientes genera sus ingresos en soles.

El Banco tercériza el servicio de cobranzas con el objetivo de obtener una mayor eficacia y eficiencia en la utilización de los recursos.

El Banco cuenta con un modelo VaR (Value at Risk) para hacer análisis de riesgo cambiario crediticio.

CUADRO N° 10: Cartera Bruta por tipo de crédito



Fuente: "Clasificación de Riesgos Cass & asociados S.A.- Informe emitido"

Elaboración: Informe de Clasificación

2.2.3. RIESGO DE MERCADO[8]

2.2.3.1. Introducción al riesgo de mercado

La creación de valor es uno de los objetivos primarios que la entidad bancaria debe buscar por medio de la banca comercial, cuyas funciones de conocimiento general son:

Captar fondos para remunerarlos a determinadas tasas de interés (como producto pasivo) y luego colocarlos o invertirlos a tasas superiores, pero considerando un nivel de riesgos aceptable.

Sin embargo es conveniente tener en claro los siguientes puntos:

- La banca comercial aún no está especializada en la gestión de los Riesgos de Mercado.

[8] Riesgo de Mercado. http://www.slideshare.net/guestb20ade6/clase-2-riesgo-de-mercado-introduccion-al-var

- Toma fondos a los plazos que sus clientes quieren invertir y los coloca a los plazos a los que otros clientes quieren financiarse. En este proceso tiene poco margen para reducir el desfase temporal entre los plazos de captación y los de colocación.

- Lo anterior implica y de hecho es normal que los plazos de captación sean más cortos que los de colocación y eso significa que la banca debe cumplir sus compromisos, aún y cuando tengan incumplimiento con sus clientes y lo cual afecta sus compromisos y utilidades.

2.2.3.2. Definición de Riesgo de Mercado

Por riesgo de mercado se entiende la probabilidad de incurrir a pérdidas por el mantenimiento de posiciones en los mercados como consecuencias de mantenimientos adversos en variables financieras – factores de riesgo que determinan el valor de dichas posiciones.

2.2.3.3. Factores de Riesgo de Mercado

Los factores de riesgo de mercado son las siguientes:

- Tipos de interés
- Tipos de cambio
- Precio de acciones
- Precio de Commodities
- Otros

En los últimos años, el riesgo de mercado se ha convertido en el centro de atención tanto en las entidades financieras como en los organismos de supervisión. Esto es por un doble motivo:

- La creciente desregulación e internalización financiera de las economías y el proceso de desintermediación financiera han obligado el aumento de la competencia.

- El incremento de la volatilidad en los factores de riesgo ha hecho necesaria la aparición de nuevos instrumentos financieros y herramientas analíticas que ayuden a gestionar el riesgo.

La gestión de riesgos ha ido mejorando hasta alcanzar mayores logros en cuanto a metodología aplicada.

2.2.3.4. Concepto VaR

El VaR es un concepto que nace a finales de los 80 de la mano de JP Morgan.

Basilea I y II toma el concepto de VaR como válido su medición del riesgo de mercado.

Es una medida que intenta integrar diferentes riesgos financieros, no es una metodología

La máxima pérdida posible en un horizonte temporal y asociado a un nivel de confianza determinado, derivada del mantenimiento de una posición en cartera.

2.2.3.5. Requerimiento de Patrimonio por Riesgo de Mercado

Actualmente existe un documento en el cual se menciona el modo de calcular el requerimiento de patrimonio para el riesgo de mercado.

El documento es el requerimiento de patrimonio efectivo por Riesgo de Mercado (Resolución SBS N° 6328-2009) en la cual se encuentra más a detalle sobre el Riesgo de Mercado

2.2.4. RIESGO OPERACIONAL

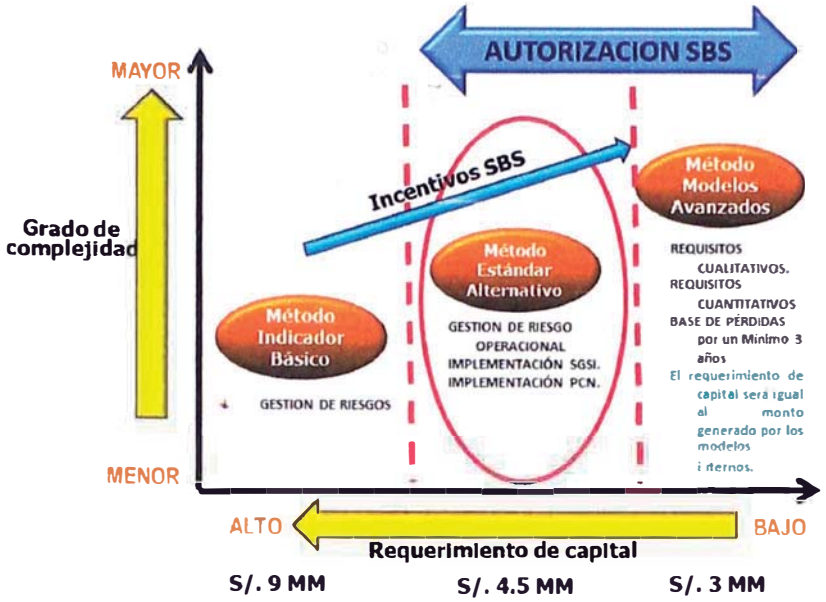
La superintendencia de Banca y Seguros, busca proteger a los clientes de las entidades financieras, para este fin solicita que los riesgos operacionales estén controlados, cada entidad tendrá Requerimiento de Patrimonio Efectivo por Riesgo Operacional de acuerdo al

nivel de madurez que se encuentre la entidad, para esto ha sacado dos resoluciones para el cumplimiento. El requerimiento de Patrimonio Efectivo por Riesgo Operativo 2115- 2116 .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:

- Método del indicador básico
- Método estándar alternativo
- Métodos avanzados

El uso del método estándar alternativo o de los métodos avanzados requiere la autorización expresa de la Entidad reguladora en tanto no se cuenten con la autorización señalada en el párrafo anterior, las empresas deberán aplicar el método del indicador básico. Para poder darnos cuenta de la diferencia de requerimiento de Capital, mostraremos este gráfico y luego pasaremos a describir cada uno de los métodos.

ESQUEMA N° 11: Esquema de Requerimiento de Capital



Fuente: Banco en Estudio

Elaboración: Banco en estudio

En el gráfico nos podemos dar cuenta que existe una gran diferencia en la Implementación de los diferentes métodos. Esto conlleva a un REQUERIMIENTO DE PATRIMONIO grande. Por lo que es necesario para el Banco, la implementación del Método Estándar Alternativo para reducir en 3.5 millones de Soles de requerimiento de capital aproximadamente.

2.2.4.1. Método del Indicador Básico

a) 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 cuentas contables definidas en las resoluciones.

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.

b) Cálculo del Requerimiento patrimonial [9]

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 (15%)

La fórmula de cálculo a utilizar es la siguiente:

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

dónde:

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 Entidad reguladora el cálculo del requerimiento patrimonial por riesgo operacional según el método del indicador básico. Esta información deberá ser remitida mensualmente vía SUCAVE, el cal es

[9] Calculo del requerimiento patrimonial Reglamento para el requerimiento de patrimonio efectivo por Riesgo Operacional (Resolución SBS N 2115-2009).

un software que utilizan los bancos para compartir información con la SBS; en un plazo que no exceda de 15 días calendario de concluido el mes a que corresponde dicho cálculo.

2.2.4.2. Método Estándar alternativo[10]

Requisitos mínimos para el uso del método estándar alternativo

Las empresas que deseen emplear el método estándar alternativo deberán cumplir con los siguientes requisitos:

- El Directorio y la Gerencia General deben participar activamente en la gestión del riesgo operacional.
- 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.
- 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.
- La empresa debe contar con una metodología de gestión del riesgo operacional que sea conceptualmente sólida y que se encuentre implementada en su totalidad.
- 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.

[10] Calculo del requerimiento patrimonial Reglamento para el requerimiento de patrimonio efectivo por Riesgo Operacional (Resolución SBS N 2115-2009).

- 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 que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operacional, y debe establecer políticas para tratar los casos de incumplimiento.
- 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.
- La empresa debe contar con una base de datos de eventos de pérdida por riesgo operacional, con las características señaladas en la normativa vigente.
- 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.
- 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.
- 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.

La evaluación de la gestión del riesgo operacional 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.

a) Determinación de líneas de negocio

En este método, las actividades de las empresas son divididas en las siguientes líneas de negocio:

Linea de negocio	Definición
Finanzas corporativas	Realización de operaciones de financiamiento estructurado y participación en procesos de titulación; 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.

b) Definición de los indicadores de exposición por riesgo operacional

Existen dos tipos de indicadores de exposición para las líneas de negocio:

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

$Gastos_i$: 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 resolución 2115 de la SBS.

Para la información correspondiente al año 2010 y siguientes se utilizará la agrupación de cuentas establecida en el Anexo 2B de la resolución 2115 SBS.

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:

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

Donde:

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.

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 (β) asociado con cada línea según se muestra en el siguiente cuadro:

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%

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:

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			$\left[\sum_{i=1}^{3} \max(S_i, 0)\right] / 3$		

Donde:

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

Las empresas deben presentar a la Entidad reguladora el cálculo del requerimiento patrimonial por riesgo operacional según el método estándar alternativo en un formato estandarizado. 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.

c) Sistema de Gestión de Seguridad de Información[11]

Un **Sistema de Gestión de la seguridad de la Información *(SGSI)*** es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

El término se denomina en Inglés "Information Security Management System" (ISMS).

El concepto clave de un SGSI es para una organización del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información

[11] Norma Técnica Peruana NTP 17799 – 2003 – ISO 27001. Buenas prácticas para la seguridad de información

minimizando a la vez los riesgos de seguridad de la información.

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.

La SBS ha definido que 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 operacionales 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.

Estructura organizacional

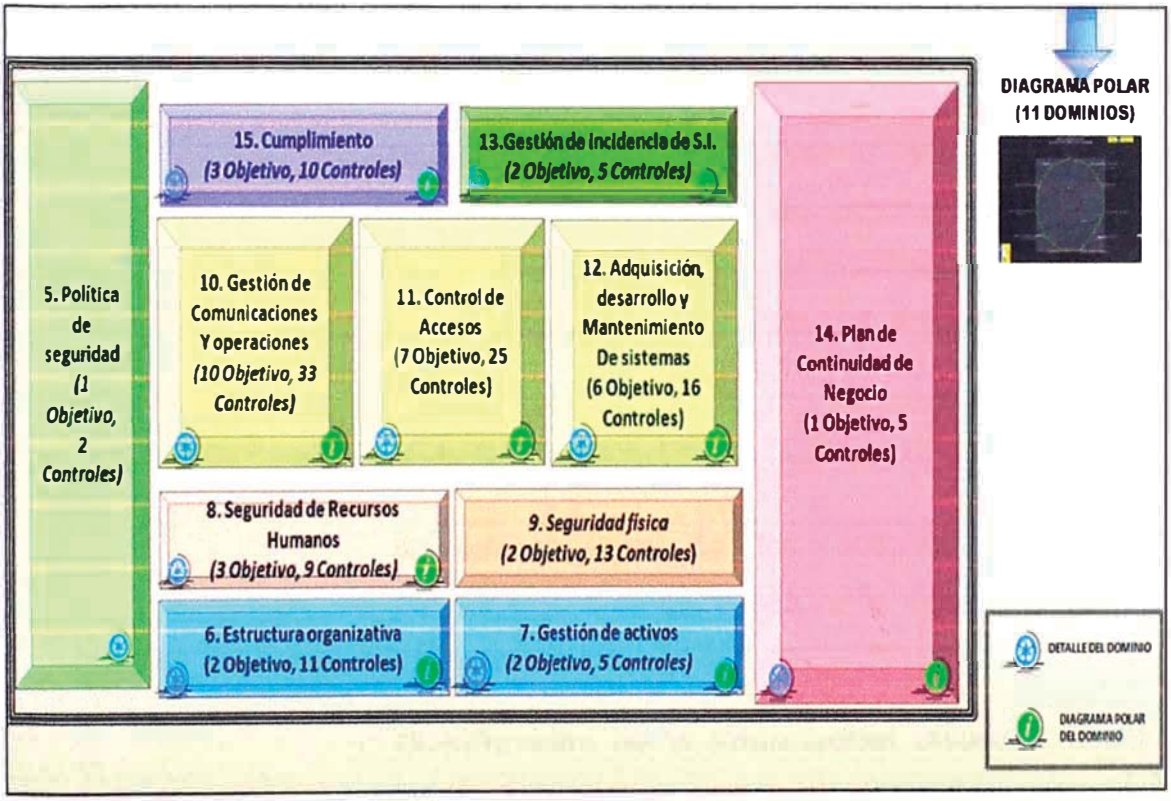
Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información señalado en el artículo anterior.

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:

- 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.

Además de la Implementación de los 133 controles que establece la ISO 17799 para toda la Organización, los cuales se desagrupan en objetivos de control para implementar el Sistema de Gestión de Seguridad de Información.

ESQUEMA 12: Tablero de Control SGSI



Fuente: ISO 27001 Information Security Management System

Elaboración: Propia

A Continuación ilustramos a detalle cada uno de los Dominios y Objetivos de control a implementar para desplegar el

Sistema de Gestión de Seguridad de Información según la Norma Técnica Peruana NTP-ISO/IEC 17799 – 2007. Código de buenas prácticas para la gestión de la seguridad de Información, Es preciso recalcar que cada uno de los objetivos de control tienen a su vez diversos controles que permiten aumentar la confidencialidad, integridad y disponibilidad de la seguridad de información.

Política de Seguridad de Información.

- **Política de seguridad de la Información**. Dirigir y dar a conocer a la gestión de la Seguridad de la Información, de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes.

Aspectos Organizativos para la Seguridad

- **Organización interna**. Gestionar la seguridad de información dentro de la organización
- **Partes Externas.** Mantener la seguridad de la información y recursos de procesamiento de la información que son accesados, procesados, comunicados, o gestionados por entidades o partes externas.

Gestión de activos

- **Responsabilidad de los activos.** Alcanzar y Mantener la protección apropiada de los activos de la organización
- **Clasificación de la información**. Asegurar que la información reciba un nivel apropiado de protección

Seguridad de Recursos Humanos

- **Previo al empleo**. Asegurar que los empleados, los contratistas y usuarios de terceras partes

comprendan sus responsabilidades, y que sean apropiados para los controles considerados y para reducir el riesgo del robo, fraude o mal uso de los recursos

- **Durante el empleo.** Asegurar que todos los empleados, contratistas y usuarios de terceras partes son conscientes de las amenazas y aspectos relacionados con la seguridad de la información, sus responsabilidades y obligaciones, y que estén equipados para respaldar la política de seguridad de la organización en el curso normal de su trabajo, y reducir el riesgo de error humano.

- **Terminación o cambio de empleo**. Asegurar que los empleados, contratistas y usuarios de terceras partes se retiran de una organización o cambian el empleo de una manera ordenada.

Seguridad Física y Ambiental

- **Áreas seguras**. Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones e información de la organización.

- **Seguridad de los equipos**. Prevenir pérdidas, daños, robo o comprometer los activos e interrupción de las actividades de la organización

Gestión de operaciones y comunicaciones

- **Procedimientos y responsabilidades operativas.** Asegurar la operación correcta y segura de los recursos de tratamiento de información.

- **Gestión de la provisión de servicios de terceras partes.** Implementar y mantener el nivel apropiado de seguridad de información y la entrega de servicio

en línea con los acuerdos de entrega de servicio de tercera parte.

- **Planificación y aceptación del sistema.** Minimizar el riesgo de falla de los sistemas.
- **Protección contra código móvil y malicioso**. Proteger la integridad del software y la información
- **Copia de seguridad.** Mantener la integridad y la disponibilidad de la información y los recursos de procesamiento de la información
- **Gestión de seguridad de la red.** Asegurar la protección de la información en las redes y la protección de su infraestructura de soporte
- **Manejo de Medios de Información**. Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de los activos, e interrupción de las actividades del negocio.
- **Intercambio de información**. Mantener la seguridad de información y e software intercambiado dentro de una organización y con cualquier entidad externa.
- **Servicios de comercio electrónico**. Asegurar la seguridad de servicios de comercio electrónico, y su utilización segura
- **Monitorización y Seguimiento.** Detectar las actividades de procesamiento de la información no autorizadas.

Control de Accesos

- **Requerimientos de negocio para control de accesos.** Controlar los accesos a la información

- **Gestión de acceso de usuarios**. Asegurar el acceso del usuario autorizados y prevenir el acceso no autorizado a los sistemas de información
- **Responsabilidades de usuario**. Prevenir el acceso de usuarios no autorizados, y comprometer o robar la información y los recursos de procesamiento de información
- **Control de acceso a la red**. Prevenir el acceso no autorizado a los servicios de red.
- **Control de acceso al sistema operativo**. Prevenir el acceso no autorizado a los sistemas operativos.
- **Control de acceso a la información y a las aplicaciones.** Prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación
- **Computación Móvil y trabajo a distancia**. Asegurar la seguridad de la información cuando se utilizan los recursos de computación móvil y trabajo a distancia.

Adquisición, desarrollo y mantenimiento de sistemas de información

- **Requerimientos de seguridad de los sistemas de información.** Asegurar que la seguridad es una parte integral de los sistemas de información
- **Correcto procesamiento de las aplicaciones.** Prevenir los errores, pérdidas, modificación no autorizada o mal uso de la información en las aplicaciones
- **Controles criptográficos.** Proteger la confidencialidad, autenticidad o integridad de la información por los medios criptográficos.

- **Seguridad de los ficheros del sistema**. Asegurar la seguridad de los activos del sistema
- **Seguridad en los procesos de soporte y desarrollo**. Mantener la seguridad del software y la información del sistema de aplicación.
- **Gestión de vulnerabilidades técnicas**. Reducir los riesgos que resultan de la exposición de las vulnerabilidades técnicas publicadas.

Gestión de incidentes de seguridad de la información

- **Informes de eventos y debilidades de seguridad de la información**. Asegurar que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente.
- **Gestión de incidentes y mejoras de la seguridad de la información**. Asegurar que un enfoque coherente y eficaz es aplicado a la gestión de los incidentes de seguridad de la información

Cumplimiento

- **Cumplimiento de los requerimientos legales**. Evitar incumplimientos de cualquier ley, estatuto, obligación o contractuales, y de cualquier requisito de seguridad.
- **Cumplimiento con las políticas, estándares y aspectos técnicos de la seguridad**. Asegurar el cumplimiento de los sistemas con las políticas y normas de la seguridad de la organización
- **Consideraciones de la auditoría de sistemas de información.** Maximizar la efectividad y minimizar

las interferencias en el proceso de auditoría del sistema de la información.

d) Sistema de Gestión de Continuidad del negocio[12]

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.

Las empresas deberán contar con una función de continuidad del negocio, la cual tendrá a su cargo las siguientes responsabilidades:

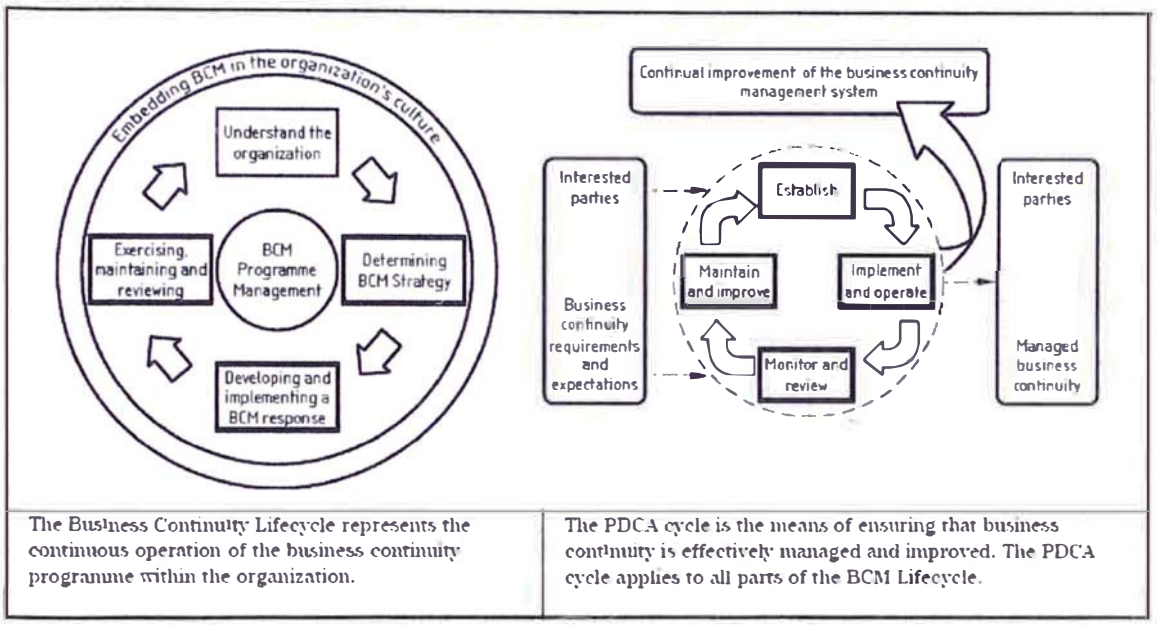
- ✓ Proponer las políticas, procedimientos y metodología apropiados para la gestión de la continuidad del negocio en la empresa, incluyendo la asignación de roles y responsabilidades;
- ✓ Velar por una gestión de la continuidad del negocio competente;
- ✓ Informar a la gerencia general y al comité de riesgos los aspectos relevantes de la gestión de la continuidad del negocio para una oportuna toma de decisiones.

[12] Business Continuity Management (BS 25999) / Circular 139 – 2009 Sistema de Gestión de Continuidad de Negocios

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.

Las Fases del Sistema de Gestión de Continuidad del Negocio son:

ESQUEMA 13: EL CICLO DE VIDA DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIOS



Fuente: BS35999 – 2007 BUSINESS CONTINUITY MANAGEMENT

Elaboración: BS 25999 Business Continuity Management

Aquí podemos apreciar las 6 fases importantes del Sistema de Gestión de Continuidad de Negocios, estas fases cumplen con el ciclo de Deming:

Entendimiento a la Organización. El propósito es permitir a la organización identificar las actividades críticas y recursos necesarios para soportar el negocio, entender las amenazas y elegir el apropiado tratamiento de riesgos.

- Análisis de Impacto al negocio

- Valorización del Riesgo
- Determinación de alternativas

- **Determinar la estrategia de continuidad de negocios**. Determinar las estrategias que permitan a la organización recuperar las actividades críticas con sus Tiempos Objetivos de Recuperación

- **Desarrollar e Implementar la Gestión de continuidad de negocios**. Permite desarrollar e implementar planes apropiados de continuidad de negocios y realizar acuerdos para administrar cualquier incidente que afecte las actividades críticas de la organización.
  - Estructura de respuesta a incidentes
  - Planes de continuidad de negocios y planes de gestión de incidentes

- **Ejecutar, mantener y revisar los acuerdos de la Gestión de Continuidad de negocios.** El propósito de esta fase es verificar la efectividad de los planes y asegurar que las actividades críticas serán recuperadas conforme a lo requerido.
  - **Ejecución del SGCN**
  - **Mantenimiento y revisión del SGCN**

- **Monitoreo y revisiones de la Gestión de Continuidad de Negocios.** El propósito es asegurar el monitoreo de la gestión de continuidad de negocio revisando su efectividad y eficiencia. Revisar la política de continuidad de negocios, objetivos y alcance, determinar y autorizar acciones para la remediación y mejora.
  - **Auditoría Interna**
  - **Gestión de Revisión del SGCN**

Desarrollar la cultura de Continuidad de Negocios en la Organización. El propósito es que toda la organización esté preparada ante cualquier evento y sepan cuáles serían sus acciones y actividades en ese momento.

2.2.4.3. 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.

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 Entidad reguladora 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).

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 reglamentos.

Para mayor detalle de lo requerido para el Método Avanzado, ver las resoluciones 2115 y 2116 de la SBS, la cual se encuentra en el anexo de este documento.

CAPÍTULO III

PROBLEMA, OBJETIVO Y MARCO TEÓRICO

3.1. IDENTIFICACIÓN DEL PROBLEMA

El Banco debe cumplir con requisitos regulatorios solicitados por la Superintendencia de Banca, Seguros y Pensiones para gestionar adecuadamente los riesgos operacionales, de seguridad de información y continuidad de negocios; a su vez disminuir el requerimiento de Patrimonio solicitado por la SBS con la Autorización ASA.

El Banco no cuenta con un Sistema de Gestión de Riesgo Operacional desplegado en la Organización, el cual es requisito para la autorización de la SBS - ASA

El Banco no cuenta con un Sistema de Gestión de Seguridad de Información desplegado en la Organización, el cual es requisito para la autorización de la SBS - ASA

El Banco no cuenta con un Sistema de Gestión de Continuidad de Negocio desplegado en la Organización, el cual es requisito para la autorización del al SBS - ASA

El problema es importante por las siguientes razones:

- El requerimiento patrimonial se incrementará sustancialmente si el Banco no implementa los sistemas de gestión para obtener la autorización del Método Estándar Alternativo.

- Cuando un Banco gestiona muy bien sus riesgos operacionales, la reducción de sus eventos de pérdida disminuye considerablemente y la reputación del Banco aumenta. Esto es una gran razón para la implementación del Sistema de Gestión de Riesgos operacionales.

- En cuanto a la Tecnología, también existen riesgos que pueden desencadenar eventos de pérdida monetaria y reputacionales; por la cual es importante minimizar esos riesgos, especialmente en banca, ya que toda la información se encuentra en diversos sistemas

- El banco debe asegurar a sus clientes su continuidad operativa a pesar de existir graves siniestros y escenarios; para ello debe desarrollar planes y probarlos a fin de obtener una retroalimentación y continuar con su proceso de mejora continua.

- La Superintendencia premia a los Bancos que tienen un nivel de madurez en la gestión de riesgos disminuyendo el requerimiento de patrimonio.

3.2. PLANTEAMIENTO DE ALTERNATIVAS DE SOLUCIÓN

3.2.1. Aumentar el patrimonio del banco mediante una inyección de liquidez.

- Un planteamiento de una solución es realizar una inyección de liquidez de aproximadamente 9 millones de soles y mantenerse en el método Básico de Riesgo Operacional; esta solución implica que los capitales inyectados no generen valor ya que mantiene el dinero inmovilizado, generando ineficiencia en la generación del valor en la organización y

limitando que el banco pueda desplegar un proceso de mejora continua.

3.2.2. Implementación de Sistemas de Gestión para reducir el requerimiento de Patrimonio solicitado por la SBS.

Este planteamiento trata sobre la postulación de la entidad bancaria a la autorización del Método Estándar alternativo (siguiente nivel del método de indicador básico), con el fin de reducir el requerimiento de capital solicitado por la SBS y disminuir los riesgos operaciones, de seguridad de información y continuidad de negocios.

Estas implementaciones permitirán aumentar el nivel de madurez del banco brindando mayor solidez al banco, así como mejores calificaciones de riesgo que se realizan en la empresa.

3.3. SELECCIÓN DE UNA ALTERNATIVA DE SOLUCIÓN

La alternativa de solución seleccionada es la implementación de los sistemas de gestión para reducir el requerimiento de patrimonio solicitado por la SBS. Las razones son el mejoramiento continuo y gestión adecuada de riesgo. Como pudimos apreciar en la elaboración de las estrategias a implementar, se da bastante prioridad a brindar solidez como banco y aumentar la reputación.

3.4. PLANES DE ACCIÓN PARA DESAROLLAR LA SOLUCIÓN PLANTEADA

3.4.1. Implementación del Sistema de Riesgo Operacional

3.4.1.1. Participación activa del Directorio y la Gerencia General en la Gestión de Riesgo operacional.

El Banco, se encuentra comprometido con la implementación de los sistemas de gestión para poder reducir el requerimiento patrimonial, además del

alineamiento en el planeamiento estratégico; esto a su vez genera la completa participación del Directorio y la gerencia general. Para esto el Gerente general delega su implementación al Gerente de División de Riesgos.

Para esto, el área de Riesgo Operacional conformado por Un gerente de Riesgo operacional, un Supervisor de riesgo operacional, dos analistas de riesgos operacionales y un practicante de riesgo operacional. Este equipo se encarga de cumplir con todos los requerimientos de la SBS, auditoría Interna, auditoria externa y de informar a la Gerencia General y al directorio sobre la gestión de Riesgo Operacional.

3.4.1.2. Función de la Gestión del Riesgo operacional

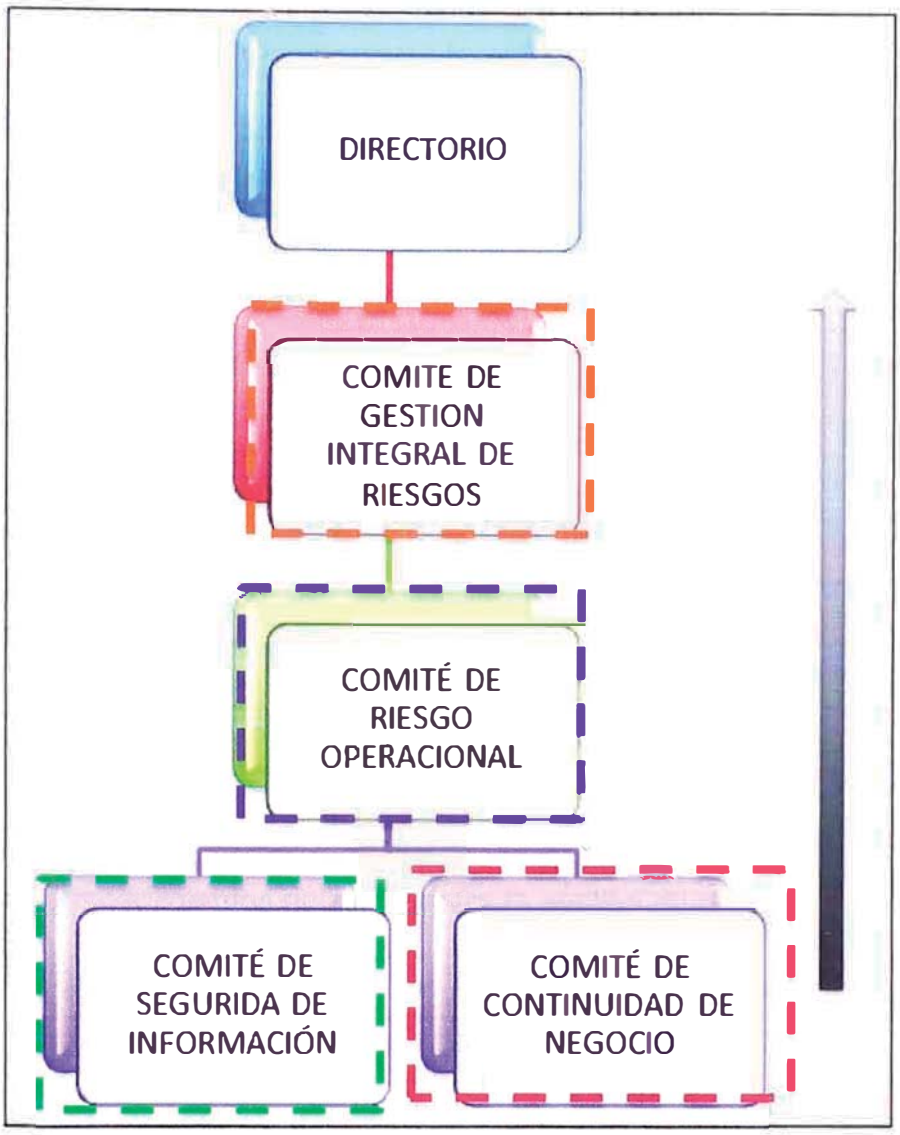
La empresa ha desarrollado todo un esquema de comunicación y toma de decisiones con respecto al riesgo operacional; generando un ambiente interno apropiado para la gestión de riesgo operacional; además se ha clarificado las responsabilidades de cada uno de los integrantes de la gestión de riesgo operacional; dicho sea de paso es todo el banco.

El área de riesgo operacional coordina y asisten a las demás áreas de la empresa en la aplicación de la metodología de riesgo; teniendo de manera clara una independencia respecto a las unidades de negocio, de apoyo así como de auditoría interna.

Es de suma importancia determinar los roles y responsabilidades de los comités y de las áreas a fin de mantener el sistema integrado de gestión de riesgos.

A continuación mostramos el esquema de los diferentes comités.

ESQUEMA N° 14: Comités creados para la Gestión de Riesgo Operacional



Fuente: Banco en estudio

Elaboración: Propia

Cada uno de los comités y personas integrantes del Sistema de Gestión de RO tienen sus responsabilidades claras en la organización; los comités y puestos integrantes son:

a) Directorio. Una de las principales funciones del directorio es que es 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.

b) Comité de Gestión Integral de Riesgos. La función de este comité es Obtener aseguramiento razonable de la implementación de administración de riesgos operacionales que resulte acorde a la dimensión y naturaleza de sus operaciones y servicios.

c) Comité de Riesgo Operacional. Asistir al Directorio y Comité de Gestión Integral de Riesgos en la responsabilidad de proveer un esquema de administración de riesgos operacionales y actuar como un canal de comunicación entre el Directorio y la Administración del Banco.

d) Comité de Continuidad de Negocios. Asegurar que la gestión que la continuidad de negocios que realice la empresa sea consistente con las políticas y procedimientos aplicados para la gestión de riesgos.

e) Comité de Seguridad de Información. Monitorear los resultados de la implementación de controles de seguridad de información, así como la toma de decisiones.

f) Gerencia General. Implementar la Gestión de Riesgo Operacional conforme a las disposiciones del Directorio y Comité de Gestión Integral Riesgos.

g) Gerencia de División de riesgos y recuperaciones. Informar al Comité de Gestión Integral de Riesgos el grado de exposición al riesgo, de acuerdo a las políticas y procedimientos establecidos.

h) Gerencia de Staff o primera línea. Implementar la Gestión de Riesgos conforme a las disposiciones del

Comité de Gestión Integral de Riesgos y la Gerencia General.

i) Gerencia de riesgo operacional. Implementar la gestión de riesgos operacionales conforme a las disposiciones del Directorio y el Comité de Gestión Integral de Riesgos.

j) Funcionario de Segunda línea (reportan a Gerentes de Staff) Garantizar el cumplimiento de las políticas, lineamientos y metodología de gestión de los riesgos operacionales para los productos bajo su responsabilidad.

k) Coordinador de Riesgo Operacional. Asistir a los Gerentes de línea en la gestión de los riesgos operacionales.

l) Auditoría Interna. Compartir información relativa a eventos de pérdida y otras situaciones de potencial riesgo operacional que sean de su conocimiento con la Gerencia de Riesgo Operacional.

m) Gerencia de División de Gestión de Proyectos y experiencia cliente. 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.

n) Gerencia de división de asesoría legal. Gestionar la implementación de políticas y procedimientos para prevenir el riesgo legal.

o) Gerencia de división de administración y finanzas. Informar los eventos de pérdida a la Gerencia de Riesgo Operativo relacionados con su función.

p) Gerencia de división de operaciones y tecnología. Informar los eventos de pérdida a la Gerencia de Riesgo Operativo relacionados con su función.

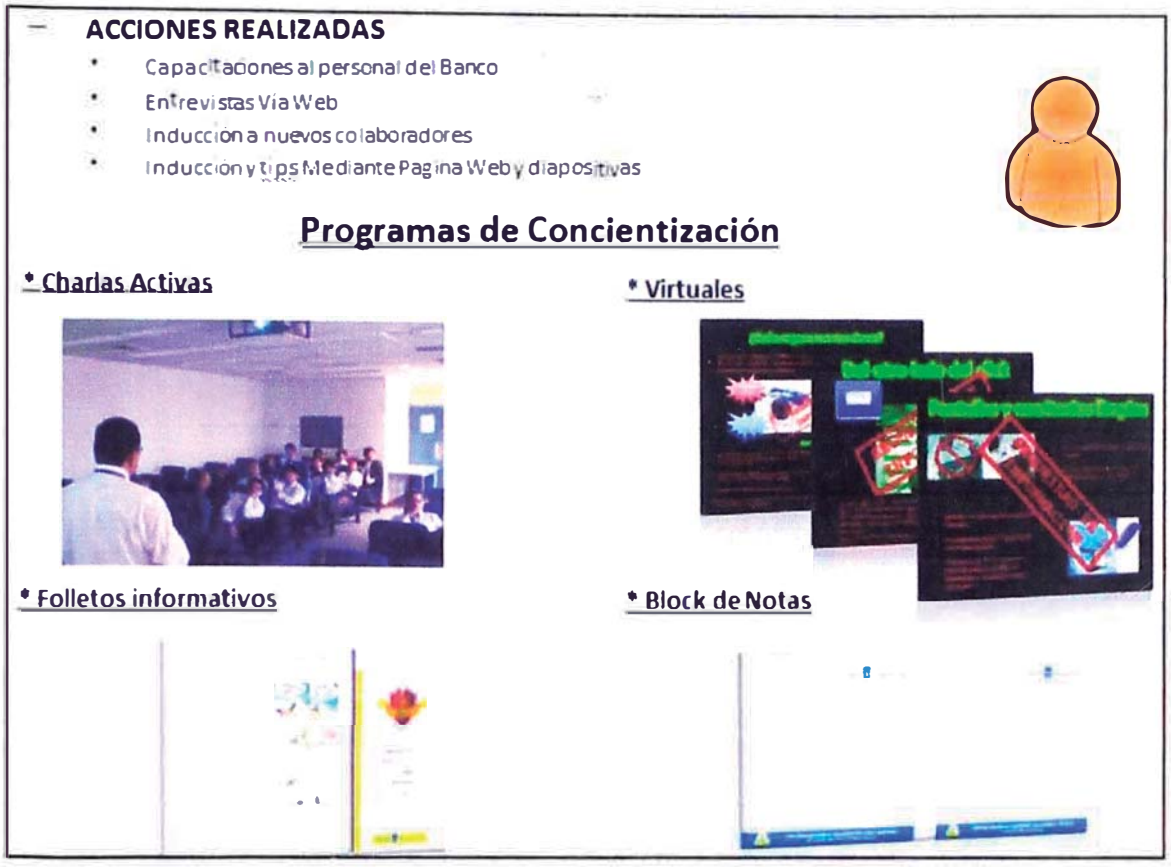
q) Colaboradores del Banco. Informar los riesgos y eventos de pérdida al Jefe inmediato y al Coordinador de Riesgo, quienes deberán reportarlo a la Gerencia de Riesgo Operacional

3.4.1.3. Programa de Capacitación al Personal

Para cumplir con este objetivo la empresa cuenta con un programa de capacitación profesional dirigido a perfeccionar los conocimientos, aptitudes y otras competencias de los colaboradores que pertenecen al área de Riesgo Operacional.

Otro programa de capacitaciones debe ser dirigido a las diferentes unidades o áreas identificadas por la unidad responsable para gestionar dichos riesgos.

ESQUEMA N° 15: Acciones sobre la Capacitación del Personal



Fuente: Propia

Elaboración: Propia

3.4.1.4. Metodología para la gestión de Riesgo Operacional

a) **Manuales de gestión de Riesgo Operacional.** La empresa ha implementado una metodología de documentación en la que el Manual de Riesgo Operacional es el documento que esboza y detalla todo el sistema de gestión de RO.

b) **Niveles de Apetito y tolerancia al riesgo operacional**. El Comité Gestión Integral de Riesgos seguirá el perfil de riesgos del banco, mediante la exposición acumulada al riesgo operacional y el nivel a pérdidas, teniendo en cuenta la complejidad y tamaño del banco, la evolución de las utilidades, gastos y requerimientos

patrimoniales a través de los límites establecidos en las políticas de apetito y tolerancia.

La política de apetito establece los límites específicos para tomar la decisión de aceptar la exposición a los riesgos operacionales por cada producto y línea de negocio del banco.

Las exposiciones al riesgo operacional se miden a través del riesgo residual de las matrices de autoevaluación de los riesgos y se monitorea el constante cumplimiento a través de la actualización del riesgo alcanzado.

El Comité de Gestión Integral de riesgos aprobará un límite general del apetito por riesgo operacional relacionado a las utilidades del ejercicio del año anterior del Banco, la mecánica de distribución en límites del apetito por riesgo operacional para cada uno de los productos y líneas de negocio y los límites resultantes.

La mecánica de distribución del apetito considera la importancia de las actividades de negocio y soporte para contribuir en la generación de la utilidad de la empresa. Por ello se distribuye en límites de forma proporcional al peso establecido en el proceso de priorización utilizado para los procesos, considerando un factor de ajuste en el peso de los procesos de soporte que por su naturaleza tienen una contribución indirecta en la utilidad.

La tolerancia al riesgo operacional, se mide a través de la valorización neta de recuperos para los eventos de pérdida operacional; para ello se considerando todos los efectos económicos del evento.

La tolerancia al riesgo operacional se manifiesta en la decisión de aceptar que los procesos permanezcan

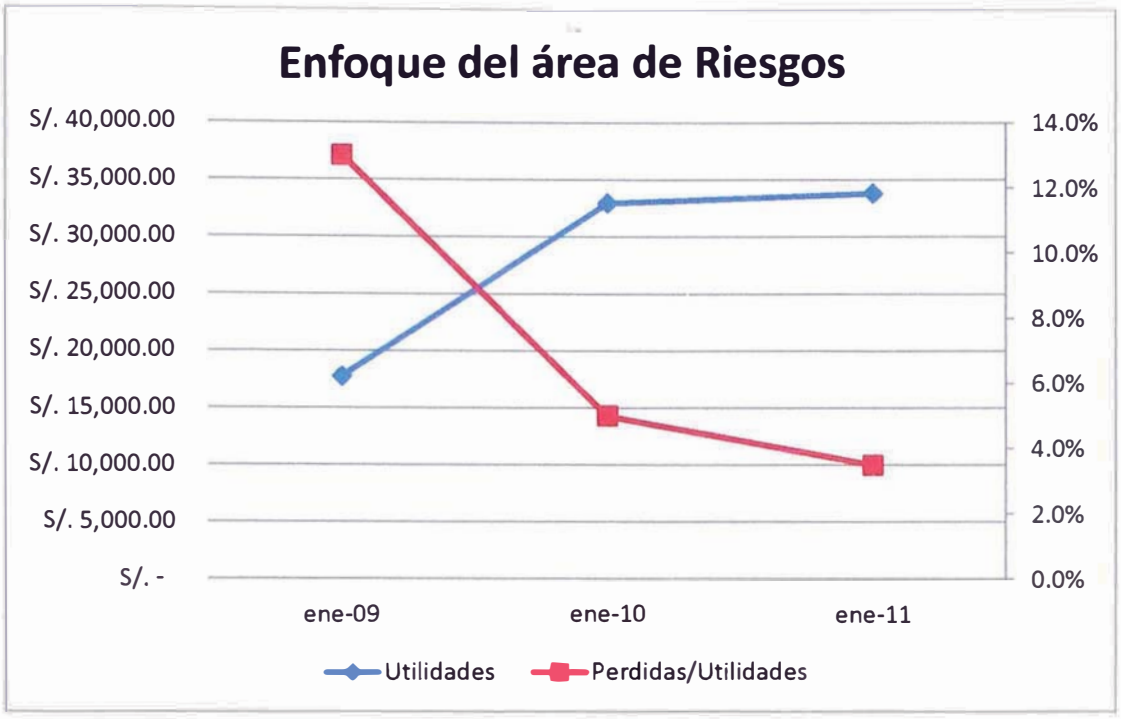
en la situación actual aunque se identifiquen eventos de pérdida operacional; sin necesidad de establecer acciones adicionales para mitigar futuras pérdidas consecuencia de dichos riesgos identificados durante el análisis y captura de eventos de pérdida. Se considera parte activa de la tolerancia la decisión de reducir la exposición mediante acciones de mitigación y establecimiento de los controles.

Las mejoras de procesos, controles, tecnología o acuerdos legales, cuyo fin sea reducir la posibilidad de pérdidas operacionales, consecuencia del análisis de los eventos de pérdida ocurridos en el banco, podrán ser solicitadas como medida preventiva por la Gerencia de Riesgo Operacional en función de la criticidad de las futuras pérdidas en caso se repitan los eventos.

Las decisiones de asumir los riesgos operacionales consecuencia de pérdidas donde el ejecutivo responsable no establezca medidas de mitigación, se sustenta en el informe de los casos de pérdida operacional neta cuyos valores sean mayores a S/.10,000 nuevos soles debidamente aprobado por la Gerencia de Riesgo Operacional.

El límite global de tolerancia anual al riesgo operacional es acumular pérdidas netas menores al 3.5% de la utilidad del año anterior o 350,000 dólares en caso las utilidades sean menores al ejercicio previó. En caso se superen los límites se deberán establecer planes de acción orientados a reforzar la mitigación de los casos de mayor cuantía.

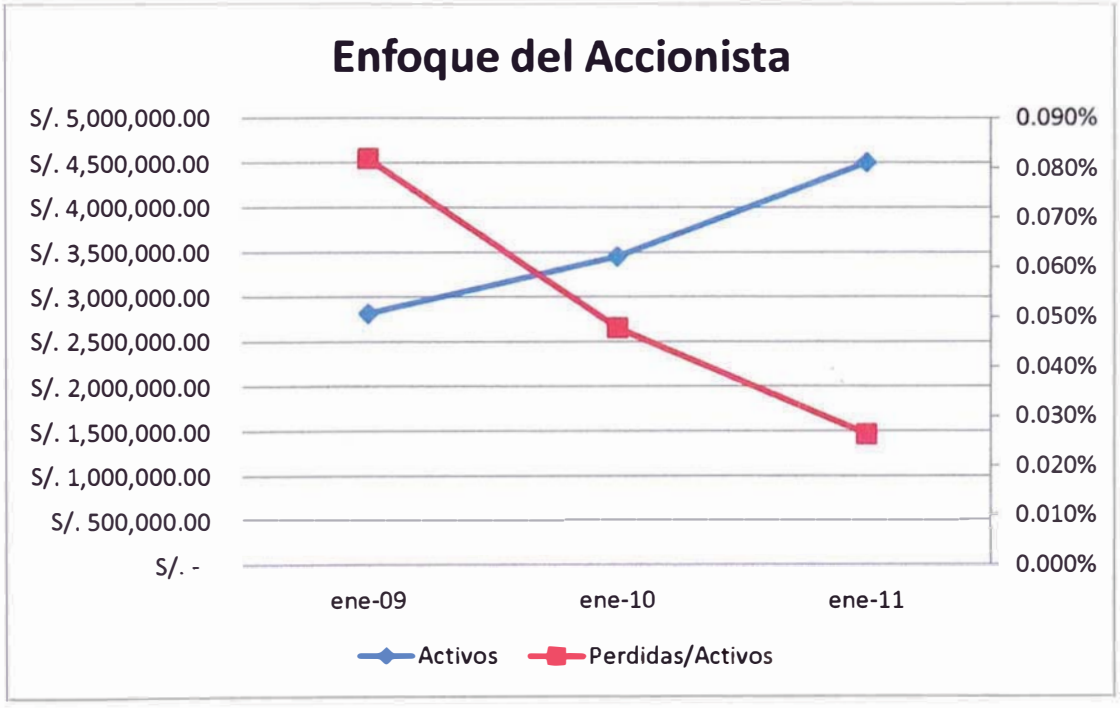
CUADRO N° 11: Enfoque del área de Riesgos



Fuente: Banco en estudio

Elaboración: Propia

CUADRO N° 12: Enfoque del Accionista



Fuente: Banco en estudio

Elaboración: Propia

c) Política de Priorización.

El Sistema de Gestión de Riesgos Operacionales de la Empresa tiene como objetivo identificar, cuantificar y mitigar los riesgos más significativos a los que se enfrenta, mientras realiza sus actividades de negocio. Consecuentemente, el BFP realizará la evaluación de los riesgos operacionales asociados a los todos los negocios (procesos vinculados a productos) de la Empresa, en función de su criticidad. Los procesos desarrollados para brindar dichos productos serán evaluados con una exhaustividad acorde a la criticidad de los mismos.

Los procesos realizados por el BFP se clasifican por su naturaleza en Estratégicos, Operativos del Negocio (Core), Control y Soporte. Sin embargo, por la naturaleza misma de los Procesos operativos del Negocio y de Soporte, son inherentemente expuestos a pérdidas operacionales; consecuentemente, la metodología de evaluación de los riesgos operacionales estará enfocada en éstos.

Se excluye de las evaluaciones, por política, a los procesos de control (dado que sus efectos podrán ser analizados en los procesos antes mencionados), y estratégicos, porque se relacionan a los riesgos estratégicos.

La mecánica para priorizar las líneas de negocio, negocios (productos) y sus procesos asociados a evaluarse, será aplicada por la Gerencia de Riesgo Operacional y el resultado aprobado por el Comité de Riesgo Operacional. Considerando los siguientes criterios:

CUADRO N° 13: Priorización de Procesos

Priorización de Productos	Priorización de Procesos
Volumen de Operaciones	Colaboradores que impacta el proceso
Impacto en los ingresos	Volumen de productos que soportan las actividades del proceso
Tamaño de Cartera de negocio	Severidad de Pérdidas económicas
Severidad de Pérdidas económicas	Administración de recursos

Fuente: Banco en estudio

Elaboración: Propia

El mecanismo para la implementación de estos criterios será desarrollado por la Gerencia de Riesgo Operacional. Asimismo, la periodicidad de la evaluación de estos productos será definido en función de la priorización establecida por la metodología de evaluación.

La Gerencia de División de Gestión de Proyectos y Experiencia a Clientes, es responsable de garantizar la vigencia del mapa de negocios y de los procesos asociados. Asimismo, también de informar a la Gestión de Riesgo Operacional sobre algún cambio, para su evaluación.

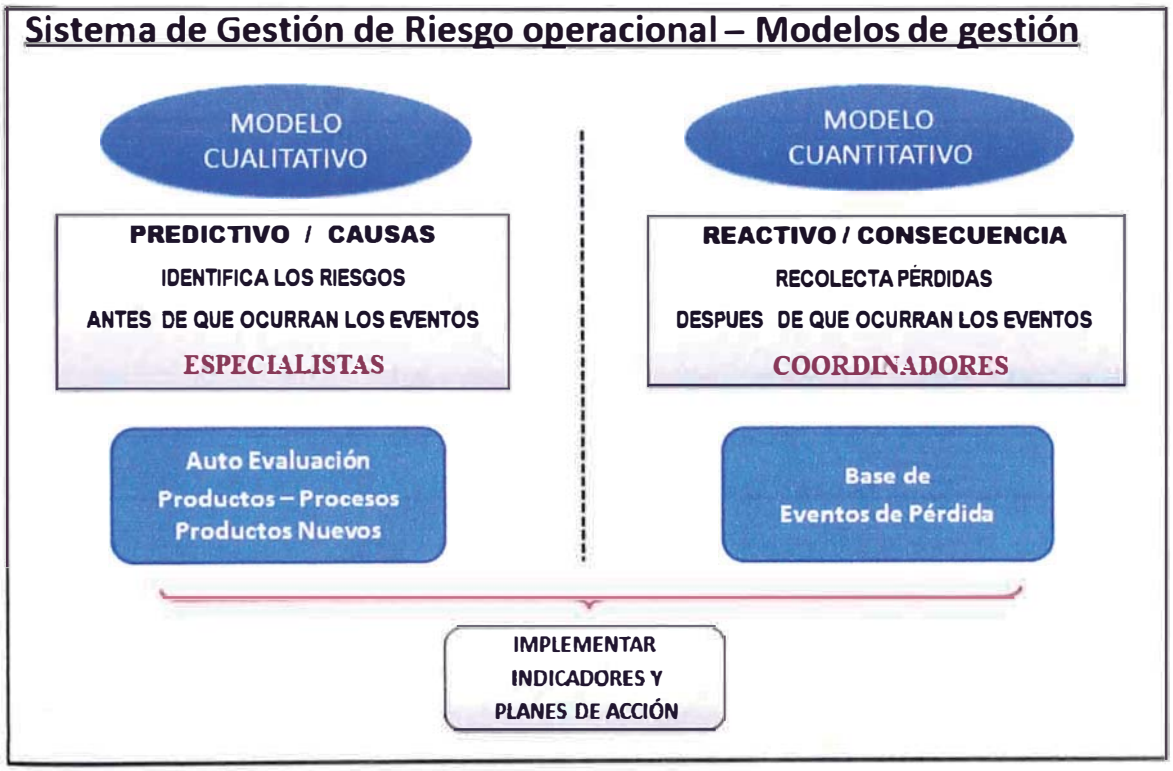
d) Autoevaluación de Riesgo Operacional

Antes de ingresar a detalles de la autoevaluación, el Banco utiliza dos modelos para gestionar los Riesgos

tomados del Estándar: El modelo Cualitativo y el cuantitativo. El primero es un modelo predictivo que se realiza mediante talleres autoevaluación el segundo es el modelo reactivo, que obtiene las consecuencias de que el riesgo se haya materializado.

Mostramos el siguiente gráfico para esquematizar mejor lo mencionado

ESQUEMA N° 16: Modelos utilizados en el Banco



Fuente: Estándar Australiana Neozelandés AS/NZS 4360-1999

Elaboración: Banco en estudio

A continuación detallamos las políticas de autoevaluación de riesgo operacional. La Gerencia de Riesgo Operacional realizará un seguimiento continuo al grado de avance de las autoevaluaciones programadas, desde su generación hasta su cierre, conforme a su plan de trabajo anual.

La autoevaluación de los riesgos operacionales está basada en la identificación previa de las debilidades a las que están expuestas los Productos y/o Procesos del Banco; en la determinación del impacto y la frecuencia y; en la evaluación de la efectividad de los controles.

Para la determinación de la efectividad de los controles, la Gerencia de Riesgo Operacional definirá los criterios para que las áreas responsables de ejecutar dichos controles evalúen su efectividad.

De igual manera, considera la identificación de alternativas para el tratamiento de los riesgos y el establecimiento de planes de acción para mitigación de los riesgos operacionales (transferir, disminuir la frecuencia y/o el impacto).

La metodología de autoevaluación se aplica mediante talleres con una dinámica de grupo, donde las áreas involucradas en el proceso con el apoyo de los coordinadores de riesgos, realizan las autoevaluaciones y, en donde la Gerencia de Riesgo Operacional cumple un rol de facilitador, asistiendo a las áreas del Banco en la identificación, evaluación, seguimiento y mitigación de los riesgos operacionales.

La Gestión de Riesgo Operacional registra la información correspondiente a las Matrices de Riesgos es soportada por el Sistema de Riesgo Operacional (OpRisk).

e) Recolección de eventos de pérdida

El Banco realiza seguimiento de las principales pérdidas por riesgo de operacional tanto por Línea de Negocio como por Tipos de Eventos y la administración de la información de los eventos de pérdida se

encuentra a cargo de la Gerencia de Riesgo Operacional.

Los Coordinadores de riesgo operacional de las Gerencias de División tienen el rol de nexo cuya principal función es apoyar en la captura de pérdidas por riesgo operacional para su incorporación en la base de datos central de pérdidas operacionales

Todo evento de pérdida informado al Coordinador de Riesgo, deberá ser reportado a través del buzón de RO mensualmente y registrado en el Sistema de Riesgo Operacional (OpRisk), con un plazo máximo de 15 días después de cerrado el Balance.

Los eventos que sean identificados por áreas de soporte que afecten a los productos y servicios, deberán ser reportados a los Coordinadores y la Gerencia de RO tan pronto se tome conocimiento. En caso no se pueda identificar las líneas afectadas por el evento de pérdida se comunicará directamente a la Gerencia de Riesgo Operacional.

El monto mínimo para el registro de eventos de pérdida es de S/. 0.01 nuevos soles o su equivalente.

Todo evento que pudiera generar una pérdida directa, deberá documentarse, inclusive en los casos en que el monto de la pérdida fuera recuperado en su totalidad.

Los eventos de pérdida operacional neta cuyos valores sean mayores a S/.10,000 nuevos soles, deberán ser documentados por la División responsable y además, en el Sistema de Gestión de Riesgo Operacional, en el cual deberá custodiar los expedientes.

La Gerencia de Riesgo Operacional es responsable de evaluar las fronteras de los eventos de pérdida por Riesgo Operacional, es decir, casos en los cuales las pérdidas operacionales traen como consecuencia o están asociadas a otros tipos riesgos como:

Pérdidas relacionadas a Riesgo de Crédito

Los eventos de pérdidas por riesgo de crédito y que tienen origen por causas catalogadas como riesgo operacional se incluirá en la base de datos de pérdidas de riesgo operacional para facilitar la gestión posterior con el fin de llevar a cabo acciones de mejora para minimizar el riesgo en el futuro. Estos eventos se marcarán en la base de datos como eventos relacionados a riesgo de crédito, para utilizar dicha información sólo para efectos de gestión y desestimarla a efectos de cálculo de capital regulatorio, y evitar así la duplicidad al estar cubierto por riesg de crédito.

Pérdidas relacionadas a Riesgo de Mercado

Las pérdidas de este tipo de riesgos originados por eventos definidos como riesgo operacional (Ej. aquellas pérdidas generadas en productos de mercado de capitales), también se han de incluir en la base de datos de pérdidas y marcarlos como eventos relacionados a riesgo de mercado.

Pérdidas relacionadas a Riesgo Legal

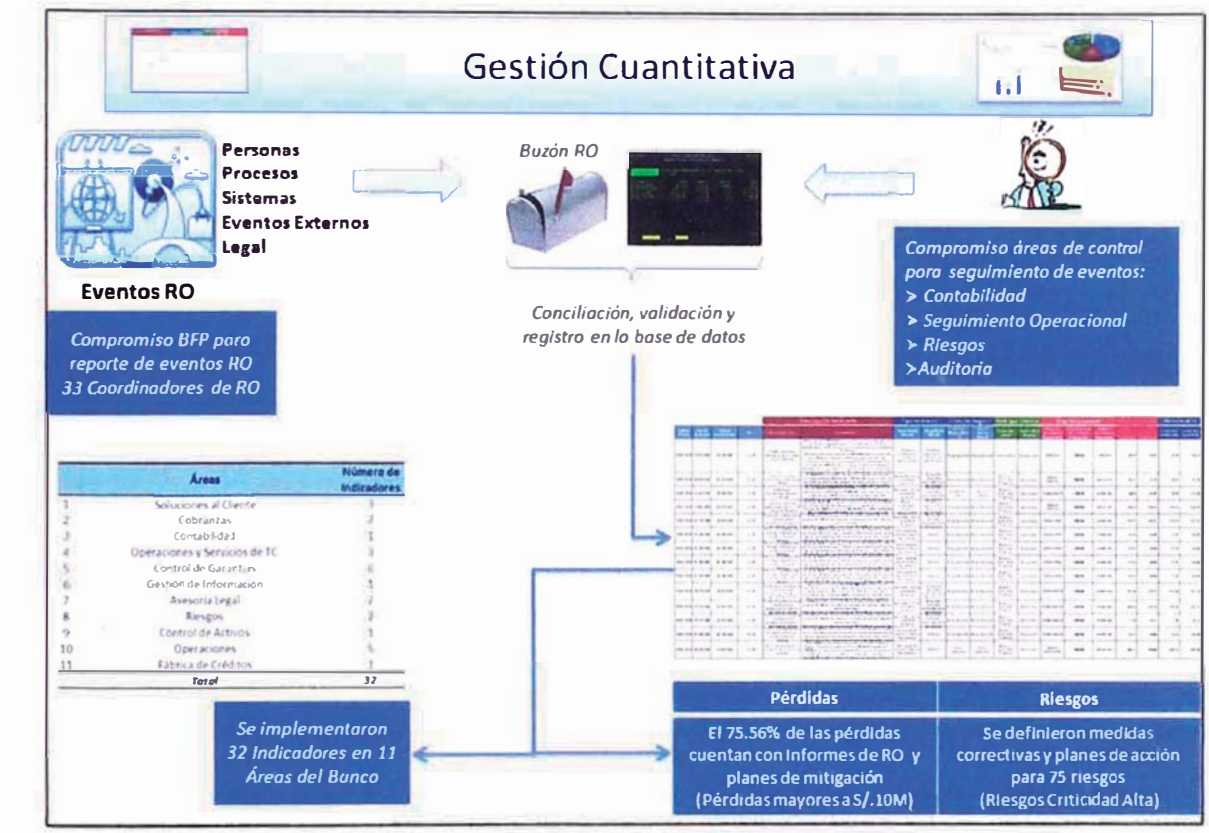
Se incluirán en la Base de datos, las pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros. Pero se excluye de la base de eventos de pérdidas por riesgo operacional:

Los gastos fijos previstos para atender los honorarios a profesionales con los que se haya suscrito un contrato de prestación de servicios permanente (Ej.: Asesoría Legal).

Todos los gastos en litigios por recuperación de créditos otorgados.

Pérdidas relacionadas a Riesgo Estratégico y de Negocio

ESQUEMA N° 17: Gestión Cuantitativa



Fuente: Banco En Estudio

Elaboración: Propia

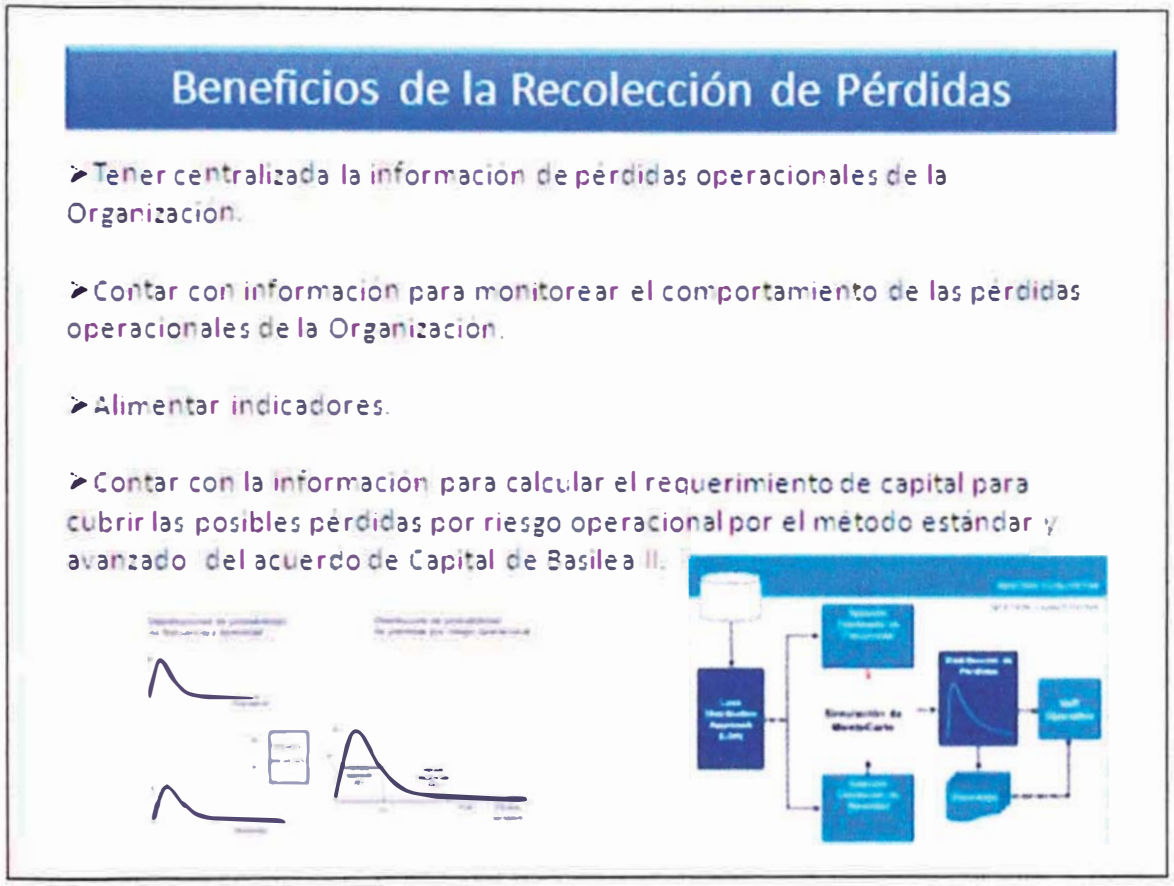
El Banco, actualmente no cuenta con la Base de Datos Suficiente para poder realizar análisis para determinar el Valor en Riesgo operacional (VaRop[13]);

[13] El *Valor en Riesgo* (VaR) es una medida del riesgo de tipo estadístico. Puede

sin embargo se realizan registros que en un futuro cercano (1 Año) servirán para establecer parámetros de medición.

A continuación se muestra los Beneficios de tener la recolección de la Base de Pérdidas

ESQUEMA N° 18: Beneficios de la Recolección de Pérdidas



Fuente: Banco en Estudio

Elaboración: Propia

---

utilizarse para estimar el riesgo de mercado de una cartera (o de una inversión) para la que no existe una serie histórica de precios, bien porque no se recogieron los datos o porque la composición de la cartera ha cambiado recientemente. La utilización del VaR se encuentra muy extendida entre las instituciones que necesitan medir el riesgo en carteras negociadas activamente. Concretando, el VaR de una cartera se define *como la máxima pérdida esperada debida a un movimiento adverso, dentro de un determinado intervalo de confianza ,a lo largo de un determinado horizonte temporal*

f) Análisis, Evaluación de Riesgo y medición de su efectividad

Para la evaluación y calificación de los riesgos, se han definido criterios, los cuales están en función de dos variables: frecuencia e impacto

Frecuencia: Está referida al número de veces en que puede materializarse el riesgo, en una ventana de 1 año. La frecuencia puede ser estimada bajo tres escenarios:

Inherente (sin controles)

Residual (con controles existentes)

Esperado (con planes de acción a futuro)

Impacto: Es la magnitud de la consecuencia si se materializa el riesgo, expresado en términos económicos.

Para la valoración de los riesgos operacionales, es decir, la determinación de su impacto en los resultados del Banco, se podrán estimar los valores potenciales que podrían producirse de materializarse el riesgo, a partir del expertise del dueño del Proceso / Producto y adicionalmente, se tomará como referencia la base de eventos de pérdida.

Calificación de la Probabilidad de Ocurrencia y del Impacto

El Banco ha definido 05 niveles de categorización, tanto para la probabilidad de ocurrencia, como para la severidad del impacto (en base a los rangos definidos para el apetito del riesgo).

Para calificar la probabilidad y el impacto de un riesgo, se deberá usar el cuadro de Criterios para la Evaluación de Riesgos y escoger el criterio más apropiado (tanto para la probabilidad como para el impacto); tomando siempre en cuenta el peor escenario (mayor calificación).

CUADRO N° 14: Niveles de Riesgo

MAPA DE CALIFICACIÓN DE RIESGOS						
		IMPACTO				
		Menos de US$ 3,000	Entre US$ 3,001 y US$ 10,000	Entre US$ 10,001 y US$ 20,000	Entre US$ 20,001 y US$ 50,000	Más de US$ 50,000
PROBABILIDAD	Muy Alta	Medio	Alto	Extremo	Extremo	Extremo
	Alta	Medio	Medio	Alto	Extremo	Extremo
	Media	Bajo	Medio	Medio	Alto	Extremo
	Baja	Bajo	Bajo	Medio	Medio	Alto
	Muy Baja	Bajo	Bajo	Bajo	Medio	Medio
		Muy Bajo	Bajo	Medio	Alto	Muy Alto

Fuente: Estándar Australiano Neozelandez AS/NZS 4160:2009

Elaboración: Propia

Determinación del Nivel de Riesgo

El Nivel de Riesgo es una medida cualitativa que permite categorizar el nivel de exposición que tiene una Institución frente a determinado riesgo, nivel que está dado por la combinación de las categorías de Impacto Monetario y la Probabilidad de Ocurrencia, en este sentido el Banco ha definido 4 Niveles:

CUADRO N° 15: Clasificación de Niveles de Riesgo

CALIFICACIÓN DEL NIVEL DE RIESGO		
PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
Muy Baja	Muy Bajo	Bajo
Muy Baja	Bajo	Bajo
Muy Baja	Medio	Bajo
Baja	Muy Bajo	Bajo
Baja	Bajo	Bajo
Media	Muy Bajo	Bajo
Muy Baja	Alto	Medio
Muy Baja	Muy alto	Medio
Baja	Medio	Medio
Baja	Alto	Medio
Media	Bajo	Medio
Media	Medio	Medio
Alta	Muy Bajo	Medio
Alta	Bajo	Medio
Muy Alta	Muy Bajo	Medio
Baja	Muy alto	Alto
Media	Alto	Alto
Media	Muy alto	Extremo
Alta	Medio	Alto
Alta	Alto	Extremo
Muy Alta	Bajo	Alto
Muy Alta	Medio	Extremo
Alta	Muy alto	Extremo
Muy Alta	Alto	Extremo
Muy Alta	Muy alto	Extremo

Fuente: Estándar Australiano Neozelandez AS/NZS 4160:2009

Elaboración: Propia

Efectividad de los controles existentes

Los riesgos operacionales identificados pueden tener asociados, a su vez, medidas de mitigación (controles), que permitan atenuar o reducir su impacto negativo.

La evaluación de la efectividad del control o controles, es determinada en función de los siguientes criterios:

Objetivo del control, se evalúa si el control implementado es correctivo (se toman acciones después de materializado el riesgo), detectivo (permite

reconocer la existencia del riesgo, previo a ejecutarse la actividad que lo genera), o preventivo (se identifica y se reduce la incidencia del riesgo).

Periodicidad del control, se evalúa la frecuencia con la que se realiza o ejecuta el control, por ejemplo si es con una periodicidad diaria, mensual, anual, etc.

Formalización del control, se evalúa si el control se encuentra debidamente formalizado o normado en un procedimiento o política y si existe evidencia alguna, cuando éste es ejecutado.

Automatización del control, se evalúa si el control implementado, es manual o automático.

g) **Tratamiento de los riesgos cuidando de relacionar metodológicamente al apetito y luego a los planes de acción.**

Los riesgos potenciales del producto o proceso, identificados en las etapas anteriores, pueden tener medidas de mitigación que permitan atenuar o trasladar su impacto negativo.

Se deberá seleccionar y aplicar una o más opciones de tratamiento para los riesgos identificados.

Entre estas opciones de tratamiento, tenemos:

Aceptar, no se realizan acciones de mitigación ni control sobre el mismo; asumiendo el nivel de probabilidad e impacto del riesgo.

Mitigar, se establece, planifica y ejecuta medidas (planes de acción), dirigidas a reducir o disminuir el nivel de probabilidad de ocurrencia y/o de impacto del riesgo.

Establecer un plan de acción, comprende definir el alcance para tratar los principales riesgos residuales identificados, así como el responsable de diseñar e implementar el plan de acción y establecer el plazo para ello.

Evitar, eliminar o rediseñar las actividades o procesos, que dan origen a situaciones de riesgo.

Transferir, se transfiere a un tercero (Proveedor/ Seguro), la obligación por las consecuencias que puede originar el riesgo.

En ninguno de los casos, el riesgo puede eliminarse, necesariamente se deberá aplicar una o más de las opciones de tratamiento, anteriormente mencionadas.

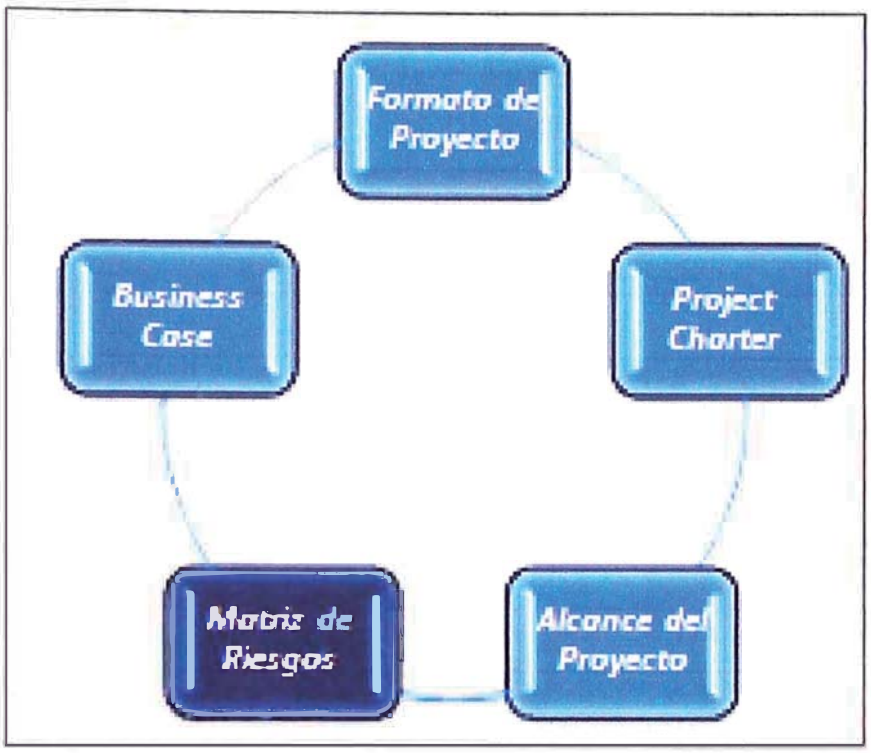
h) Evaluación de Riesgos Operacionales previo al Lanzamiento de Nuevos Productos y ante cambios en el Ambiente Operativo e Informático

La evaluación de riesgos operacionales previa al lanzamiento de nuevos productos o ante cambios importantes a nivel operativo e informático se encuentra alineada a los procesos de Autoevaluación que se realizan para los principales productos y procesos del Banco. La principal característica de este tipo de evaluación es el carácter preventivo que busca asegurar niveles óptimos de apetito y tolerancia al riesgo operacional para el Banco.

El banco realiza un monitoreo de los principales cambios que se generen dentro de la organización a través del flujo de control y aprobación de nuevas iniciativas establecido por la Gerencia de Planeamiento y Calidad . La Gerencia de Riesgo Operacional participa de manera activa en la identificación de riesgo y

validación de planes de acción que permitan mitigar los riesgos identificados

ESQUEMA N° 19: Evaluación previo al lanzamiento



Fuente: Banco en Estudio

Elaboración: Propia

3.4.1.5. Recursos Suficientes

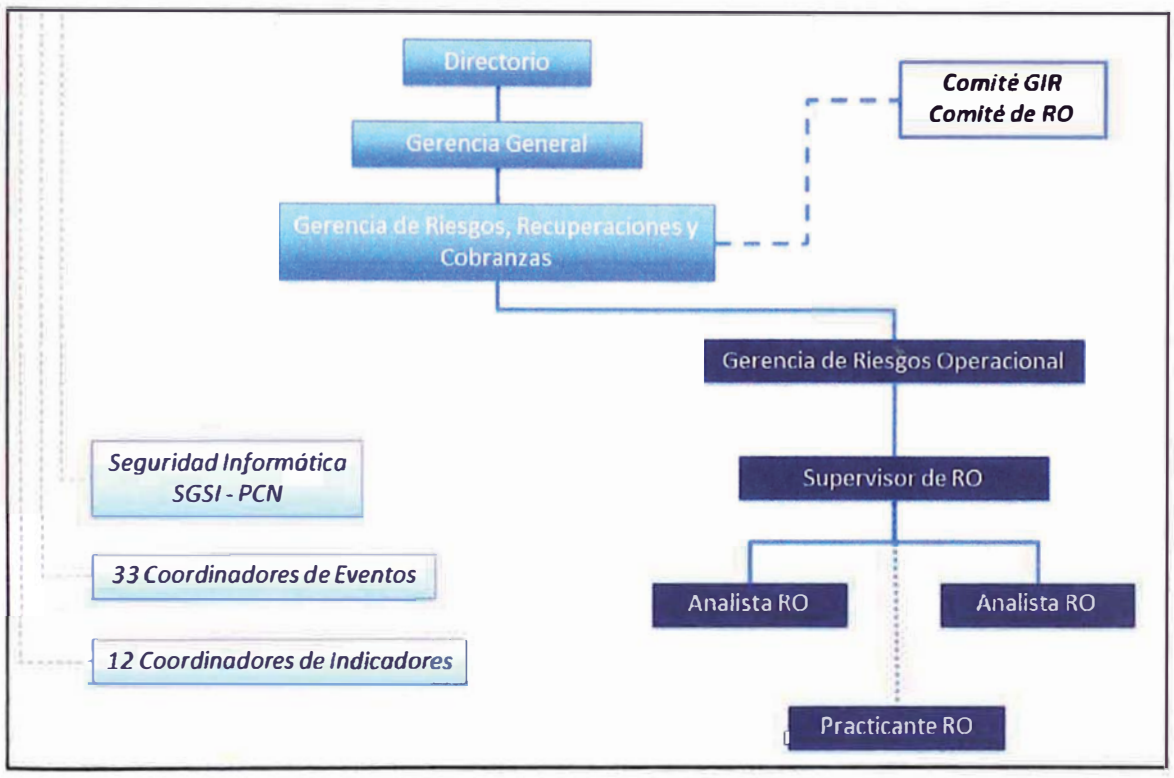
Al hablar de recursos suficientes, en primer lugar se habla del área de Riesgo operacional que existe en el Banco, el cual está conformado por un Gerente de Riesgo operacional, un Supervisor de Riesgo Operacional, 2 analistas de riesgo operacional y 1 practicante de Riesgo Operacional, los cuales han venido laborando para poder cumplir con las exigencias.

Por otro lado, el equipo de riesgo operacional se debe soportar por sistemas informáticos los cuales apoyan a toda la gestión de riesgo operacional; en este caso la empresa ha decidido comprar la licencia de un software de Riesgo Operacional que es utilizado por la Casa Matriz;

esto permite una transferencia de conocimiento rápida y eficiente.

El riesgo operacional no funciona si es centralizado, una estrategia tomada por el área de riesgo operacional es descentralizar la gestión de riesgo mediante COORDINADORES DE RIESGO, los cuales se encuentran en las áreas de negocio y de apoyo. Esto permite poder percibir una retroalimentación al momento de realizar las evaluaciones.

ESQUEMA N° 20: Organigrama de Riesgo operacional



Fuente: Banco en Estudio

Elaboración: Propia

3.4.1.6. Remisión de información periódica a interesados internos e externos

El Comité de Gestión Integral de Riesgos es responsable de aprobar los objetivos y estructura mínima de los reportes a generarse y comunicarse como parte del Sistema de Gestión de los Riesgos Operacionales. Los

mismos deberán ser validados por el Directorio del BANCO. Asimismo, el Comité RO y la Gerencia de Riesgo Operacional son responsables de proponer y desarrollar, respectivamente, la implementación y los cambios de dichas políticas a través de las metodologías apropiadas.

3.4.1.7. Procedimientos para asegurar cumplimiento de metodología para gestión del riesgo operacional

El grado de nivel de cumplimiento es evaluado periódicamente conforme a los criterios de la mecánica de Indicadores de evaluación utilizados para el esquema de Incentivos de la Gerencia de Primera Línea

Los casos de incumplimiento de las políticas del presente manual serán informados por la Gerencia de Riesgo Operacional al Comité de Gestión Integral de Riesgos, mismo que tomará las acciones pertinentes.

3.4.1.8. Incentivos para mejorar la gestión de riesgo operacional

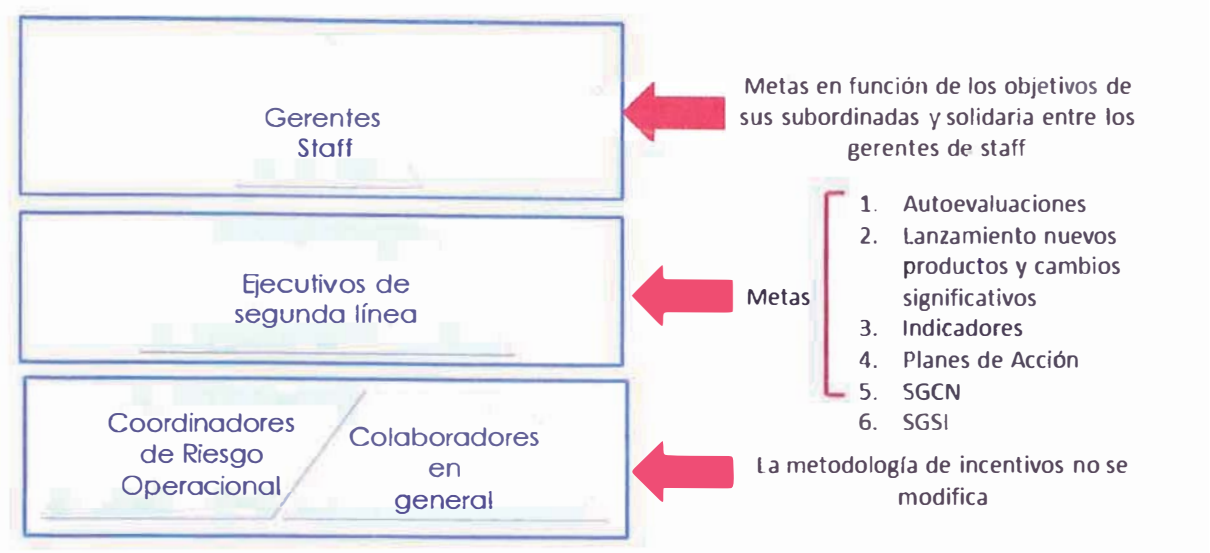
Como parte de un sistema eficiente de gestión del riesgo operacional, el Banco ha creado un programa de incentivos que tiene como objetivo el promover la eficiencia de la gestión del riesgo operacional.

El programa de incentivos está dirigido a todo el personal de la empresa y estará dividido en dos segmentos:

Gerentes de primera

Coordinadores de riesgo operacional y Colaboradores en general.

ESQUEMA N° 11,9: Política de Incentivos



Fuente: Banco en Estudio

Elaboración: Banco en Estudio

3.4.1.9. Gestión de la base de datos de pérdida de eventos de pérdida por riesgo operacional

El Banco realiza seguimiento de las principales pérdidas por riesgo de operacional tanto por Línea de Negocio como por Tipos de Eventos y la administración de la información de los eventos de pérdida se encuentra a cargo de la Gerencia de Riesgo Operacional.

Los Coordinadores de riesgo operacional de las Gerencias de División tienen el rol de nexo cuya principal función es apoyar en la captura de pérdidas por riesgo operacional para su incorporación en la base de datos central de pérdidas operacionales

Todo evento de pérdida informado al Coordinador de Riesgo, deberá ser reportado a través del buzón de RO mensualmente y registrado en el Sistema de Riesgo Operacional (OpRisk), con un plazo máximo de 15 días después de cerrado el Balance.

Las bases de datos de pérdidas son conciliadas periódicamente de forma contable y presentaciones en el

comité Integral de Riesgos. En esta base de eventos de pérdida se identifican y se evalúan nuevos riesgos como resultado de dicho análisis.

CUADRO N° 16: Eventos de Pérdidas por Riesgo Operacional

EVENTOS DE RIESGO OPERACIONAL		TIPOS DE EVENTOS						
		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	Finanzas Corporativas							
	Negociación y Ventas							
	Banca Minorista	UDS 150,167 8 Eventos	USD 196,428 126 Eventos	USD 3,283 3 Eventos	USD 84,935 106 Eventos	USD 1,694 1 Evento	USD 2,975 106 Eventos	USD 97,887 118 Eventos
	Banca Comercial		USD 6,494 2 eventos		USD 5,000 1 Evento			USD 271,307 11 Eventos
	Liquidación y Pagos		USD 3,737 2 Eventos		USD 21,750 1 Evento		USD 75,352 38 Eventos	USD 98,325 39 Eventos
	Otros Servicios							USD 5,290 3 Eventos
	Múltiples Líneas de Negocio			USD 2,674 2 Eventos				USD 28,695 49 Eventos

Fuente: Banco en Estudio

Elaboración: Propia

3.4.1.10. Revisión periódica independiente de la gestión de riesgo operacional por parte de Auditoría Interna

El Auditor del Banco garantizará la evaluación independiente, al menos cada tres años de la gestión del riesgo operacional,

3.4.1.11. Revisión periódica independiente de la gestión del riesgo operacional por parte de una sociedad de Auditoría Externa.

El banco deberá contratar auditorías externas por parte de una Sociedad de Auditoría Externa o Empresa Consultora Especializada seleccionada por el Comité de Auditoría.

3.4.2. Implementación del Sistema de Gestión de Seguridad de Información

El objetivo del Sistema de Gestión de Seguridad de Información es salvaguardar los activos de información cuidando la integridad, disponibilidad y confidencialidad de la información, para esto se definió el alcance del sistema de Gestión de Seguridad de Información.

3.4.2.1. Política y Organización del SGSI

El Banco es una institución orientada a mantener una posición de vanguardia en el sector de negocios y perfeccionarse con relación a sus competidores en la adopción de tendencias globales que permitan un sistema de gestión de la continuidad del negocio adecuada a su tamaño y a la complejidad de sus operaciones.

En concordancia con su misión y visión el Banco ha decidido la implementación de un sistema de gestión de seguridad de información orientado a que la organización pueda implementar medidas para reducir la exposición a la fuga de información, prevenir el fraude informático, gestionar y reducir progresivamente los incidentes de Seguridad de Información en los activos de información considerados en el alcance del sistema, a fin de alcanzar el cumplimiento de las regulaciones aplicables para el BFP.

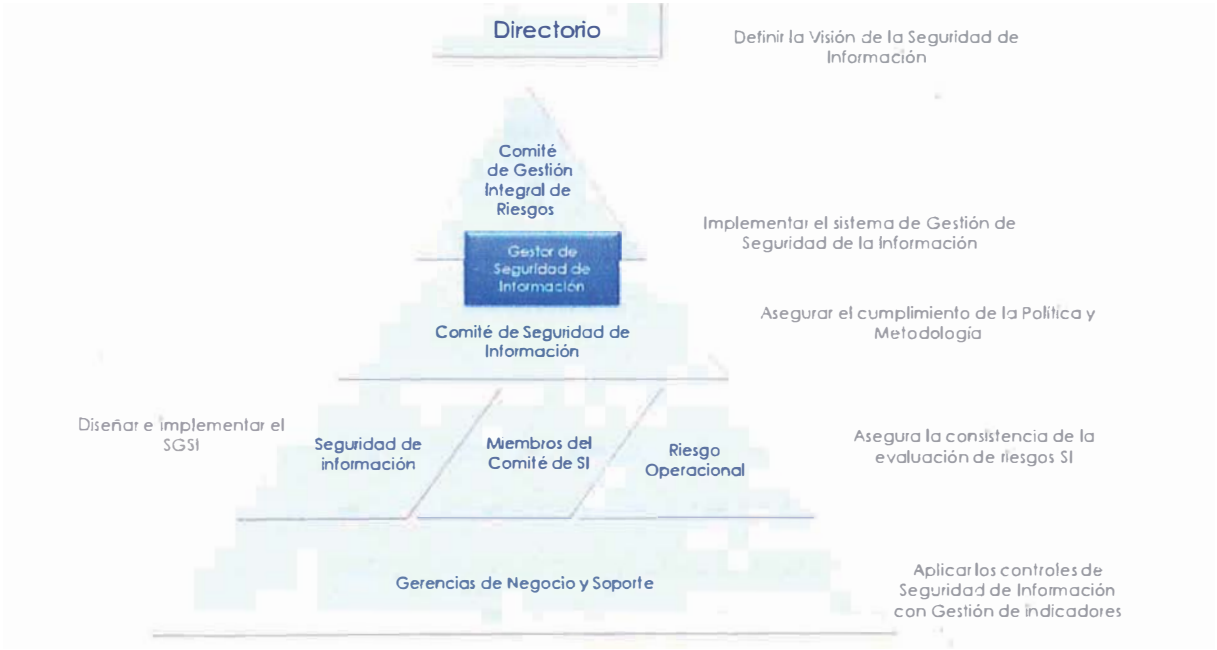
Los objetivos generales de la política son: Asegurar el cumplimiento de la política y metodología a nivel institucional; asegurar la razonabilidad de los controles implementados sea coherente con la estructura de la tecnología de información y riesgos de seguridad de información del banco; asegurar el cumplimiento regulatorio dentro del alcance del sistema de gestión de Seguridad de Información.

El alcance del Sistema de Gestión de Seguridad de Información se enfoca a los activos de información con información sensible que se soportan en medios físicos y/o magnéticos, establecida en base a los procesos de clasificación de información para las áreas de negocios y áreas de Apoyo del Banco.

La organización del sistema de gestión de seguridad de información ha sido definida estableciendo las diferentes responsabilidades de los involucrados, los cuales permiten una implementación eficiente del sistema a lo largo de toda la organización.

A continuación se presentan las responsabilidades de la gestión de Seguridad de la Información.

ESQUEMA N° 21: Organización del SGSI



Fuente: Banco en estudio

Elaboración: Banco En estudio

3.4.2.2. Mecánica Operativa del Sistema de gestión de seguridad de Información

El modelo de Gestión de Seguridad de información resalta la necesidad de establecer un proceso continuo que permita que las políticas, lineamientos y estrategias definidos estén alineados a los objetivos de negocios del Banco. En el siguiente gráfico muestra los componentes de dicho modelo y su interrelación:

ESQUEMA N° 22: Mecánica Operativa del SGSI

Fuente: Banco en estudio

Elaboración: Propiao

Con el objetivo de lograr una administración de seguridad eficaz y eficiente se deben tomar en cuenta tres aspectos importantes que forman la base de la arquitectura de seguridad implementada. Ellos son la estructura organizacional de la Gestión de la Seguridad de Información, el programa de concientización del personal en temas relacionados a Seguridad de Información, el compromiso y apoyo de la alta gerencia:

- **Estructura Organizacional para la Gestión de la Seguridad de información**

El establecimiento de una estructura organizacional para la Gestión de la Seguridad de Información, permite articular los esfuerzos relacionados con la Gestión de la Seguridad de Información en el Banco, así como el desarrollo de un Gobierno de la Seguridad de Información entre el Banco y sus empresas clientes a fin de lograr una exitosa implementación de todos los componentes de la Gestión de la Seguridad de Información.

Para la implementación del SGSI en el Banco, se ha implementado un Sistema para poder soportar toda la implementación: MODULO RISK MANAGER

- **Programa de Concientización**

Consiste en asegurar que todos los niveles de la organización estén conscientes de la importancia y la necesidad de una Gestión de la Seguridad de Información como forma de garantizar el logro de los objetivos del negocio.

La toma de conciencia es un componente clave para identificar y tomar las acciones adecuadas para mitigar los riesgos de Seguridad de Información. Un entrenamiento continuo del personal y la adecuada divulgación de las amenazas a las que están expuestos los procesos de negocios, son componentes esenciales de las medidas de mitigación de los riesgos.

Es responsabilidad de la Jefatura de Seguridad de Información concientizar y proporcionar entrenamiento al personal a su cargo para crear las competencias necesarias para la Gestión de la Seguridad de Información.

- **Compromiso de la Alta Gerencia**

El éxito de cualquier programa de Gestión de la Seguridad de Información depende del apoyo de la Alta

Gerencia, el cual establece la estrategia, prioridades y dotación de recursos humanos, financieros y logísticos necesarios para este proceso.

3.4.2.3. Gestión de Servicios Externos

Para la gestión de Servicios externos, el Banco hizo el análisis de todos los proveedores que cuenta el banco así como se realizaron visitas los cuales apoyan a realizar la gestión de Servicios externos, saber qué información ingresa al banco y que información sale del banco, que información es más crítica. Esto a su vez se coloca en el software de manera de registro.

Para esto se implementan las siguientes Normas que permiten un cumplimiento de estos controles.

Normas
Norma de Gestión de Servicios Externos

3.4.2.4. Gestión de Activos

La Clasificación y Control de los activos de información del banco tiene el fin de Asegurar su protección adecuada y contribuir con la gestión de riesgos mediante el control de los activos de la organización, así mismo el inventario de activos contribuirá efectivamente en la gestión de riesgos.

Para cumplir con este punto se realizan una serie de inventarios los cuales deben reflejar los activos de información que cuenta el Banco.

Para esto se implementan las siguientes Normas que permiten un cumplimiento de estos controles.

Normas
Norma de Clasificación y Control de Activos

3.4.2.5. Seguridad del Personal

El presente documento tiene como finalidad orientar, normar y controlar la ejecución y desarrollo de los procesos de inicio, mantenimiento y término de la relación laboral, llevados a cabo por el personal del departamento de Recursos Humanos.

Para esto se implementan las siguientes Normas que permiten un cumplimiento de estos controles.

Normas
Norma del Módulo de Administración de Recursos Humanos
Norma de Reclutamiento y Selección del Banco

3.4.2.6. Seguridad Física y Ambiental

El documento tiene como objetivo minimizar los riesgos potenciales creados por amenazas accidentales y/o deliberadas (ataque, pérdida, robo o daño a los sistemas de información), a los que se encuentran expuestos los recursos informáticos físicos, que puedan ocasionar la interrupción total o parcial de las actividades del negocio, a través de la definición de controles, procedimientos y/o mecanismos que permitan una máxima protección a un

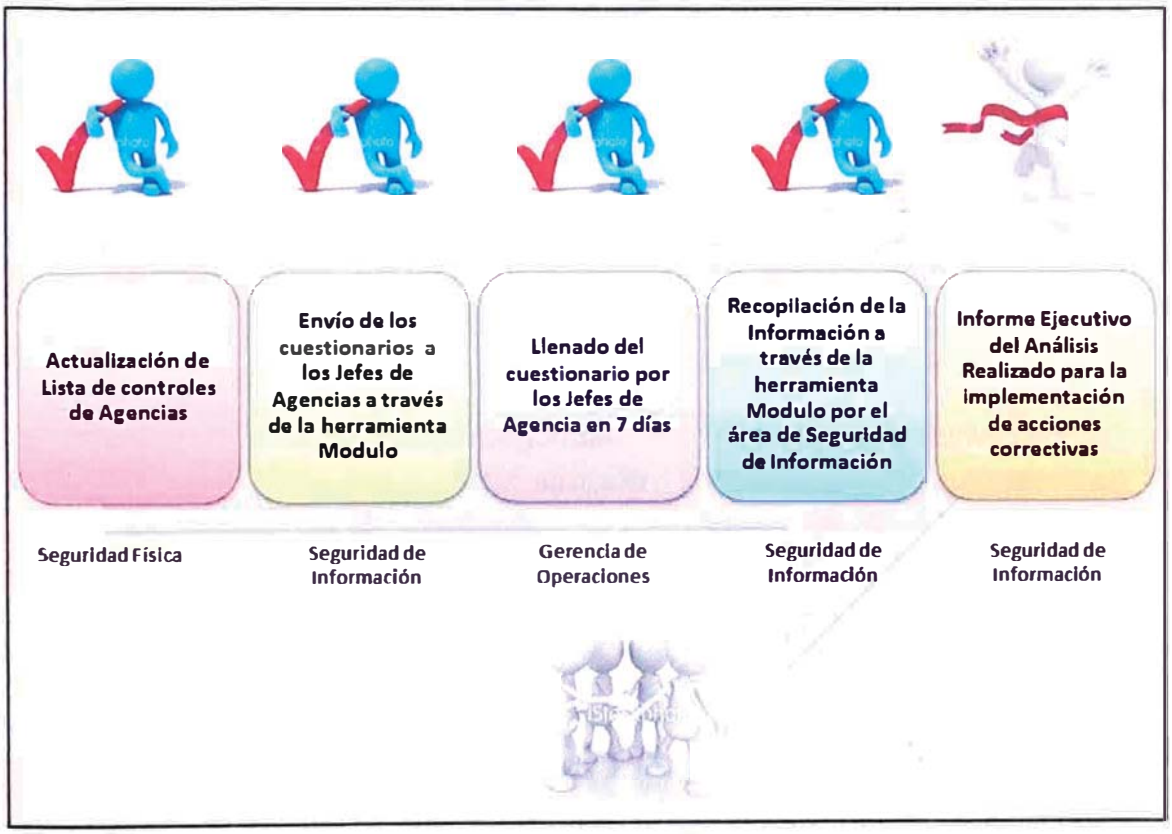
costo razonable. Además de evitar accesos no autorizados, daños e interferencias contra los locales y la información de la Organización.

Otro documento proporciona lineamientos donde se establecen medidas de seguridad en el ingreso a las áreas restringidas de Tecnología, definiendo al personal autorizado y las excepciones del caso.

Para esto se implementan las siguientes Normas que permiten un cumplimiento de estos controles.

Normas
Norma de Seguridad Fìsica y Ambiental
Norma de Acceso a Areas Restringidas de Tecnología
Control de Ingreso y Salida del personal-Operadores Centro Proc.de Datos
Norma de Seguridad de Control de Claves y Llaves en Oficinas

ESQUEMA N° 23: Proceso de Monitoreo de Gestión de Riesgo de Seguridad física en Agencias



Fuente: Banco en estudio

Elaboración: Propia

3.4.2.7. Seguridad de las Operaciones y Comunicaciones

El objetivo del presente documento es proporcionar los lineamientos para asegurar una operación correcta y segura de los recursos de tratamiento de información. Así mismo, establecer procedimientos y responsabilidades para la gestión y operación de todos los recursos del tratamiento de información, esto incluye desarrollo de instrucciones apropiadas de operación y procedimiento de respuestas ante incidencias.

Para mayor referencia se tienen los siguientes documentos en el siguiente Link publicado en el Portal de Normas y Procedimientos de la Organización

Normas	Procedimiento de Control
Norma de Procedimientos y Responsabilidades Operativas	**Procedimiento Operacionales y Responsabilidades Operativas** Procedimiento de Instalación del sistema de cajas en Oficinas del BFP
Norma de Seguridad para la Administración y Monitoreo de Servidores	Procedimiento de Monitoreo de actividad no autorizada en Bases de datos y Servidores del BFP
Norma de Gestión de Servicios Externos	**Procedimiento de controles de servicios a terceros**
Norma de Análisis de Necesidades del Sistema	**Procedimiento de Planeamiento y Disponibilidad de Infraestructura de TI**
Norma de Protección contra Código Malicioso	Procedimiento de monitoreo del funcionamiento de la Red Perimetral

	Procedimiento de Código malicioso
Norma de Instalación de Código Móvil	**Procedimiento de Seguridad de Medios Removibles**
Norma de Respaldo y Recuperación de Información Crítica	**Procedimiento de Copias de Respaldo** Procedimiento de Copia de Respaldo y Destrucción de Información
Norma de Seguridad de Redes	Procedimiento de monitoreo del funcionamiento de la Red Perimetral
Norma de Seguridad para el Firewall	Procedimiento de monitoreo del funcionamiento de la Red Perimetral
Norma de Manejo de Medios de Almacenamiento	**Procedimiento de Seguridad de Medios Removibles** **Norma de Uso Aceptable de Recursos.**
Norma de Acceso Remoto	Procedimiento para el Aseguramiento de los Procesos Batch
Norma de Intercambio de Información	**Procedimiento de Controles de Seguridad de Intercambio de Información**
Norma de Comercio Electrónico	NO APLICA
Norma de Monitorización y Seguimiento	**Procedimiento de Monitoreo de las Actividades de Procesamiento de Información**
Norma de Administración del Sistema	
Norma de	

Sincronización de Relojes	
Norma de Registro de Errores	

3.4.2.8. Norma de Control de Accesos

El objetivo del presente documento es establecer los lineamientos para controlar los accesos a la información, medios de procesamiento y procesos del Banco basándose en los requerimientos de seguridad y de negocio de la Organización.

Para mayor referencia se tienen los siguientes documentos en el siguiente Link publicado en el Portal de Normas y Procedimientos de la Organización

Normas	Procedimiento de Control
Norma de Control de Accesos	
Norma de Gestión de Acceso de Usuarios	**Procedimiento de revisión periódica de accesos**
Norma de Responsabilidades de Usuario	
Norma de Control de Acceso a la Red	Procedimiento de Solicitud y Atención de Requerimiento de Perfil de Usuarios
Norma de Control de Acceso a las Aplicaciones e Información	Procedimiento de Solicitud y Atención de Requerimiento de Perfil de Usuarios Requerimiento de Perfil de usuarios -Uso de Colaboradores Finales Autorizados Requerimiento de Perfil de usuarios - Uso de Gerentes y-

	o Jefes Aprobadores Instructivo Requerimiento de Perfil de usuario – Uso de Seguridad de Información Instructivo Requerimiento de Perfil de usuario - Accesos Business Intelligence y otros Instructivo para Compartir Carpetas de usuario en Estaciones de Trabajo del BFP
Norma de Información Móvil y de Teletrabajo	**Instructivo de Acceso a la VPN con Token** **Informe de Acceso a la VPN con Token**

3.4.2.9. Seguridad en la adquisición y Desarrollo de Software

El objetivo del presente documento es establecer los lineamientos necesarios para la protección del equipamiento Hardware de amenazas o uso mal intencionado de ella y para la protección del uso indebido o no autorizado del Software.

El objetivo del presente documento es fijar los lineamientos para minimizar los riesgos operativos inherentes al proceso de Gestión de Proyectos Informáticos.

Para mayor referencia se tienen los siguientes documentos en el siguiente Link publicado en el Portal de Normas y Procedimientos de la Organización

Normas	Procedimiento de Control
Norma de Seguridad de los Sistemas	Procedimiento de Pase a Producción
Norma de Instalación y actualización de	

Software - Sistemas operativos - Parches	
Norma de Desarrollo de Sistemas	**Procedimiento de Requisitos Seguridad de SI** Metodología de Desarrollo de Software
Norma de Seguridad de las Aplicaciones del Sistema	**Procedimiento Protección de Datos Prueba**
Norma de Controles Criptográficos	
Norma de Seguridad de los Archivos del Sistema	**Procedimiento Proteccion de Datos Prueba**
Norma de Control de Versiones	
Norma de Seguridad para la Fuga de Información	
Norma de Desarrollo de Software por Terceros	
Norma de Gestión de la Vulnerabilidad Técnica	**Procedimientos de Controles Gestion de Vulnerabilidades Tecnicas**

3.4.2.10. Gestión de Incidentes

El documento establece los lineamientos para asegurar que los eventos y vulnerabilidades (debilidades) en la Seguridad de Información sean comunicados de manera oportuna bajo procedimientos formales y responsables asignados, para permitir una acción correctiva a tiempo, donde la organización pueda aprender de los incidentes y estar lista para la recolección de evidencias.

Para mayor referencia se tienen los siguientes documentos en el siguiente Link publicado en el Portal de Normas y Procedimientos de la Organización

Normas	Procedimiento de Control
Norma de Gestión de Incidentes de la Seguridad de Información	**Procedimiento de Gestión de Incidencias(ITIL)**

3.4.2.11. Gestión de Cumplimiento

El documento establece los lineamientos para asegurar el cumplimiento de los requerimientos legales, las políticas, estándares, aspectos técnicos de la seguridad y las consideraciones de la auditoría de sistemas de información.

Evitar incumplimientos de cualquier ley, estatuto, obligación reguladora o contractual y de cualquier requerimiento de Seguridad; así como asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional, además de maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema de información.

Para mayor referencia se tienen los siguientes documentos en el siguiente Link publicado en el Portal de Normas y Procedimientos de la Organización

Normas
Norma de Cumplimiento

3.4.2.12. Gestión de Riesgos de Seguridad de Información

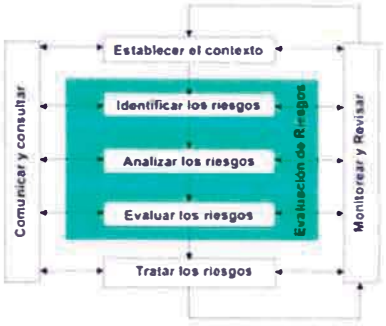
Para la Gestión de Riesgos se ha implementado un software: Modulo Risk Management; el cual tiene una

metodología de Gestión de Riesgos que se basa en el Estándar australiano Neozelandés AS/NZS 4360:2009; el cual tiene las siguientes Fases.

ESQUEMA N° 24: Procesos de Gestión de Riesgo de Seguridad de Información

AS/NZS 4360 : 2005 – Proceso de Gestión de Riesgos

- Busca equilibrar las oportunidades de ganancias y reducción de pérdidas.



Modulo Risk Manager : Fases de Análisis de Riesgo

* Tabla de Comparación

Framework Risk Manager	AS/NZS 4360 : 2005
Inventariar	. Establecer Contexto
Analizar	. Analizar Riesgos
Evaluar	. Evaluación de Riesgos . Plan para tratamiento de riesgos . Aceptación del Riesgo
Tratar	. Implementación del Plan para tratamiento de Riesgos . Monitorización continua y análisis crítico del riesgo. . Mantenimiento y Mejoramiento del Proceso de Gestion de Riesgo.

Fuente: GRC – AS/NZS 4360

Elaboración: Propio

Criterios de priorización para la evaluación de Riesgos de Seguridad de Información

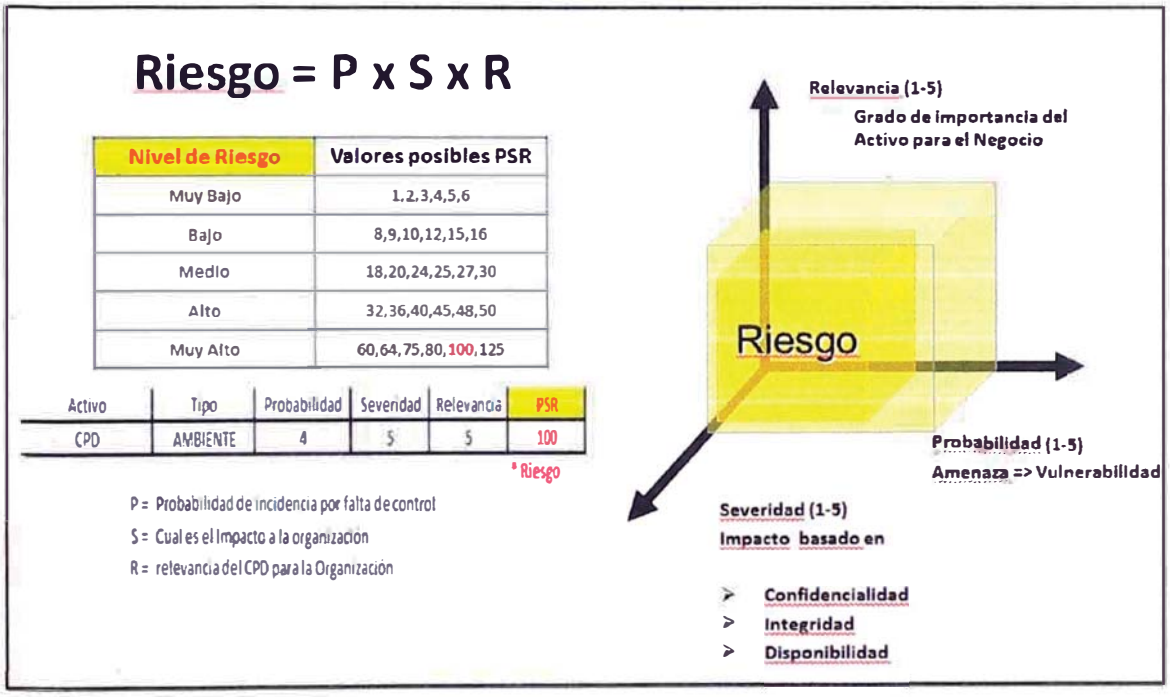
El proceso de Gestión de Riesgos de Seguridad de Información tiene como objetivo identificar y mitigar los riesgos a los que se ven sometidos los activos de Información del Banco, los mismos que están asociados a los diversos procesos del Banco, a fin de establecer y ejecutar planes de acción, para cada nivel de riesgo identificado, el cual permitirá gestionar los riesgos adecuadamente y evitar que éstos impacten negativamente en el logro de los objetivos del BF, contribuyendo a

asegurar la confidencialidad, disponibilidad e integridad de la información.

Como resultado btendremos un mapa de riesgos actualizado que muestre de manera clara y objetiva los niveles de riesgos de los activos de información relacionados a los procesos de negocio del Banco; obteniendo una retroalimentación para establecer nuevas medidas de protección y/o estándares de seguridad, contribuyendo al mejoramiento continuo de la seguridad de la Información en el Banco.

A continuación se muestra el modelo Gráfico de la Gestión de riesgo de Seguridad de Información.

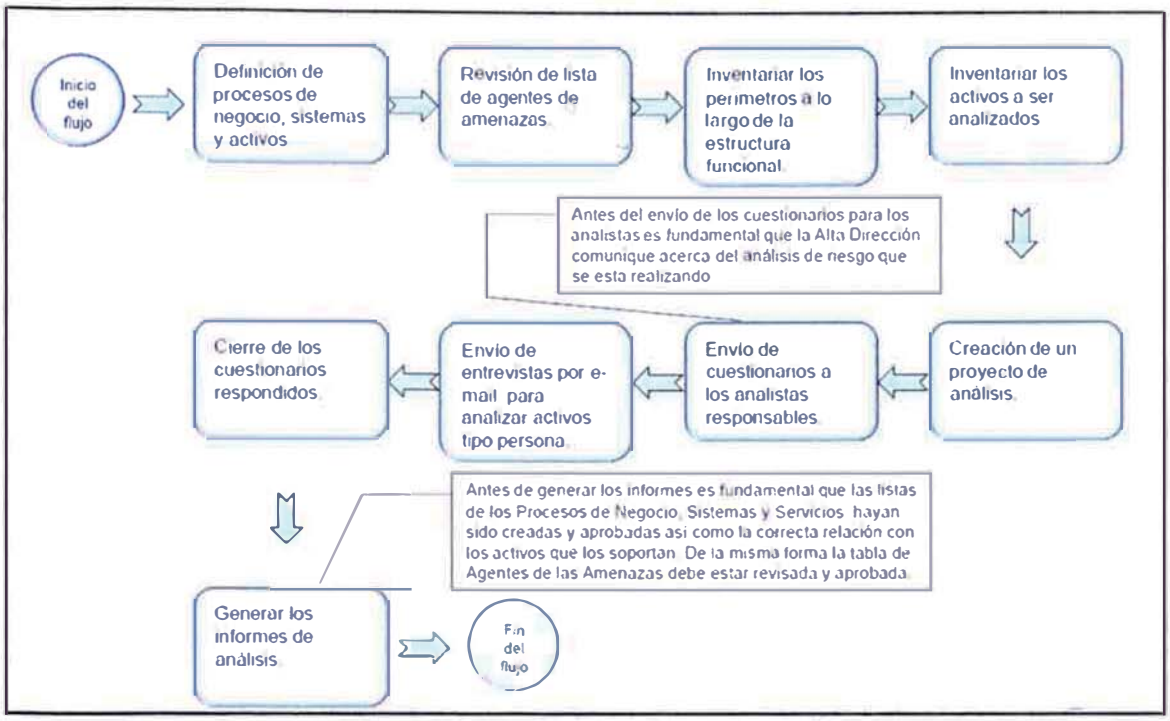
ESQUEMA N° 25: Medición de Riesgo en Seguridad de Información



Fuente: Banco en estudio

Elaboración: Banco en Estudio

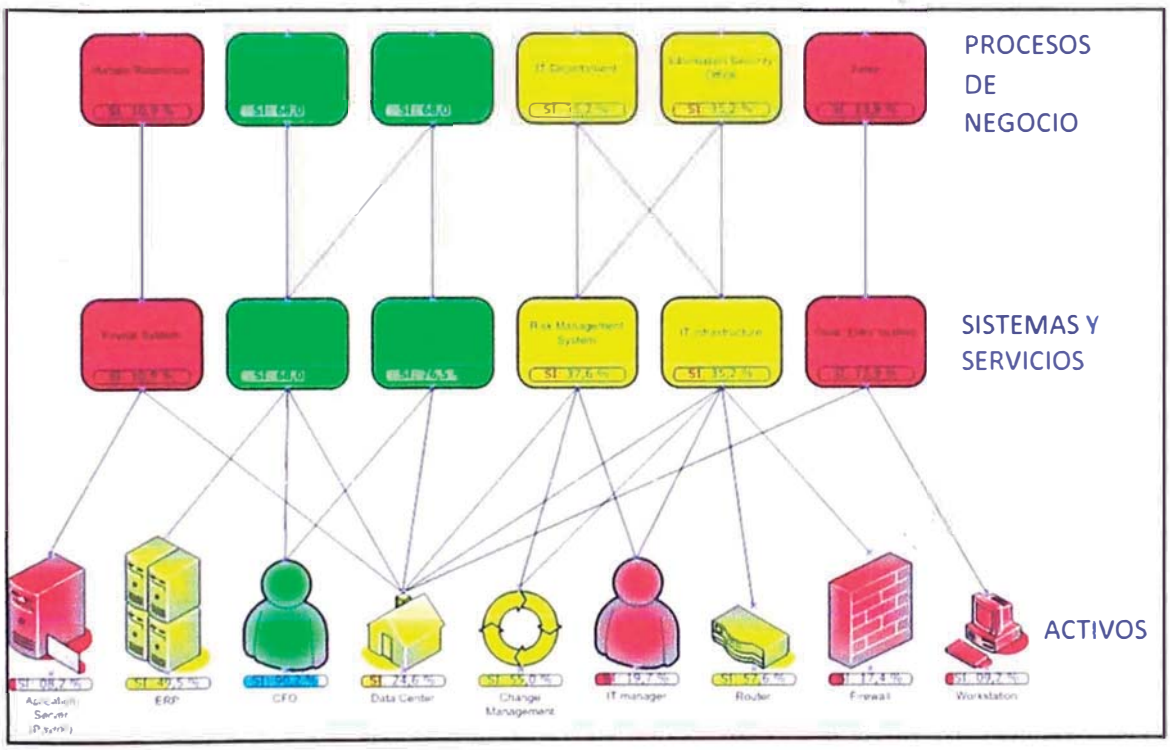
ESQUEMA N° 26: Flujo de Procesos de la Gestión de Riesgos de SI



Fuente: Governance Risk and Compliance

Elaboración: Propia

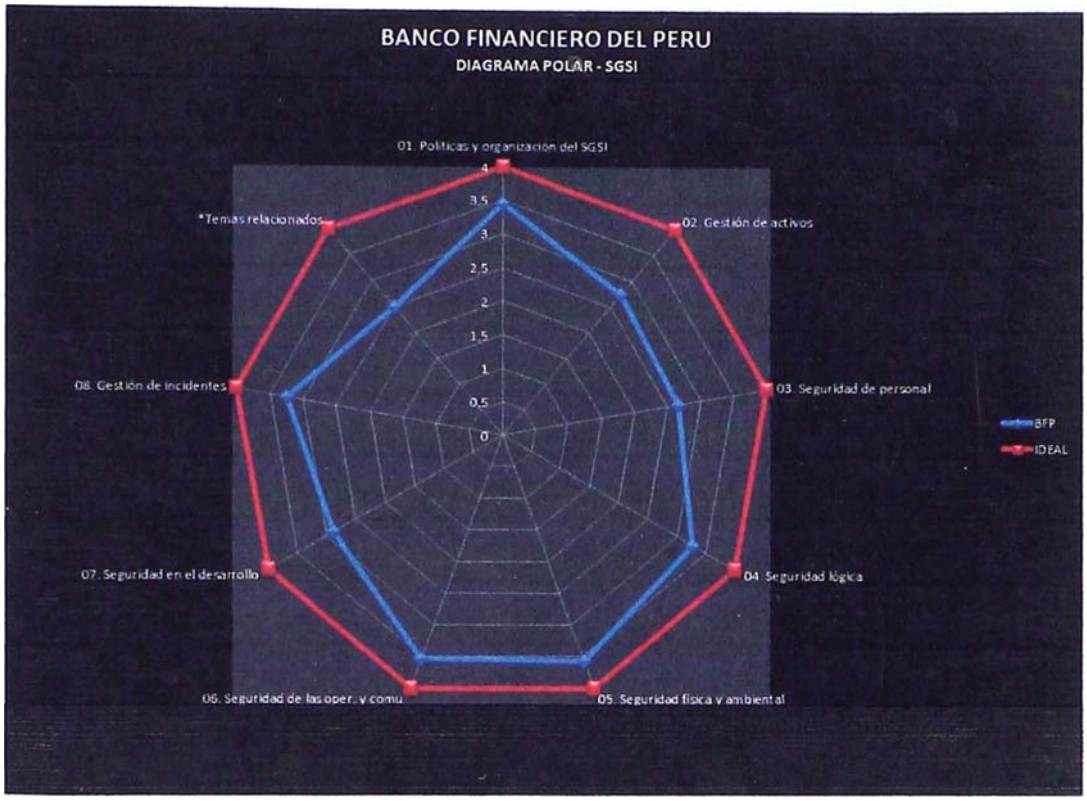
ESQUEMA N° 27: Gestión de Riesgos del SGSI



Fuente: Banco en estudio

Elaboración: Banco en Estudio

ESQUEMA N° 28: Radar de Cumplimiento del Sistema de Gestión de Seguridad de Información



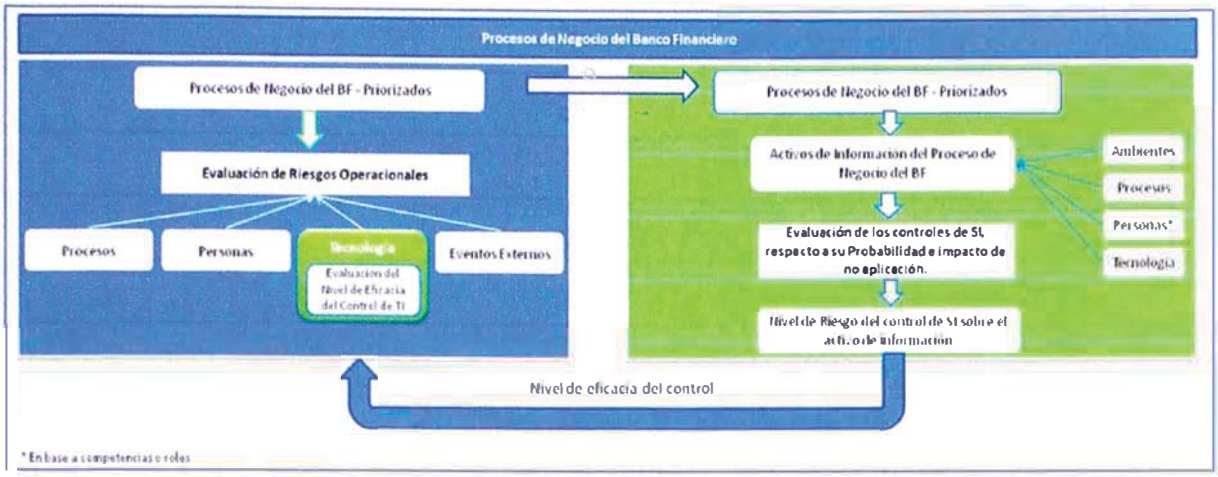
Fuente: Banco en estudio

Elaboración: Banco en Estudio

El objetivo es evaluar los principales riesgos de Seguridad de Información generados por los activos de información (aplicaciones, servicios de TI, otros) que soportan a los procesos de negocio. Además de definir estrategias y opciones de priorización para mitigar el riesgo a niveles aceptables para la organización.

A continuación se muestra el alineamiento entre las Metodologías de Riesgo Operativo y Seguridad de Información, el cual es importante para identificar la mecánica de comunicación entre los documentos.

ESQUEMA N° 29: Enlace de la Metodología de RO, con la Metdología de Riesgo del SGSI



Fuente: Banco en estudio

Elaboración: Banco en Estudio

3.4.3. Implementación del Sistema de Continuidad de Negocios

La implementación del Sistema de Gestión de Continuidad de Negocios se basa en la Norma BS 25999, a continuación mostramos la mecánica operativa del SGCN.

ESQUEMA N° 30: Mecánica Operativa del SGCN

Fuente: Banco en estudio

Elaboración: Banco en Estudio

La gestión de la continuidad del negocio, está orientada a asegurar las operaciones del Banco, con lo que priorizará los procesos y/o servicios de negocio críticos necesarios para continuar en funcionamiento durante y después de un incidente no planificado.

Asegurar que la gestión de la continuidad del negocio se incorpore en los procesos y estructura del Banco.

La responsabilidad del directorio, gerencia y áreas del Banco deben estar claras para implementar las políticas.

Se ha definido que lo prioritario ante un evento de interrupción operativa será mantener un nivel adecuado de liquidez para cumplir con los compromisos del Banco hacia sus principales grupos de interés; por tanto, uno de los criterios utilizados para definir la criticidad de un proceso se basará en dicha prioridad.

Identificación de los riesgos de continuidad del negocio así como del impacto de los mismos en la organización.

Seleccionar la estrategia de continuidad teniendo en cuenta el análisis del riesgo, las consideraciones legales técnicas y económicas.

Implementar la estrategia seleccionada apoyada en Planes de Gestión de Crisis, Planes de Recuperación de Negocios, Planes de Emergencia, Planes de Recuperación de Servicios de TI y Planes de Contingencia Menores.

Asegurar que los principales proveedores de servicios críticos cuenten con planes de continuidad y que a su vez cumplan periódicamente con la ejecución de pruebas y el respectivo mantenimiento.

Analizar periódicamente o cuando se requiera, el impacto por inclusión de un nuevo proceso de negocio o presencia de un incidente crítico que no hubiese sido considerado. Asimismo, cambios significativos en la infraestructura tecnológica que soporta los principales procesos, fusión con otra empresa, implementación de un nuevo producto y/o servicio, cambio de sedes, entre otros.

Realizar Programas y Procesos de Prueba que permitan validar los planes implementados así como identificar oportunidades de mejora a través del análisis y monitorización de eventos, así como del resultado de las revisiones de Auditoría.

Monitorear permanentemente el nivel de integración de la gestión de la continuidad del negocio a la cultura organizacional, a fin de identificar requerimientos adicionales.

El sistema de gestión de la continuidad del negocio, no sólo implica el establecimiento e implementación de un plan para proteger a sus empleados, procesos y cadena de suministro, sino que también busca concientizar acerca de los conceptos e importancia de la continuidad del negocio en la organización.

El acceso a información de los Planes de Continuidad del Negocio clasificada como CONFIDENCIAL, será de acceso y uso restringido.

3.4.3.1. Entendimiento Estratégico y operativo del negocio

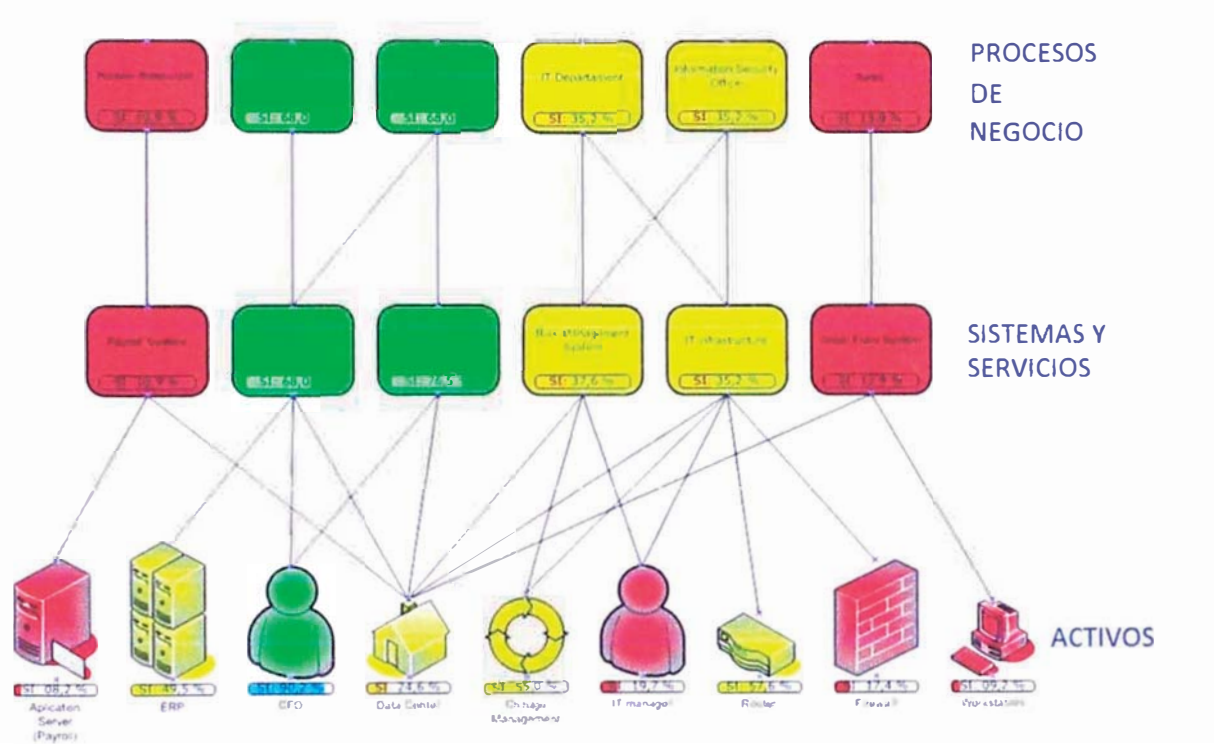
Para la implementación de este punto es necesario conocer la lista total de procesos del banco e identificar la responsabilidad de actualizarlo. En este caso la responsabilidad de mantener la lista de procesos para todo el banco ha sido otorgado al área de Gestión de Proyectos y servicio al cliente.

Además de ello, actualizar la lista de sistemas que soportan los procesos del Banco, esto permitirá tener una visión global de los sistemas y procesos orientados al negocio.

Otro punto importante es el inventario de activos de información que permiten identificar el soporte de los sistemas de información.

Todo este esquema de entendimiento Operativo del negocio lo podemos apreciar en el siguiente Gráfico.

ESQUEMA N° 31: Mapa de Riesgo de Continuidad de Negocios.



Fuente: Banco en estudio

Elaboración: Banco en Estudio

3.4.3.2. Análisis de Impacto y Evaluación

El desarrollo del análisis de impacto en el negocio (BIA) se realizó aplicando la metodología alineada con el estándar internacional BS-25999 que considera las mejores prácticas del BCI (Business Continuity Institute) y DRII (Disaster Recovery Institute International). En este sentido,

la metodología utilizada consideró la ejecución de las siguientes fases:

a) Planificación del BIA

Esta fase considera la estructuración, personalización de los siguientes aspectos:

- Planear las principales tareas, roles y responsabilidades asociadas a la ejecución del BIA.

- Establecer el alcance de la aplicación del BIA en función a las premisas y lineamientos base de priorización definidos por la alta gerencia del banco.

- Estructuración y personalización del cuestionario BIA a aplicar, basado en el entendimiento integral del BFP, evidenciado en los cuatro componentes de levantamiento de información:

i) Procesos de Negocio.- Orientado a identificar los procesos y actividades asociadas a cada una de las áreas a las que se aplicaría el BIA, precisando principalmente los siguientes aspectos:

- Tiempo de Recuperación Objetivo (RTO)

- Responsable

- Dependencia de procesos

ii) Impacto No Financiero.- Orientado a medir cualitativamente los impactos no financieros por la paralización de los procesos de negocio en función a los siguientes aspectos:

- Impacto en el Servicio al Cliente (Cliente Externo)

- Impacto en la Imagen del banco

- Impacto en la Eficiencia Operativa (Cliente Interno)

- En el formato del BIA se considera el impacto Financiero (>70,000.00)

iii) Requerimientos.- Orientado a identificar los requerimientos necesarios para la recuperación de los procesos, en términos de:

- Puestos de trabajo

- Recursos

- Registros Vitales

- Proveedores

- Logística

- Servicios de TI

iv) Compromisos.- Orientado a recopilar información de obligaciones del banco referentes a:

- Reportes Regulatorios

- Servicios a Terceros

b) Ejecución de talleres y entrevistas

Esta fase considera la estructuración, personalización de los siguientes aspectos:

i) Planificar y coordinar tres talleres y diferentes entrevistas.

ii) Inducir en temas de Programas de Continuidad de Negocios e instrucción para el diligenciamiento de cuestionarios, a los facilitadores quienes colaborarían durante los talleres del BIA.

iii) Ejecutar talleres asistidos para los participantes del BIA.

iv) Revisar y validar información mediante entrevistas.- Esta fase consideró la estructuración, personalización de los siguientes aspectos:

c) Análisis

Este paso comprende el análisis de la información recabada y ejecución de entrevistas y reuniones adicionales con colaboradores del Área de Seguridad de Información y Continuidad de Negocio. Este análisis se focalizó en los siguientes aspectos:

i) Confirmación de RTOs de los procesos, principalmente de los críticos (Hasta 4hrs.) que deben tener una prioridad Alta de recuperación luego de ocurrido un evento de desastre.

ii) Validar el cumplimiento de los criterios de respuesta de los usuarios, se solicitó el ajuste y mejora de las respuestas que incumplían los criterios establecidos para resolver el cuestionario de cada área según los Criterios del BIA que garanticen el Alineamiento que se muestran en el Anexo "A".

iii) Identificación de brechas de cobertura entre RTOs de los procesos críticos requeridos por el negocio y los cubiertos por el Plan de Continuidad de Negocio (PCN).

iv) Identificación de brechas de cobertura entre RTOs de los servicios críticos de TI requeridos por el negocio y los ofrecidos por el área de TI.

Leyenda de colores

Color		RTO "Hasta 4 Hrs."
Color		RTO "Hasta 12 Hrs."
Color		RTO "Hasta 24 Hrs."
Color		RTO "Hasta 48 Hrs."

Color  RTO "Hasta 5 Días"

Color  RTO "Hasta 10 Días"

Color  RTO "Mayor a 10 Días"

d) Resultados del análisis de impacto

Con la finalidad de facilitar la toma de decisiones por parte de la Gerencias del Banco, se ha dispuesto un análisis desagregado en dos partes las cuales están comprendidas en las siguientes secciones:

Sección I: Se muestran los reportes de los resultados consolidados a nivel del banco.

Sección II: Se muestran los reportes de los resultados para cada área de negocio.

Pudiéndose apreciar principalmente a través de estos reportes la priorización de los procesos y actividades en función de la criticidad de su recuperación para el banco de acuerdo con los Tiempos de Recuperación Objetivo, según la siguiente definición:

Prioridad Muy Alta.- Para aquellos procesos y actividades con RTOs de Hasta 4 Hrs., considerados con "Criticidad Muy Alta" luego de ocurrido el evento de desastre.

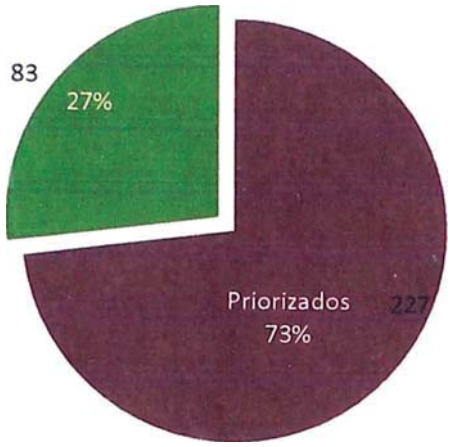
Prioridad Alta.- Para los procesos y actividades con RTOs de 12 Hrs., 24 Hrs. y 48 Hrs., considerados con "Criticidad Alta" luego de ocurrido el evento de desastre.

Prioridad Media.- Para los procesos y actividades con RTOs de 5 Días y 10 Días., considerados con "Criticidad Media" luego de ocurrido el evento de desastre.

Prioridad Baja.- Para los procesos y actividades con RTOs mayores a los 10 Días., considerados "Sin Criticidad" luego de ocurrido el evento de desastre.

A continuación mostramos los siguientes resultados del BIA orientado a los procesos:

CUADRO 17 : Priorización de Procesos

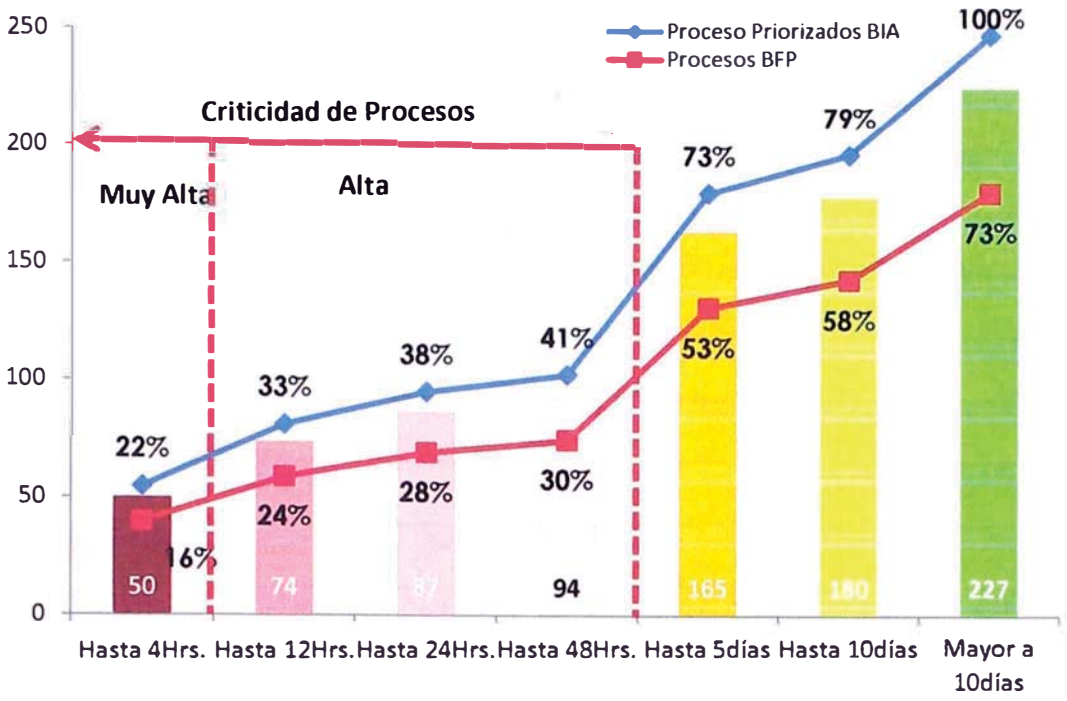


Fuente: Banco en estudio

Elaboración: Banco en Estudio

El Banco cuenta con 310 procesos mapeados (Procesos del Banco), al llevar a cabo el taller de BIA los responsables de las areas priorizaron los procesos que consideran criticos, en caso de una crisis estos nos permitira cierta cantidad de procesos que nos permitiran continuar con el negocio y luego reestablecer el negocio en su totalidad. El gráfico Nro. 2 nos permite observar cuantos fueron los procesos priorizados (227 procesos priorizados, 73 % de los procesos del Banco). Esta priorizacion nos permite analizar unicamente los procesos de interes, para orientar nuestros esfuerzos en la recuperacion de la liquidez del negocio, y mantener los servicios basicos de atencion al cliente.

CUADRO 18 Gráfico Cobertura de Procesos por RTO



Fuente: Banco en estudio

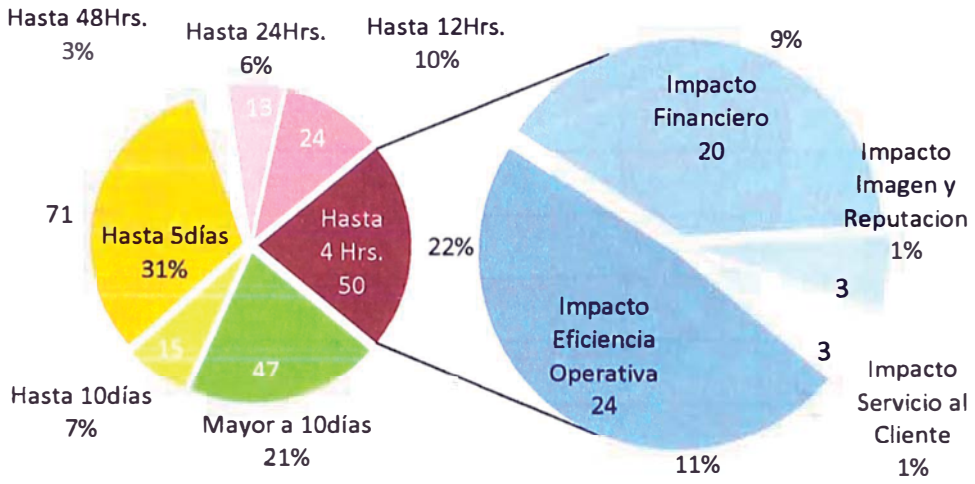
Elaboración: Banco en Estudio

En el grafico anterior se muestra en el eje horizontal los RTO´s determinados para el BIA,en el eje vertical se muestran la cantidad de procesos requeridos por cada unidad de tiempo. Las barras muestran los procesos en forma acumulada para cada unidad de tiempo. La línea de color rojo nos indica la cantidad porcentual de procesos BIA cubiertos al llevar a cabo los procesos indicados por cada unidad de tiempo. La línea de color azul nos indica la cantidad porcentual de procesos del Banco que se cubren al llevar a cabo los procesos indicados por cada unidad de tiempo. Además como se mencionó anteriormente (Resultados del Análisis de Impacto) los RTO se encuentran subdivididos según su criticidad Muy Alta y Alta.

El gráfico se debe leer de la siguiente manera en la categoría de "Hasta 4 Hrs." debemos operar los 50

procesos con criticidad Muy Alta, es decir estos deben ser restablecidos en ese lapso de tiempo. Esto representa el 16 % de los procesos priorizados y el 22 % de todos los procesos del banco, los cuales se muestran en forma acumulada en el grafico anterior. En la siguiente categoría ("Hasta 12 Hrs.") se observa que de cubrir los procesos adicionales a los antes mencionados estaríamos cubriendo el 24 % de los procesos priorizados.

CUADRO 19 Gráfico Nivel de Impacto por RTO



Fuente: Banco en estudio

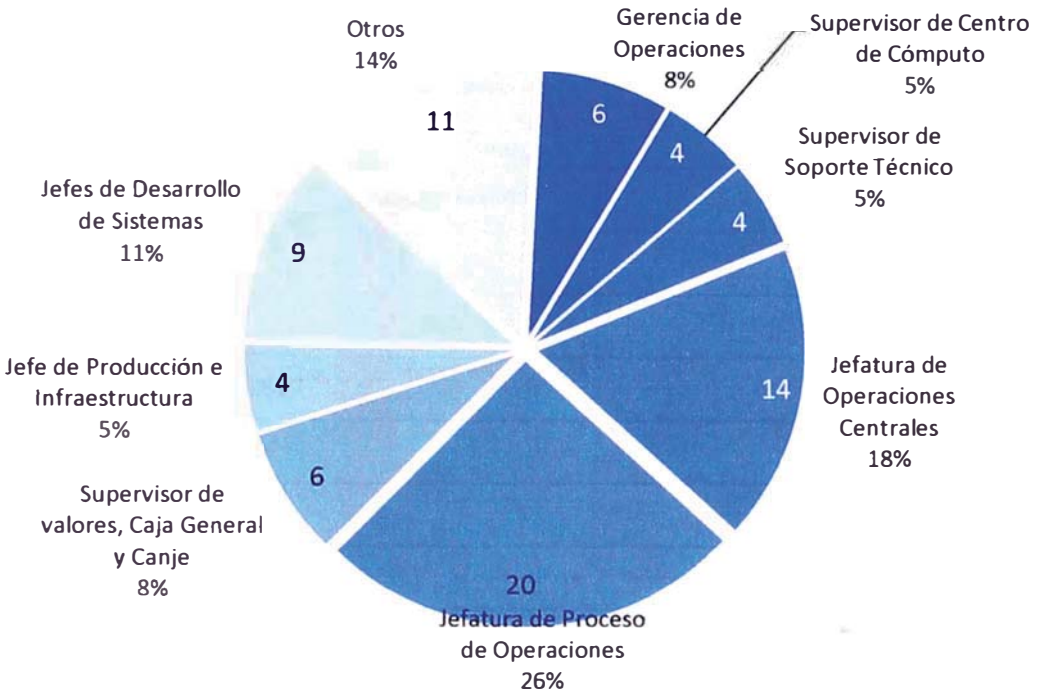
Elaboración: Banco en Estudio

En el grafico se muestran dos gráficos tipo "pie", el de la izquierda muestra los procesos priorizados en función al RTO dado en el impacto, el de la derecha muestra los frentes en los cuales pueden ser impactado el negocio y la cantidad de procesos que lo componen para la categoría de "Hasta 4 Hrs.".

El gráfico debe leerse: "Hasta 4 Hrs." existen 50 procesos que ante la imposibilidad de llevarse a cabo impactarían al BFP en los siguientes frentes: 24 procesos en el frente de Eficiencia Operativa, (11 % de los 50

procesos), 20 de estos en el frente Financiero, 3 en el frente de Servicio al Cliente y otros 3 en el frente de Imagen y Reputación.

GRAFICO 04 Gráfico Área de Operaciones y Tecnología (Área de mayor dependencia en la categoría de "Hasta 4 Horas")



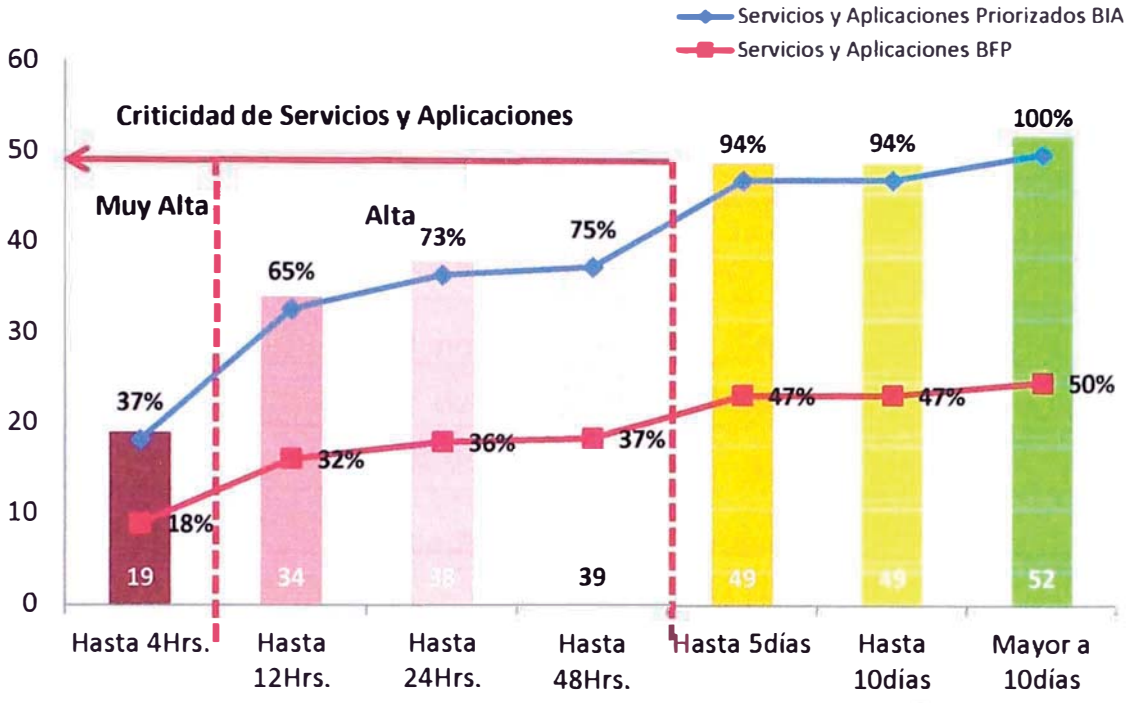
Fuente: Banco en estudio

Elaboración: Banco en Estudio

En el grafico se muestra los procesos que dependen de la Gerencia de Operaciones y Tecnología por ser la Gerencia con mayor demanda (mayor dependencia). Dentro de la Gerencia antes mencionada las áreas que soportan los procesos son las que se muestran, debemos tomar en cuenta que un proceso puede depender de más de un área. Las áreas agrupadas en la clasificación otros corresponden a las áreas cuyos procesos dependientes no superan el 4 % de los 78 procesos de la categoría Hasta 4 Hrs.

El Banco cuenta con 105 servicios y aplicaciones durante el taller BIA se han priorizado solo 52 de estos.

Cuadro 20 Gráfico Cobertura de Servicios y Aplicaciones según RTO



Fuente: Banco en estudio

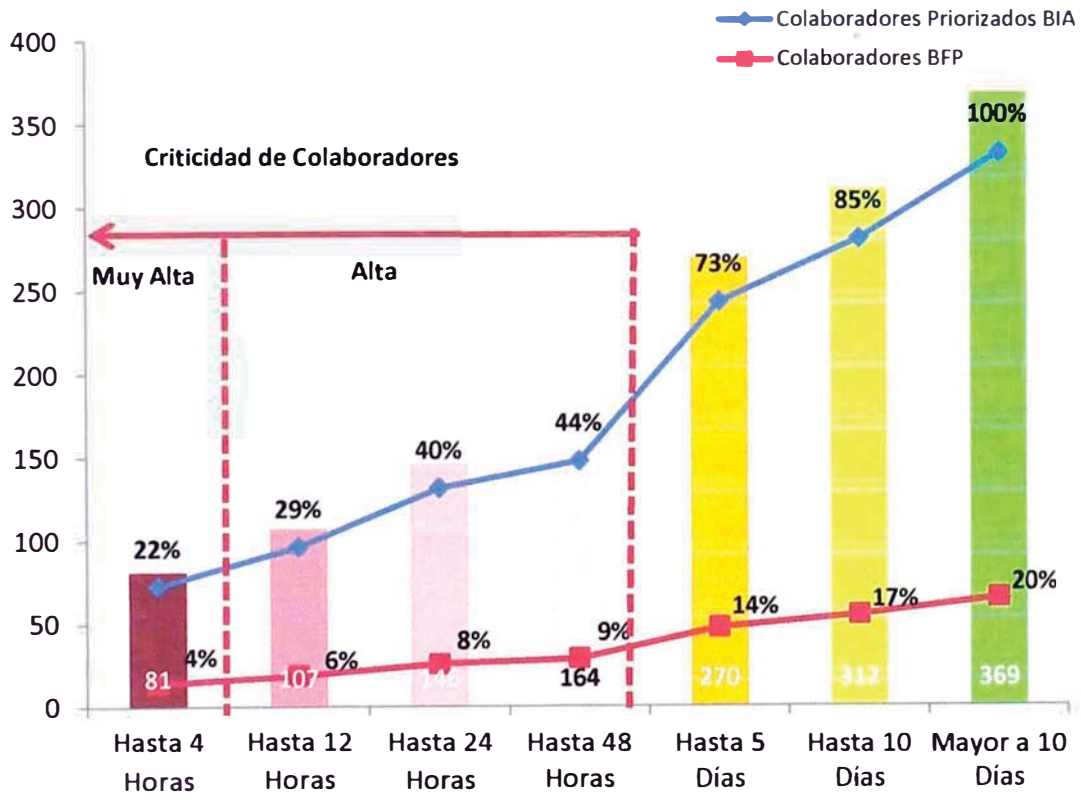
Elaboración: Banco en Estudio

En el grafico se muestra en el eje horizontal los RTO´s determinados para el BIA, en el eje vertical se muestran la cantidad de servicios y aplicaciones requeridos por cada unidad de tiempo. Las barras muestran los servicios y aplicaciones en forma acumulada para cada unidad de tiempo. La línea de color roja nos indica la cantidad porcentual de servicios y aplicaciones BIA cubiertos al llevar a cabo los procesos indicados por cada unidad de tiempo. La línea de color azul nos indica la cantidad porcentual de servicios y aplicaciones BFP que se cubren al llevar a cabo los procesos indicados por cada unidad de tiempo. Los RTO se encuentran subdivididos según su criticidad Muy Alta y Alta.

El gráfico se debe leer de la siguiente manera en la categoría de "Hasta 4 Hrs." debemos operar los 19 servicios y aplicaciones con criticidad Muy Alta, es decir estos deben ser restablecidos en ese lapso de tiempo. Esto representa el 18 % de los servicios y aplicaciones priorizados y el 37 % de los servicios y aplicaciones del banco, los cuales se muestran en forma acumulada en el grafico anterior. En la siguiente categoría ("Hasta 12 Hrs.") se observa que de cubrir los servicios y aplicaciones adicionales a los antes mencionados estaríamos cubriendo el 65 % de los procesos priorizados.

El Banco cuenta con 1888 colaboradores a nivel nacional, durante el taller BIA se han priorizado un total de 369 de estos.

Cuadro 21 Gráfico Cobertura de Colaboradores según RTO



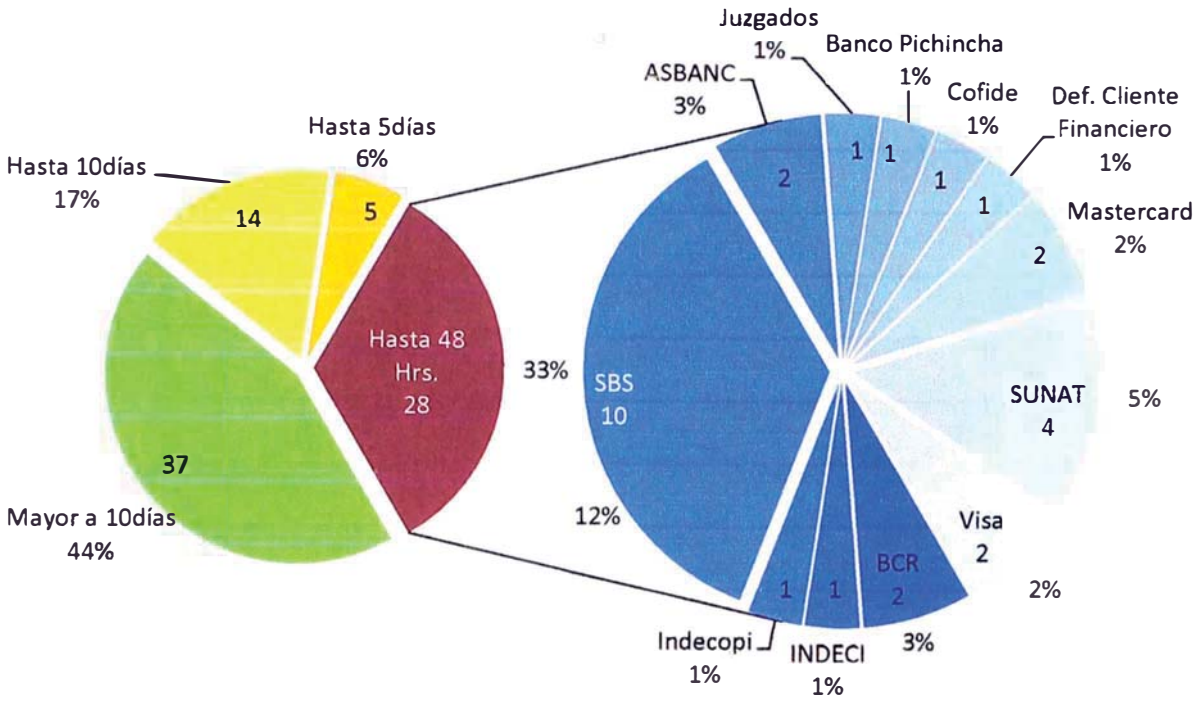
Fuente: Banco en estudio

Elaboración: Banco en Estudio

En el grafico se muestra en el eje horizontal los RTO´s determinados para el BIA, en el eje vertical se muestran la cantidad de colaboradores requeridos por cada unidad de tiempo. Las barras muestran la cantidad de colaboradores en forma acumulada para cada unidad de tiempo. La línea de color roja nos indica la cantidad porcentual de colaboradores priorizados BIA necesarios para llevar a cabo los procesos indicados por cada unidad de tiempo. La línea de color azul nos indica la cantidad porcentual de colaboradores BFP que se cubren al llevar a cabo los procesos indicados por cada unidad de tiempo. Además como se mencionó anteriormente (Punto 1.5. Resultados del Análisis de Impacto) los RTO se encuentran subdivididos según su criticidad Muy Alta y Alta.

El gráfico se debe leer de la siguiente manera en la categoría de "Hasta 4 Hrs." debemos contar con la presencia de 81 colaboradores con criticidad Muy Alta, es decir estos deben estar disponibles en ese lapso de tiempo. Esto representa el 4 % de los colaboradores priorizados BIA y el 22 % de los colaboradores del banco, los cuales se muestran en forma acumulada en el grafico anterior. En la siguiente categoría ("Hasta 12 Hrs.") se observa que se requieren otros colaboradores adicionales a los antes mencionados y contaríamos con el 6 % de los colaboradores priorizados BIA.

Gráfico 05 Gráfico Priorización de Entidades Reguladoras



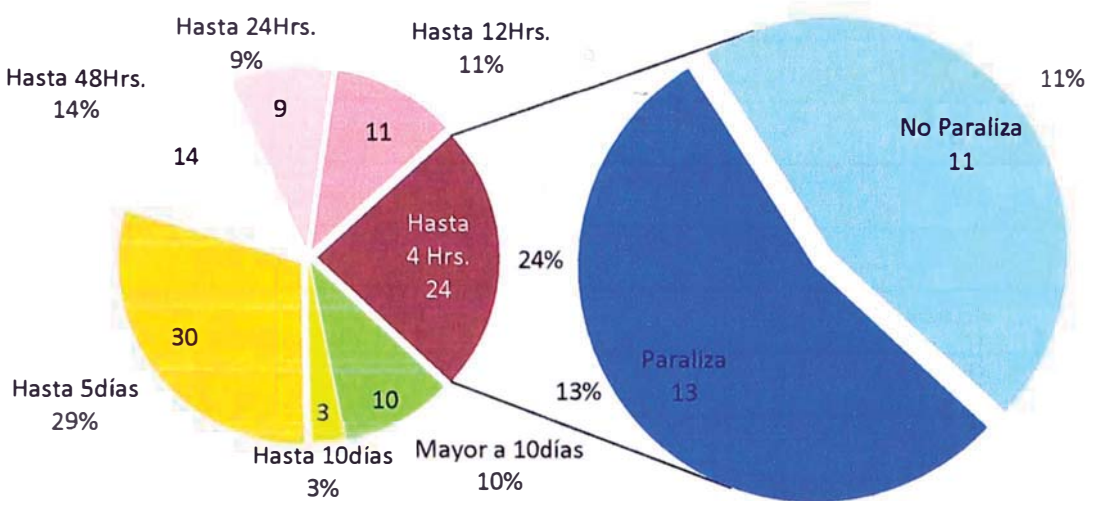
Fuente: Banco en estudio

Elaboración: Banco en Estudio

En el grafico se muestran dos gráficos tipo "pie", el de la izquierda muestra los reportes regulatorios priorizados en función al Tiempo Máximo de Demora de Entrega, el de la derecha muestra las entidades regulatorias a que componen la categoría de "Hasta 4 Hrs.".

El gráfico debe leerse: "Hasta 4 Hrs." deben remitirse 28 reportes regulatorios, 10 reportes deben ser emitidos a la SBS lo cual representa el 12 % de estos 28, y asi con las demás entidades.

Grafico 06 Gráfico Proveedores Criticos (paralizan procesos) según RTO



Fuente: Banco en estudio

Elaboración: Banco en Estudio

En el grafico se muestran dos gráficos tipo "pie", el de la izquierda muestra los proveedores críticos en función al RTO de los procesos que estos proveedores deben soportar, el de la derecha muestra si estos procesos ante la imposibilidad de ser atendido por el proveedores paralizan o no el procesos para la categoría de "Hasta 4 Hrs.".

El gráfico debe leerse: "Hasta 4 Hrs." existen 24 proveedores críticos, 13 proveedores paralizan el proceso en caso de no poder atender al banco lo cual representa el 13 % de estos 13, 11 proveedores no paralizan el procesos.

3.4.3.3. Plan de Gestión de Crisis

El plan de gestión de crisis ha sido orientado para determinar las primeras respuestas que se tendrá cuando tengamos un evento o escenario que pueda interrumpir la normal operación del Banco. Este plan está conformado por tres niveles; estratégico, táctico y operativo.

ESQUEMA32 Esquema de Gestión del Plan de Gestión de Crisis

Orientado al logro del objetivo del SGCN: Planifica, dirige, define y establece los lineamientos a seguir durante la contingencia.

Traduce los lineamientos estratégicos en acciones concretas: Dirige, programa, coordina, organiza y supervisa las acciones a desarrollar.

Acciones concretas a ejecutar: Realiza, ejecuta los procedimientos de contingencia.

Fuente: Banco en estudio

Elaboración: Banco en Estudio

3.4.3.4. Plan de Gestión de Continuidad

El plan de continuidad del Negocio, es aquel plan en donde debe reflejar en cada procedimiento que seguirán las diferentes áreas para que puedan recuperar el negocio de manera eficiente. Aquí se trabaja con cada uno de los procesos y áreas, de tal manera que cada uno mantenga actualizado los planes de continuidad de cada proceso.

3.4.3.5. Planes de Emergencia

Con respecto a Planes de emergencia; el banco lo tiene actualizado, ya que el jefe de Seguridad Física es el responsable de desarrollar toda una estrategia y planes de emergencia en caso de algún evento que pueda afectar al negocio.

3.4.3.6. Plan de Recuperación de los Servicios de TI

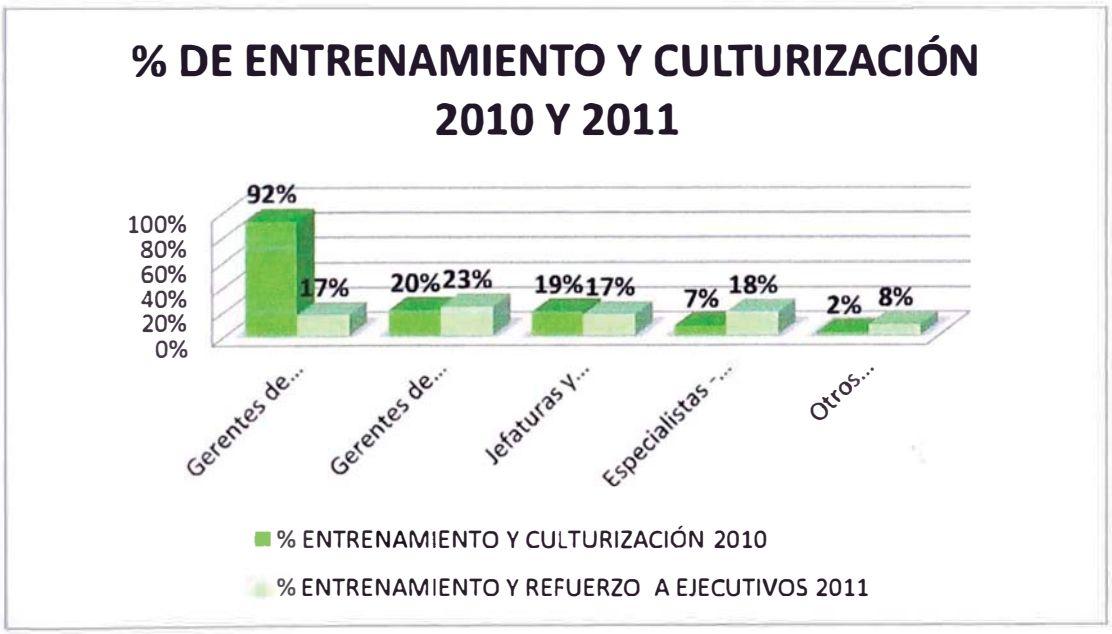
Esta es la parte más costosa del proyecto, aquí se orientamos a que los Servicios más Críticos de la Parte de TI sean replicados en un sitio alterno; con la condición de que si ocurre algún escenario catastrófico, el banco está en la capacidad de tener el soporte tecnológico más importante a la disposición del negocio

3.4.3.7. Capacitación y despliegue de Pruebas de Continuidad de Negocios

El equipo de continuidad tiene la responsabilidad de generar la cultura de continuidad de Negocio en el banco, por lo tanto crea anualmente un programa de capacitaciones. Este cronograma se traduce en personal capacitado para poder cumplir su función en el SGCN.

A continuación mostramos algunas estadísticas de culturización

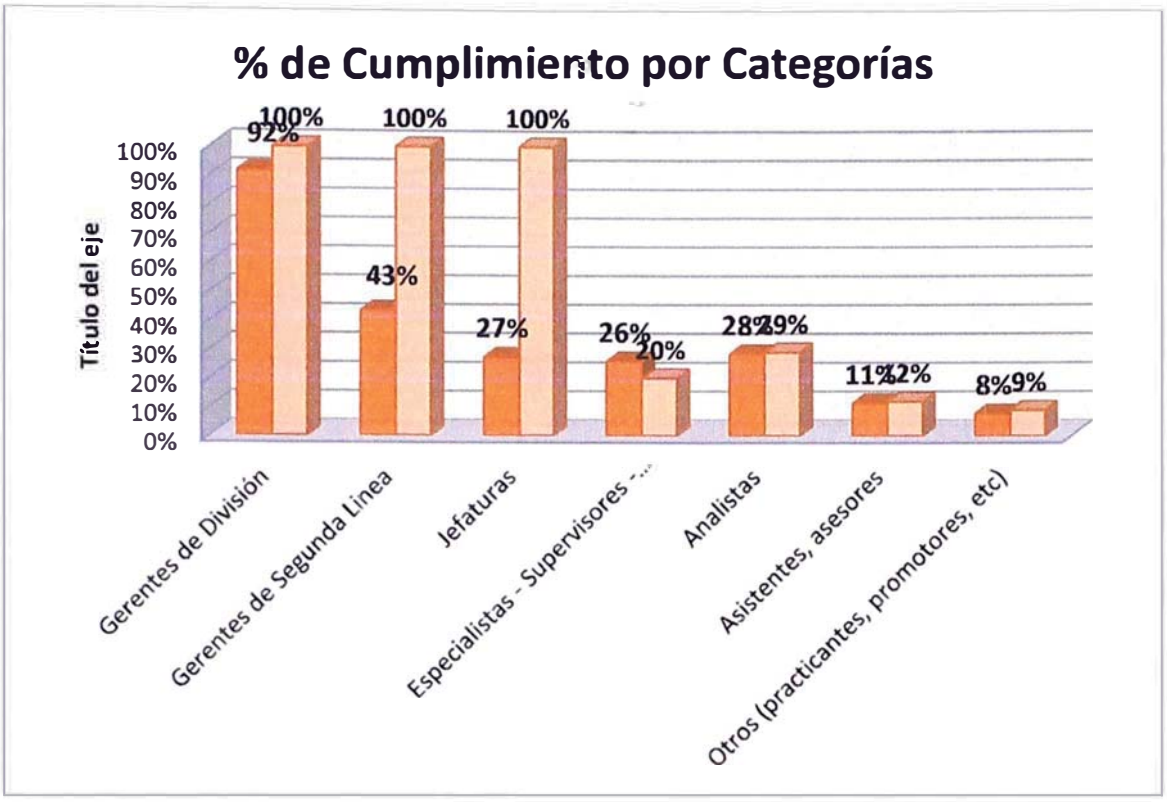
Cuadro 22 Entrenamiento y Culturización de SGSI y SGCN



Fuente: Banco en estudio

Elaboración: Banco en Estudio

Cuadro 23 Meta en Entrenamiento y Culturización de SGSI y SGCN



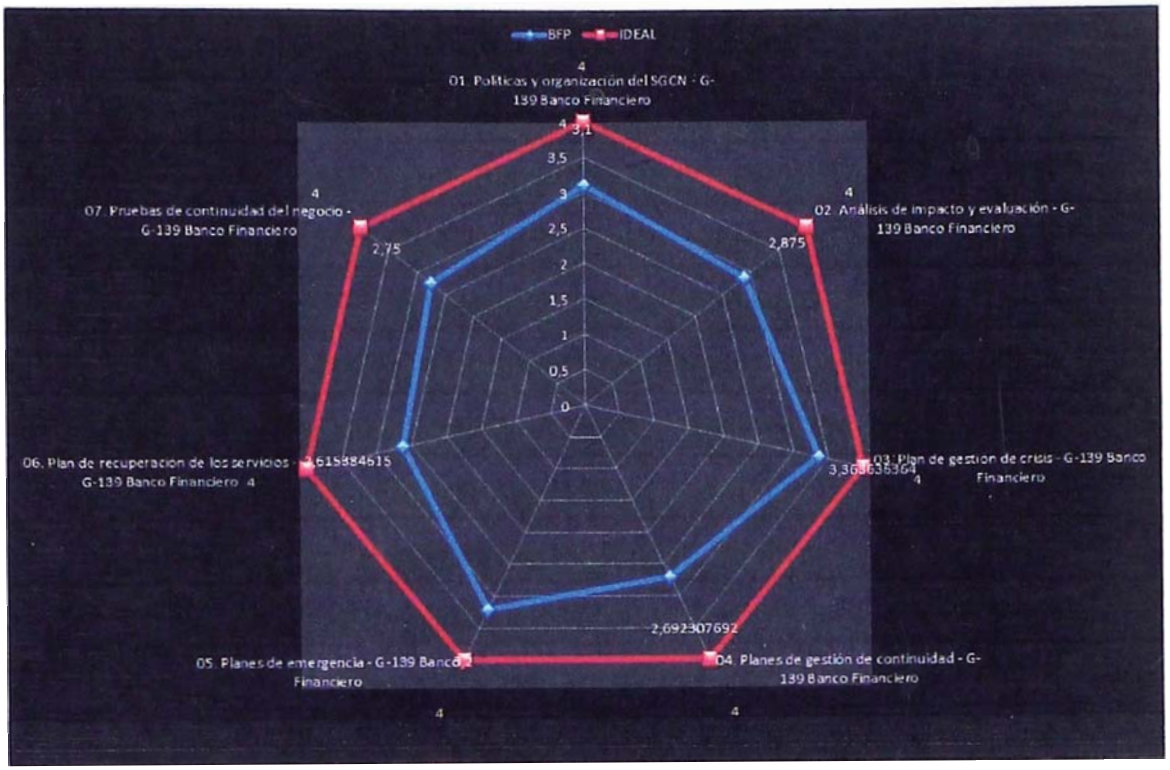
Fuente: Banco en estudio

Elaboración: Banco en Estudio

3.4.3.8. Modelo y Evaluación del Sistema

El Sistema de gestión de Continuidad de Negocios tiene que retroalimentarse, para esto se realiza una evaluación del Modelo. La retroalimentación se implementa contratando una consultora para la identificación de las brechas que se tiene en el sistema; retroalimentación de auditoría interna, externa y SBS.

ESQUEMA N° 33: Radar de Cumplimiento del Sistema de Gestión de Continuidad del Negocio



Fuente: Banco en estudio

Elaboración: Banco en Estudio

CAPÍTULO IV

ANALISIS BENEFICIO COSTO

4.1. SELECCIÓN DE CRITERIOS DE EVALUACIÓN

Todas estas implementaciones de Sistemas de Gestión tanto de Riesgo Operacional, Seguridad de Información y Continuidad de Negocios tienen un objetivo, el cual es aumentar el nivel de madurez al gestionar los riesgos y a su vez Obtener el Método Estándar Alternativo otorgado por la Superintendencia de Banca, Seguros y AFP's para disminuir el Requerimiento de Patrimonio por Riesgo operacional.

Actualmente el Banco se encuentra en el Método Básico de cálculo de Patrimonio Efectivo por Riesgo Operacional.

La diferencia estimada de Requerimiento de Patrimonio por Riesgo operacional entre el Cálculo por método Básico y cálculo por método Alternativo se muestra en el siguiente cuadro:

Cuadro 24 Estimación de Requerimiento de Patrimonio por RO

	2012	2013	2014
Diferencia estimada en Requerimiento de Patrimonio por los diferentes métodos	S/. 9.558.473,85	S/. 14.365.070,62	S/. 20.132.986,74

Fuente: SBS

Elaboración: Propia

Aquí podemos apreciar que si implementamos el método Estándar alternativo, para el año 2012 se podrá reducir el requerimiento de patrimonio en 9,5 MM; para el 2013 en 14 MM y para el 2014 en 20 MM.

Este dinero que se ahorra puede utilizarse para generar más colocaciones y obtener mayor rentabilidad

En el cuadro siguiente podemos apreciar cuales son las diferencias entre tener un Método de Cálculo básico y Método estándar Alternativo. Este último lo que permite es obtener una cálculo de requerimiento de patrimonio orientado a Líneas de Negocio, esto nos brinda gestionar mejor los riesgo.

Cuadro 25: Análisis de Diferencias Monetarias entre Patrimonio Básico y Alternativo

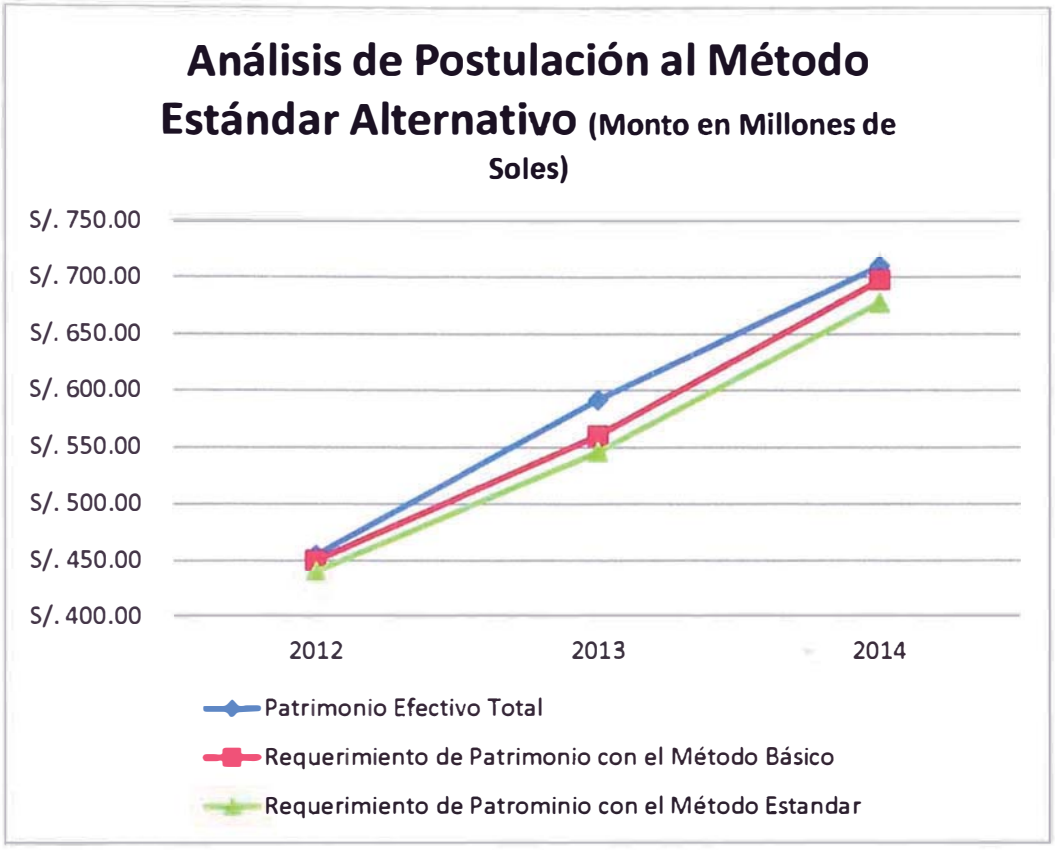
	2009	2010	2011	2012	2013	2014
Patrimonio Efectivo Total	S/. 318.279.000,00	S/. 344.989.303,00	S/. 379.520.723,00	S/. 455.424.867,60	S/. 592.052.327,88	S/. 710.462.793,46
Factor de Ajuste de Riesgo Operacional	0,40	0,40	0,50	0,60	0,80	1,00
Requerimiento de Patrimonio con el Método Básico	S/. 260.464.750,00	S/. 293.306.580,00	S/. 364.898.600,00	S/. 450.381.142,18	S/. 560.515.045,20	S/. 697.942.094,14
a) Requerimiento de Patrimonio por Riesgo de Crédito	S/. 241.615.360,00	S/. 272.979.390,00	S/. 337.047.380,00	S/. 421.309.225,00	S/. 526.636.531,25	S/. 658.295.664,06
b) Requerimiento de Patrimonio por Riesgo de Mercado	S/. 6.046.330,00	S/. 4.693.760,00	S/. 4.376.710,00	S/. 5.038.933,33	S/. 5.038.933,33	S/. 5.038.933,33
c) Requerimiento de Patrimonio por Riesgo Operacional	S/. 12.803.060,00	S/. 15.633.430,00	S/. 23.474.510,00	S/. 24.032.983,85	S/. 28.839.580,62	S/. 34.607.496,74
Requerimiento de Patrominio con el Método Estandar	S/. 260.464.750,00	S/. 293.306.580,00	S/. 364.898.600,00	S/. 440.822.668,33	S/. 546.149.974,58	S/. 677.809.107,40
a) Requerimiento de Patrimonio por Riesgo de Crédito	S/. 241.615.360,00	S/. 272.979.390,00	S/. 337.047.380,00	S/. 421.309.225,00	S/. 526.636.531,25	S/. 658.295.664,06
b) Requerimiento de Patrimonio por Riesgo de Mercado	S/. 6.046.330,00	S/. 4.693.760,00	S/. 4.376.710,00	S/. 5.038.933,33	S/. 5.038.933,33	S/. 5.038.933,33
c) Requerimiento de Patrimonio por Riesgo Operacional	S/. 12.803.060,00	S/. 15.633.430,00	S/. 23.474.510,00	S/. 14.474.510,00	S/. 14.474.510,00	S/. 14.474.510,00

Fuente: SBS

Elaboración: Propia

Mostramos gráficamente la diferencia de cálculos de requerimiento de patrimonio

Cuadro 26: Análisis de Postulación al Método Estándar Alternativo



Fuente: SBS

Elaboración: Propia

Un patrimonio que no se mueve en la empresa o en el giro de negocio y permanece en Caja y bancos es improductivo; no genera ganancias ni agrega valor a la organización; por lo tanto es necesario que cada activo trabaje para generar rentabilidad. En ese sentido, se elaboró un gráfico en el que muestra las Oportunidades de Inversión por diferencia de método de cálculo de Requerimiento de Patrimonio

El dinero que se ahorra puede destinarse a diferentes proyectos en el Banco, ya sea en colocaciones, proyectos de inversión, proyectos de mejora continua, o inversión en el recurso humano el cual es valioso para la organización.

En tal caso para Obtener la Autorización del Método estándar Alternativo, se necesita la Aprobación de la SBS, Auditoría Externa, Auditoría Interna con la implementación de los Sistemas de Gestión de Riesgo Operacional; Sistema de Gestión de Seguridad de Información y Sistema de Gestión de Continuidad de Negocios.

4.2. INFORMACIÓN DE LA SITUACIÓN ECONÓMICA ACTUAL DE IMPLEMENTACIÓN DE LOS SISTEMAS DE GESTIÓN.

Se ha elaborado un cuadro donde nos muestran los costos de implementación de los tres sistemas de Gestión; a continuación describiremos uno a uno a fin de detallar la situación económica actual y proyectada a los años 2012 – 2013- 2014

4.2.1. Costos de Implementación del Sistema de Gestión de Riesgo Operacional

A continuación mostramos el cuadro con **"los requerimientos puntuales de la SBS"** y los costos realizados en la implementación del Sistema de Gestión de Riesgo Operacional (Las proyecciones realizadas son para los años 2012 – 2013 – 2014)

IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN PARA LA AUTORIZACIÓN AL MÉTODO ESTANDAR ALTERNATIVO	2009	2010	2011	2012	2013	2014
Sistema de Gestión de Riesgo Operacional	**S/. 508,933.33**	**S/. 976,933.33**	**S/. 933,200.00**	**S/. 736,866.67**	**S/. 736,866.67**	**S/. 736,866.67**
4.2.1.1. Participación activa del Directorio y la Gerencia General en la Gestión de Riesgo operacional.	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.1.2. Función de la Gestión del Riesgo operacional	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.1.3. Programa de Capacitación al Personal	S/. 26,000.00	S/. 26,000.00	S/. 50,000.00	S/. 40,000.00	S/. 40,000.00	S/. 40,000.00
4.2.1.4. Metodología para la gestión de Riesgo Operacional	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
a) Manuales de gestión de Riesgo Operacional	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
b) Niveles de Apetito y tolerancia al riesgo operacional.	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
c) Política de Priorización.	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
d) Autoevaluación de Riesgo Operacional	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
e) Recolección de eventos de pérdida	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -

f) Análisis y Evaluación de Riesgo y medición de su efectividad	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
g) Tratamiento de los riesgos cuidado de relacionar metodológicamente al apetito y luego a los planes de acción.	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
h) Evaluación de Riesgos Operacionales previo al Lanzamiento de Nuevos Productos y ante cambios en el Ambiente Operativo e Informático	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
i) Evaluación de Riesgos Operacionales previo al Lanzamiento de Nuevos Productos o Servicios y ante Cambios Importantes en el ambiente operativo e informático	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
j) Indicadores claves (KRI) que son actualizados periódicamente	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.1.5. Recursos Suficientes	S/. 327,600.00	S/. 795,600.00	S/. 498,200.00	S/. 498,200.00	S/. 498,200.00	S/. 498,200.00
a) Recursos Humanos Suficientes	S/. 327,600.00	S/. 327,600.00	S/. 459,200.00	S/. 459,200.00	S/. 459,200.00	S/. 459,200.00
b) Tecnología para soportar el Sistema de Gestión de Riesgo Operacional	S/. -	S/. 468,000.00	S/. 39,000.00	S/. 39,000.00	S/. 39,000.00	S/. 39,000.00
4.2.1.6. Revisión de información periódica a interesados internos y externos	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.1.7. Procedimientos para asegurar cumplimiento de metodología para gestión del riesgo operacional	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.1.8. Incentivos para mejorar la gestión de riesgo operacional	S/. 48,000.00	S/. 48,000.00	S/. 48,000.00	S/. 48,000.00	S/. 48,000.00	S/. 48,000.00
4.2.1.9. Gestión de la base de datos de pérdida de eventos de pérdida por riesgo operacional	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.1.10. Revisión periódica independiente de la gestión de riesgo operacional por parte de Auditoría Interna y Consultoría	S/. 16,333.33	S/. 16,333.33	S/. 155,000.00	S/. 59,666.67	S/. 59,666.67	S/. 59,666.67
a) Consultoría en sistema de Gestión de Riesgo Operacional			S/. 138,666.67	S/. 43,333.33	S/. 43,333.33	S/. 43,333.33
b) Auditoría Interna	S/. 16,333.33	S/. 16,333.33	S/. 16,333.33	S/. 16,333.33	S/. 16,333.33	S/. 16,333.33

4.2.1.11. Revisión periódica independiente de la gestión del riesgo operacional por parte de una sociedad de Auditoría Externa.	S/. 91,000.00	S/. 91,000.00	S/. 182,000.00	S/. 91,000.00	S/. 91,000.00	S/. 91,000.00

A continuación mostraremos los detalles del cuadro mostrado anteriormente.

4.2.1.1. Participación activa del Directorio y la Gerencia General en la Gestión de Riesgo operacional. El directorio y la gerencia General participan activamente en el Sistema de gestión de Riesgo operacional, teniendo reuniones mensuales y asignando recursos para su implementación y mantenimiento del sistema. Este punto es una exigencia de la SBS, sin embargo no se coloca costo, ya que el Directorio y la Gerencia ven la organización como un todo.

4.2.1.2. Función de la Gestión del Riesgo operacional. El costo en este caso es cero, porque se encuentran inmersos en el acápite de Recursos Suficientes, ya que los recursos deben establecer todas las funciones y formalizarlas.

4.2.1.3. Programa de Capacitación al Personal. Se designaron presupuestos anuales de 26 000 soles en el 2009 y 2010 para la capacitación de los colaboradores del área de Riesgo operacional, así como a todos los colaboradores; en el 2011 se incrementó a 50 000 soles por la implementación de un sistema E-learning de capacitación y postulación al ASA; en los siguientes años se estima un presupuesto de 40 000 para la capacitación a los recursos.

4.2.1.4. Metodología para la gestión de Riesgo Operacional. El presupuesto designado para este ítem es cero, porque se está considerando en el presupuesto de "4.2.1.5 Recursos suficientes", ya que este es el responsable de diseñar la metodología e implementarla.

4.2.1.5. Recursos Suficientes. Existe un presupuesto designado para este ítem; que a su vez se divide en dos puntos importantes: Recursos Humanos Suficientes y Tecnología que soporta a RO. Para el primero se ha tomado en consideración los costos de un Gerente de Riesgo Operacional, dos analistas de RO y un practicante de RO, a partir del 2011 se amplió a un Supervisor de RO. Para el segundo ítem la empresa ha comprado un software de RO, que ayuda a la gestión de RO.

4.2.1.6. Revisión de información periódica a interesados internos y externos. El equipo de Riesgo Operacional (incluido en el presupuesto de Recursos Suficientes) realiza presentaciones internas y externas al área, brindando una comunicación a los colaboradores de todas las acciones que se realizan en Riesgo operacional así como a los comités creados.

4.2.1.7. Procedimientos para asegurar cumplimiento de metodología para gestión del riesgo operacional. El equipo de Riesgo Operacional (incluido en el presupuesto de Recursos Suficientes) realiza la documentación pertinente al SGRO.

4.2.1.8. Incentivos para mejorar la gestión de riesgo operacional. El equipo de Riesgo Operacional brinda incentivos a los colaboradores que contribuyan con identificar posibles riesgos operacionales para poder mitigarlos a tiempo. El presupuesto es de 800 soles mensuales para 5 colaboradores del Banco.

4.2.1.9. Gestión de la base de datos de pérdida de eventos de pérdida por riesgo operacional. Uno de los analistas de Riesgo operacional (considerado en el presupuesto de Recursos Suficientes) realiza la gestión de Base de Pérdidas, realizando reportes a los diferentes comités de RO.

4.2.1.10. Revisión periódica independiente de la gestión de riesgo operacional por parte de Auditoría Interna y Consultoría. El banco contrata a Consultores y Auditores para poder tener una revisión independiente solicitado por el ente regulador. Con respecto a la Consultoría, el Banco ha contratado desde el 2011 a ***K- Globalis***, una firma consultora para reducir brechas de los sistemas de Gestión. Con respecto a la auditoría Interna , el banco cuenta con un auditor interno especializado en Riesgo Operacional, es cual dedica su tiempo a detectar oportunidades de mejora en el sistema.

4.2.1.11. Revisión periódica independiente de la gestión del riesgo operacional por parte de una sociedad de Auditoría Externa. El Banco ha venido contratando a la Auditora externa ***KPMG*** para poder tener una revisión independiente sobre el sistema de RO. La frecuencia es anual. En el año 2011 se contrató a otra auditoría más, ya que la SBS requiere el análisis del Sistema de RO por parte de dos auditoras para postular a la SBS.

4.2.2. Costos de Implementación del Sistema de Gestión de Seguridad de la Información

A continuación mostramos el cuadro de los costos realizados en la implementación del Sistema de Gestión de Seguridad de la Información (Las proyecciones realizadas son para los años 2012 – 2013 – 2014)

IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN PARA LA AUTORIZACIÓN AL MÉTODO ESTANDAR ALTERNATIVO	2009	2010	2011	2012	2013	2014
Sistema de Gestión de Seguridad de Información	**S/. 742,733.33**	**S/. 1,114,933.33**	**S/. 1,399,800.00**	**S/. 1,253,466.67**	**S/. 1,253,466.67**	**S/. 1,253,466.67**
4.2.2.1. Política y Organización del SGSI	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.2.2. Organización del Sistema de Gestión de Seguridad de Información	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.2.3. Mecánica Operativa del Sistema de gestión de seguridad de Información	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.2.4. Gestión de Servicios Externos	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.2.5. Gestión de Activos	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.2.6. Seguridad del Personal	S/. 211,400.00	S/. 271,600.00	S/. 436,800.00	S/. 476,800.00	S/. 476,800.00	S/. 476,800.00
a) Recursos Humanos Suficientes	S/. 211,400.00	S/. 271,600.00	S/. 436,800.00	S/. 436,800.00	S/. 436,800.00	S/. 436,800.00
b) Capacitación a los colaboradores por el E learning	S/. -	S/. -	S/. -	S/. 40,000.00	S/. 40,000.00	S/. 40,000.00
4.2.2.7. Seguridad Física y Ambiental	S/. 424,000.00	S/. 424,000.00	S/. 522,000.00	S/. 522,000.00	S/. 522,000.00	S/. 522,000.00
a) Recursos Humanos Suficientes	S/. 112,000.00	S/. 112,000.00	S/. 210,000.00	S/. 210,000.00	S/. 210,000.00	S/. 210,000.00
b) Tecnología que soporta el sistema de Seguridad Física y Ambiental	S/. 312,000.00	S/. 312,000.00	S/. 312,000.00	S/. 312,000.00	S/. 312,000.00	S/. 312,000.00
4.2.2.8. Seguridad de las Operaciones y Comunicaciones	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.2.9. Control de Accesos a los sistemas del banco	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.2.10. Seguridad en la adquisición y Desarrollo de Software	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.2.11. Gestión de Incidentes	S/. -	S/. -	S/. 52,000.00	S/. 52,000.00	S/. 52,000.00	S/. 52,000.00
a) Herramienta para Gestión de Incidentes	S/. -	S/. -	S/. 52,000.00	S/. 52,000.00	S/. 52,000.00	S/. 52,000.00

4.2.2.12. Gestión de Cumplimiento	S/.	107,333.33	S/.	107,333.33	S/.	337,000.00	S/.	150,666.67	S/.	150,666.67	S/.	150,666.67
a) Consultoría en sistema de Gestión de Seguridad de Información					S/.	138,666.67	S/.	43,333.33	S/.	43,333.33	S/.	43,333.33
b) Auditoria Interna	S/.	16,333.33	S/.	16,333.33	S/.	16,333.33	S/.	16,333.33	S/.	16,333.33	S/.	16,333.33
c) Auditoría Externa	S/.	91,000.00	S/.	91,000.00	S/.	182,000.00	S/.	91,000.00	S/.	91,000.00	S/.	91,000.00
4.2.2.13. Gestión de Riesgos de Seguridad de Información	S/.	-	S/.	312,000.00	S/.	52,000.00	S/.	52,000.00	S/.	52,000.00	S/.	52,000.00
b) Tecnología para soportar el Sistema de Gestión de Riesgo Operacional	S/.	-	S/.	312,000.00	S/.	52,000.00	S/.	52,000.00	S/.	52,000.00	S/.	52,000.00

A continuación mostraremos los detalles del cuadro mostrado anteriormente.

4.2.2.1. Política y Organización del SGSI. La política y la organización del SGSI es realizada por el equipo de implementación del SGSI; este equipo está considerado en el punto 4.2.2.6 – Seguridad de personal – Recursos Humanos suficientes.

4.2.2.2. Organización del Sistema de Gestión de Seguridad de Información. La organización del SGSI es realizada por el equipo de implementación del SGSI; este equipo está considerado en el punto 4.2.2.6 – Seguridad de personal – Recursos Humanos suficientes. Es importante recalcar que la organización del SGSI estaba en todo momento respaldada por la Gerencia General.

4.2.2.3. Mecánica Operativa del Sistema de gestión de seguridad de Información. La mecánica Operativa del SGSI es realizada por el equipo de implementación del SGSI; este equipo está considerado en el punto 4.2.2.6 – Seguridad de personal – Recursos Humanos suficientes.

4.2.2.4. Gestión de Servicios Externos. La Gestión de Servicios Externos es realizada por el equipo de implementación del SGSI; este equipo está considerado en el punto 4.2.2.6 – Seguridad de personal – Recursos Humanos suficientes.

4.2.2.5. Gestión de Activos. La gestión de Activos es realizada por el equipo de implementación del SGSI; este equipo está considerado en el punto 4.2.2.6 – Seguridad de personal – Recursos Humanos suficientes.

4.2.2.6. Seguridad del Personal. Para este ítem existen dos partes importantes: Recursos Humanos suficientes y la capacitación para los colaboradores en general. En el primero, en el 2009 se contaba con 3 personas enfocadas a implementar el SGSI, en el 2011, se adicionó un recurso más para poder afianzar la implementación del SGSI. Por otro lado, en el segundo ítem, en el 2012 se presupuestó la capacitación para todos los colaboradores respecto a Seguridad de Información en los diferentes niveles.

4.2.2.7. Seguridad Física y Ambiental. Para este punto existen dos partes importantes: Los recursos humanos suficientes para poder implementar la seguridad física en toda la institución orientada a la seguridad de la información y la tecnología necesaria para poder tener la gestión de alarma en la seguridad de las diferentes agencias del BFP. Es necesario mencionar además que se realizaba un check list en las agencias para poder mejorar la seguridad física en el Banco.

4.2.2.8. Seguridad de las Operaciones y Comunicaciones. La gestión de Seguridad de Operaciones y Comunicaciones es realizada por el equipo de implementación del SGSI y el equipo de tecnología; estos equipos están siendo considerado en el punto 4.2.2.6 – Seguridad de personal – Recursos Humanos suficientes.

4.2.2.9. Control de Accesos a los sistemas del banco. El control de Seguridad de accesos es realizada por el equipo de implementación del SGSI, dentro de este punto se encuentra la gestión de accesos, el cual está considerado en el punto 4.2.2.6 – Seguridad de personal – Recursos Humanos suficientes.

4.2.2.10. Seguridad en la adquisición y Desarrollo de Software. La gestión de Seguridad de Operaciones y Comunicaciones es realizada por el equipo de implementación del SGSI y el equipo de tecnología; estos equipos están siendo considerado en el punto 4.2.2.6 – Seguridad de personal – Recursos Humanos suficientes.

4.2.2.11. Gestión de Incidentes. La gestión de Incidentes es realizada por el equipo de implementación del SGSI y el equipo de tecnología (ITIL); además el banco ha implementado en el 2011 un software de gestión de incidentes para agilizar la implementación con un presupuesto anual de $ 20, 000.

4.2.2.12. Gestión de Cumplimiento. Para la gestión de cumplimiento tenemos 3 puntos importantes: La consultoría en SGSI, Auditoría Interna y Auditoría Externa; para el primer Item, el banco contrato a una Consultora en el 2011 para la determinar las brechas del SGSI; con respecto a la auditoría interna, el banco tiene una persona designada para reportar a los auditores internos sobre las oportunidades de mejora del SGSI y para el tercer Item: Auditoría externa, el banco contrata anualmente una auditoría externa el cual es requisito para el funcionamiento de los banco e inclusive para la postulación al Método Estándar alternativo.

4.2.2.13. Gestión de Riesgos de Seguridad de Información. El Banco ha adquirido un software que ayuda a la Gestión de Riesgo Tecnológico y de Seguridad de Información: Modulo Risk Manager; el cual costó UD$ 120, 000.00 con una licencia anual de US$ 20,000.00 anuales; la ventaja comparativa con otros sistemas de riesgos, es que este software

también lo viene utilizando la SBS; el cual brinda al Banco un alineamiento metodológico con el ente regulador reduciendo brechas en la gestión de Riesgos de Seguridad de la Información.

4.2.3. Costos de Implementación del Sistema de Gestión de Continuidad del Negocio

A continuación mostramos el cuadro de los costos realizados en la implementación del Sistema de Gestión de Continuidad de Negocios (Las proyecciones realizadas son para los años 2012 – 2013 – 2014)

IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN PARA LA AUTORIZACIÓN AL MÉTODO ESTANDAR ALTERNATIVO	2009	2010	2011	2012	2013	2014
Sistema de Gestión de Continuidad de Negocios	**S/. 78,000.00**	**S/. 78,000.00**	**S/. 1,516,666.67**	**S/. 173,333.33**	**S/. 1,421,333.33**	**S/. 173,333.33**
4.2.3.1. Entendimiento Estratégico y operativo del negocio	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.3.2. Análisis de Impacto y Evaluación	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.3.3. Plan de Gestión de Crisis	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.3.4. Plan de Gestión de Continuidad	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.3.5. Planes de Emergencia	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.3.6. Plan de Recuperación de los Servicios de TI	S/. -	S/. -	S/. -	S/. -	S/. -	S/. -
4.2.3.7. Capacitación y despliegue de Pruebas de Continuidad de Negocios	S/. 78,000.00	S/. 78,000.00	S/. 1,378,000.00	S/. 130,000.00	S/. 1,378,000.00	S/. 130,000.00
a) Inversión en Tecnología para replicar los sistemas Críticos del banco	S/. 52,000.00	S/. 52,000.00	S/. 1,300,000.00	S/. 52,000.00	S/. 1,300,000.00	S/. 52,000.00
b) Despliegue de todo el personal para las pruebas de continuidad	S/. 26,000.00	S/. 26,000.00	S/. 65,000.00	S/. 65,000.00	S/. 65,000.00	S/. 65,000.00
c) Inversión en Capacitación Mediante Capsulas	S/. -	S/. -	S/. 13,000.00	S/. 13,000.00	S/. 13,000.00	S/. 13,000.00
4.2.3.8. Modelo y Evaluación del Modelo	S/. -	S/. -	S/. 138,666.67	S/. 43,333.33	S/. 43,333.33	S/. 43,333.33
a) Consultoría en sistema de Gestión de Continuidad de Negocios	S/. -	S/. -	S/. 138,666.67	S/. 43,333.33	S/. 43,333.33	S/. 43,333.33

A continuación mostraremos los detalles del cuadro mostrado anteriormente.

4.2.3.1. Entendimiento Estratégico y operativo del negocio. El presupuesto para el entendimiento estratégico y operativo se encuentra inmerso en la Capacitación y despliegue de los planes de continuidad de Negocios.

4.2.3.2. Análisis de Impacto y Evaluación. El presupuesto para el análisis de impacto y evaluaciónse encuentra inmerso en la Capacitación y despliegue de los planes de continuidad de Negocios.

4.2.3.3. Plan de Gestión de Crisis. El presupuesto para la elaboración del plan de gestión de crisis se encuentra inmerso en la Capacitación y despliegue de los planes de continuidad de Negocios.

4.2.3.4. Plan de Gestión de Continuidad. El presupuesto para el plan de gestión de continuidad se encuentra inmerso en la Capacitación y despliegue de los planes de continuidad de Negocios.

4.2.3.5. Planes de Emergencia. El presupuesto para los planes de emergencia se encuentra inmerso en la Capacitación y despliegue de los planes de continuidad de Negocios.

4.2.3.6. Plan de Recuperación de los Servicios de TI. El presupuesto para los planes de recuperación de los servicios tecnológicos se encuentra inmerso en la Capacitación y despliegue de los planes de continuidad de Negocios.

4.2.3.7. Capacitación y despliegue de Pruebas de Continuidad de Negocios. Con respecto a la capacitación al personal responsable de la implementación del SGCN, el Banco ha asignado un presupuesto de US$ 25,000.00 a partir del 2011; además de asignar un recurso para una capacitación a todo el personal del banco por US$ 5,000.00. En el siguiente punto se encuentra las inversiones tecnológicas realizadas para poder replicar los sistemas de

información y el funcionamiento de toda la base de datos desde el sitio alterno Tecnológico implementado, el cual asciende a los US$ 500,000.00 para el 2011 y el 2013, esta es una estrategia de inversión progresiva que se ha optado para aumentar el nivel de madurez con respecto a la continuidad de los negocios.

4.2.3.8. Modelo y Evaluación del Modelo. El banco ha solicitado el apoyo de una consultora K-Globalis para determinar las brechas que existe entre el actual Sistema de Gestión de Continuidad de Negocios y los solicitado por la SBS. Este apoyo valioso ha sido solicitado a partir del 2011 con miras a postular al método estándar alternativo en el 2012.

4.3. RESULTADOS DE LA SOLUCIÓN PLANTEADA

A continuación Mostramos el análisis del proyecto que se inició el abril del 2009. Todo proyecto debe tener su rentabilidad asociada para poder Invertir. Aquí mostramos nuestro análisis del proyecto:

COK Banco	20%

IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN PARA LA AUTORIZACIÓN AL MÉTODO ESTANDAR ALTERNATIVO	2009	2010	2011	2012	2013	2014
Beneficios	**S/. -**	**S/. -**	**S/. -**	**S/. 5,352,745.35**	**S/. 8,044,439.55**	**S/. 11,274,472.57**
Beneficio estimado por Obtener la autorización del uso del método de Cálculo patrimonial Estándar Alternativo	S/. -	S/. -	S/. -	S/. 9,558,473.85	S/. 14,365,070.62	S/. 20,132,986.74
Costos Totales de Implementación del Proyecto a lo Largo del tiempo	**S/. 1,329,666.67**	**S/. 2,169,866.67**	**S/. 3,849,666.67**	**S/. 2,163,666.67**	**S/. 3,411,666.67**	**S/. 2,163,666.67**
Sistema de Gestión de Riesgo Operacional	**S/. 508,933.33**	**S/. 976,933.33**	**S/. 933,200.00**	**S/. 736,866.67**	**S/. 736,866.67**	**S/. 736,866.67**
Sistema de Gestión de Seguridad de Información	**S/. 742,733.33**	**S/. 1,114,933.33**	**S/. 1,399,800.00**	**S/. 1,253,466.67**	**S/. 1,253,466.67**	**S/. 1,253,466.67**
Sistema de Gestión de Continuidad de Negocios	**S/. 78,000.00**	**S/. 78,000.00**	**S/. 1,516,666.67**	**S/. 173,333.33**	**S/. 1,421,333.33**	**S/. 173,333.33**
Flujo de Caja	**S/. (1,329,666.67)**	**S/. (2,169,866.67)**	**S/. (3,849,666.67)**	**S/. 3,189,078.69**	**S/. 4,632,772.88**	**S/. 9,110,805.91**

VAN	S/. 1,608,217.26
TIR	32%

El proyecto ha sido evaluado con las siguientes pautas:

El requerimiento de patrimonio solicitado por el ente regulador es de 9,5MM en el 2012 menor si no se realizaría la implementación; esto patrimonio tiene una palanca (D/P) del 8 en promedio y este dinero que se coloca en el mercado puede generar una ganancia de 7% (spread bancario en escenario pesimista) que equivale a 5,352,745.35 nuevos soles.

Los costos de Implementación de los 3 sistemas de Gestión han sido calculados con las inversiones tecnológicas, pago a los colaboradores que soportan el sistema de gestión, consultorías, auditorías y todo lo requerido para poder realizar la implementación eficiente.

Podemos apreciar que el VAN del proyecto S/. 1,608,217.26 soles durante los 6 años del proyecto; esto se da siempre y cuando se obtenga la autorización ASA por la SBS en este año 2012.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Los entes reguladores de cada país buscan reducir los riesgos bancarios implementando una serie de Políticas, resoluciones y circulares. En el Perú la SBS exige a los banco la implementación de la Resolución 2115 – 2116 y las Circulares G-140 y G-139; estas regulaciones solicitan la implementación de los sistemas de Gestión de Riesgo Operacional, Seguridad de Información y Continuidad del Negocio que tienen el objetivo final de gestionar eficientemente los riesgos operacionales y reducir el requerimiento de patrimonio por Riesgo Operacional.

Para la implementación de los Sistemas de gestión requeridos (RO, SI y CN) y obtener el Método Estándar Alternativo (ASA) se debe invertir un promedio de 2,5 MM de soles anuales en un banco de 4,5 Billones de soles en Activos y 379 Millones en Patrimonio.

Con la autorización del ASA se proyecta una reducción del requerimiento de patrimonio para el año 2012 es de S/. 9.5 MM; para el 2013 es de S/. 14.3 MM y para el 2014 es de S/. 20.1 MM; permitiendo colocar estos montos en el mercado para obtener rentabilidad.

Las proyecciones de reducción de patrimonio son utilizados como Capital de trabajo para el banco en el que se puede obtener un margen al colocarlo en el negocio a una tasa spread (7% modelo pesimista) y apalancándose con 8 veces el patrimonio (D/P = 8). Estas proyecciones

permitirán generar en el modelo S/. 5.3MM en el 2012; S/. 8 MM en el 2013 y S/. 11.2 MM en el 2014; estos montos son proyectados como ganancias netas que el banco.

Al analizar todo el esquema de inversiones y retornos de flujos de caja; podemos apreciar que el proyecto tiene una VAN de S/. 1.6MM a lo largo de 6 años de proyecto; con un costo de oportunidad del 20%.

La implementación del proyecto dura 6 años de los cuales los 3 primeros son para implementar los Sistemas de Gestión y los 3 años últimos para mantener el ciclo de mejora continua.

Para asegurar el éxito de la implementación de los sistemas de gestión es fundamental la participación de la alta dirección y los recursos que se asigna para implementar eficientemente los sistemas de gestión.

Sistema de gestión de Riesgo Operacional

Para la implementación los Sistemas de gestión de Riesgo Operacional y obtener el Método Estándar Alternativo (ASA) se debe invertir un promedio de 800 M de soles anuales.

El efecto de la implementación del Sistema de Gestión de Riesgo operacional ha permitido reducir las Pérdidas desde un 13% en el 2009, pasando por un 5% en el 2010 y finalmente llegando a un 3.5% en el 2011 con respecto a las utilidades. Esto representa una mejora continua en los procesos, el cual permite gestionar de manera eficiente los riesgos operacionales y crear una cultura.

Es importante contar con los recursos suficientes para poder implementar los planes de acción y desplegar la metodología de Riesgo Operacional.

En éxito en la implementación de RO, es involucrar a los colaboradores, motivándolos de manera permanente.

Es fundamentar incluir a entes externos como las auditorías internas, auditorías externas y consultorías que aportan diversos enfoques y oportunidades de mejora.

Sistema de gestión de Seguridad de la Información

- Para la implementación los Sistemas de gestión de Seguridad de la Información y obtener el Método Estándar Alternativo (ASA) se debe invertir un promedio de 1.2 MM de soles anuales.

- El efecto de la implementación del Sistema de Seguridad de la Información ha contribuido a identificar los principales incidentes y a reducir el riesgo tecnológico. El Banco es una empresa que debe contar con sistemas con alta disponibilidad, confidencialidad e integridad de los datos para no impactar negativamente en los negocios que genere el banco o en la reputación.

- Para un ordenamiento y control de la información se debe realizar un inventario de los activos de información, organizándolo por tipo y prioridad por procesos, esto permite aumentar la seguridad de Información en activos de información (tecnología, personas, procesos y ambiente).

- Para crear una cultura de seguridad y su correcta puesta en marcha, se debe priorizar la comunicación constante a todos los colaboradores, así como la capacitación de estos.

- Se debe crear un comité de Seguridad de información en donde los participantes sean de diferentes áreas, con el fin de aprobar planes de acción y monitoreo de indicadores de gestión.

- Es necesario estructurar perfiles y accesos de los colaboradores con la finalidad de reducir cualquier riesgo de seguridad de la información que se convierta en pérdidas monetarias.

- Cada proyecto que implique desarrollo y/o adquisición tecnológica debe cumplir con los controles establecidos para reducir riesgos.

- La gestión de incidentes en Seguridad de información debe ser medible; para ello se debe presentar y comunicar los incidentes; aprender de ellos y mejorar los procesos que den como resultado su reducción.

- La compra del software de Seguridad de Información, permitió alinearse al ente regulador agilizando los reportes necesarios para la gestión.

Sistema de Gestión de Continuidad de Negocios

- Para la implementación los Sistemas de gestión de Continuidad de negocios y obtener el Método Estándar Alternativo (ASA) se debe invertir un promedio de 580 M de soles anuales.

- El efecto de la implementación del Sistema de Continuidad de negocios ha contribuido a tener planes de acción ante cualquier escenario catastrófico; permitiendo mantener la continuidad del Banco y aumentar el respaldo de los clientes ante el banco.

- En la primera fase "Entendimiento a la organización" se identificó cuáles son los procesos más importantes mediante el Análisis de impacto al negocio. En nuestro caso podemos notar que el 16% de todos los procesos son los procesos que hay que darle prioridad en caso de algún desastre o interrupción de las operaciones del Banco. Esto a su vez genera la priorización de los sistemas de información (aplicativos) que deben estar replicados para continuar con el negocio en caso de un desastre (según los escenarios elegidos)

- Los planes del SGCN (Plan de Gestión de crisis, plan de continuidad de negocios, plan de emergencia, y plan de recuperación de TI) deben ser diseñados de tal forma que se puedan aplicar a la realidad y deben ser probadas, para esto el Comité de Continuidad de Negocio debe aprobar los detalles.

- El despliegue de las pruebas de Continuidad de negocios deben estar planificados por líneas de negocio; debe haber una coordinación permanente entre la parte de negocios y la parte de soporte tecnológico para evitar cualquier dificultad. Esta es la fase más crítica del SGCN; porque el banco debe operar con el respaldo tecnológico alterno y no hacer sentir al cliente alguna inoperatividad. Para esto es recomendable invertir en recursos tecnológicos y operativos para poder realizar pruebas exitosas.

RECOMENDACIONES

Para la implementación de los sistemas de Gestión se necesita un equipo idóneo y constantemente capacitado para poder dirigir y convencer a todo el personal de apoyar a reducir cualquier tipo de riesgo y así buscar la mejora continua.

Es muy importante preparar esquemas de inversiones a la Alta Gerencia y al directorio, ya que toda implementación de un sistema de Gestión empieza por los que dirigen el destino de la empresa; debe haber un compromiso de la alta dirección y los colaboradores en general para poder reducir los riesgos operacionales, de seguridad de información y continuidad de Negocios.

Las inversiones realizadas deben estar alineadas a las recomendaciones solicitadas por los entes reguladores; ayudando a reducir el tiempo de entendimiento e implementación.

Como podemos notar, las inversiones fuertes se realizan a partir del año 2012; año en que el banco postulará a la autorización; para esto es importante prever los flujos de caja para evitar picos de inversiones que puedan afectar a la liquidez del banco.

Para la postulación al método estándar alternativo (ASA) y obtener la autorización de la SBS, se recomienda tener una metodología de documentación de sistemas de gestión de tal manera que los auditores y la propia SBS tengan una visión clara de la magnitud del trabajo que se realiza.

Es muy importante que el equipo que implemente el sistema de gestión tenga una reunión semanal al menos el primer año para monitorear los avances; así mismo mostrar los beneficios de la implementación a las diferentes áreas y también la visión de toda la empresa. Todos deben ser partícipes de la implementación empezando por el directorio y la gerencia.

BIBLIOGRAFÍA

Proyectos de Inversión – Formulación y Evaluación – Nassir Sapag Chain – 2007

Operational Risk - Practical Approaches to Implementation – Ellen Davis

Resolución 2115 – 2009 Reglamento para el requerimiento de patrimonio efectivo por riesgo operacional

La gestión del riesgo operacional – De la teoría a su Aplicación – Ana Fernández Laviada -2010

Diseño de un Sistema de Gestión de Seguridad de Información – Alberto G. Alexander – 2007

ISO 2001 – 2005 Information Security System Management

BS 25999 – 2007 Business Continuity Management

Planes de Contingencia – La Continuidad del Negocio en las Organizaciones – Juan Gaspar Martínez- 2004

Reglamento para la gestión del riesgo operacional (Resolución SBS N° 2116-2009).

Reglamento para el requerimiento de patrimonio efectivo por Riesgo de Mercado (Resolución SBS N° 6328-2009).

Reglamento para el requerimiento de patrimonio efectivo por Riesgo de Crédito (Resolución SBS N° 14354-2009).

On competition – Michael E. Porter - 2008

Norma Técnica Peruana – NTP-ISO/IEC 17799 – 2007. Código de Buenas prácticas para la Gestión de Seguridad de Información

Operational risk Capital and Insurance in Emerging Markets – Rocío Paredes-Leandro. Superintendencia de Banca, Seguros y Administradoras privadas de fondos de pensiones.

Finanzas Corporativas – Introducción al VaR – Iván Mascareñas. Universidad Complutense de Madrid.

Examinando los Riesgos macroeconómicos en Basilea II. Propuestas de supervisión para economías emergentes. Juan José Marthans. Superintendencia de Banca, Seguros y Administradoras privadas de fondos de Pensiones

Estándar Australiano AS/NZS 4360 : 1999 Administración de riesgos

Requerimiento de capital bancario y ciclos económicos en un modelo de DSGE. Hamilton Galindo. Superintendencia de Banca, Seguros y administradoras privadas de fondos de pensiones

Total Quality Management – Poornima M. Charantimath 2006

Elaboración del plan estratégico y su implementación a través del cuadro de mando Integral – Daniel Martínez Pedrós – Artemio Milla Gutiérrez - 2005

GLOSARIO DE TERMINOS

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 operacional: El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.

Pérdida: Es un impacto negativo en los ingresos o en el valor patrimonial de la empresa.

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.

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.

Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

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:

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.

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.

Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

Riesgo: La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.

ANEXOS

AS/NZS 4360:1999
Estándar Australiano
Administración de Riesgos

Administración de Riesgos

Contenido

1 Alcance , aplicación y definiciones 3
1.1 Alcance 3
1.2 Aplicación 3
1.3 Definiciones 3
2 Requerimientos de administración de riesgos 6
2.1 Propósito 6
2.2 Política de administración de riesgos 6
2.3 Planeamiento y recursos 6
2.4 Programa de implementación 7
2.5 Revisión gerencial 7
3 Vista general de la administración de riesgos 8
3.1 General 8
3.2 Elementos principales 8
4 Proceso de administración de riesgos 10
4.1 Establecer el contexto 10
4.2 Identificación de riesgos 12
4.3 Análisis de riesgos 13
4.4 Evaluación de riesgos 15
4.5 Tratamiento de los riesgos 16
4.6 Monitoreo y revisión 19
4.7 Comunicación y consulta 19
5 Documentación 20
5.1 General 20
5.2 Razones para documentar 20
Apéndices
A Aplicaciones de administración de riesgos 21
B Pasos en el desarrollo e implementación de un programa de administración de riesgos 22
C Interesados 24
D Fuentes genéricas de riesgo y sus áreas de impacto 25
E Ejemplos de definición y clasificación de riesgos 28
F Ejemplos de expresiones cuantitativas de riesgos 30
G Identificar opciones para tratamiento de los riesgos 31
H Administración y documentación de riesgos 32

Alcance, aplicación y definiciones

1.1 Alcance

Este Estándar provee una guía genérica para el establecimiento e implementación el proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.

1.2 Aplicación

La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones.
Administración de riesgos es el término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. Administración de riesgos es tanto identificar oportunidades como evitar o mitigar pérdidas.
Este Estándar puede ser aplicado a todas las etapas de la vida de una actividad, función, proyecto, producto o activo. El beneficio máximo se obtiene generalmente aplicando el proceso de administración de riesgos desde el principio.
A menudo se llevan a cabo una cantidad de estudios diferentes en las diferentes etapas de un proyecto.
nota: Este Estándar se puede aplicar a un amplio rango de actividades u operaciones de cualquier empresa pública, privada o comunitaria, o grupo.
Se brindan ejemplos en el Apéndice A.

1.3 Definiciones

Para el propósito de este Estándar se aplican las definiciones de abajo.

1.3.1 Aceptación de riesgo: una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
1.3.2 Administración de riesgos: la cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.
1.3.3 Análisis árbol de eventos: una técnica que describe el rango y secuencia posibles de los productos que podrían surgir de un evento iniciado.
1.3.4 Análisis árbol de fallas: un método de ingeniería de sistemas para representar las combinaciones lógicas de varios estados del sistema y causas posibles que pueden contribuir a un evento especificado (denominado evento superior o "top event").
1.3.5 Análisis de modos y efectos de fallas (FMEA): un procedimiento por el cual se analizan modos de fallas potenciales en un sistema técnico. Se puede extender un FMEA para realizar lo que se denomina análisis de modo, efecto y criticidad de fallas (FMECA). En un FMECA, cada modo de falla identificado es ordenado de acuerdo a la influencia combinada de su probabilidad de ocurrencia y severidad de sus consecuencias.
1.3.6 Análisis de riesgo: un uso sistemático de la información disponible para determinar cuan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

1.3.7 Análisis de sensibilidad: examina cómo varían los resultados de un cálculo o modelo a medida que se cambian los supuestos o hipótesis individuales.

1.3.8 Azar de riesgo: una fuente de daño potencial o una situación con potencial para causar pérdidas.

1.3.9 Consecuencia: el producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia. Podría haber un rango de productos posibles asociados a un evento.

1.3.10 Control de riesgos: la parte de administración de riesgos que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.

1.3.11 Costo: de las actividades, tanto directas como indirectas, involucrando cualquier impacto negativo, incluyendo pérdidas de dinero, de tiempo, de mano de obra, interrupciones, problemas de relaciones, políticas e intangibles.

1.3.12 Evaluación de riesgo: el proceso global de análisis de riesgo y evaluación de riesgo, ver la Figura 3.1.

1.3.13 Evaluación de riesgos: el proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgo objetivos u otro criterio.

1.3.14 Evento: un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo particular.

1.3.15 Evitar un riesgo: una decisión informada de no verse involucrado en una situación de riesgo.

1.3.16 Financiamiento de riesgos: los métodos aplicados para fondear el tratamiento de riesgos y las consecuencias financieras de los riesgos.
nota: En algunas industrias financiamiento de riesgos se refiere sólo al fondeo de las consecuencias financieras de los riesgos.

1.3.17 Frecuencia: una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado. Ver también Probabilidad.

1.3.18 Identificación de riesgos: el proceso de determinar qué puede suceder, por qué y cómo.

1.3.19 Ingeniería de riesgos: la aplicación de principios y métodos de ingeniería a la administración de riesgos.

1.3.20 Interesados: aquella gente y organizaciones que pueden afectar, ser afectados por, o percibir ellos mismos ser afectados, por una decisión o actividad.
nota: El término puede incluir también partes interesadas tal como lo define la ISO 14050:1998 y la AS/NZS ISO 14004:1996.

1.3.21 Monitoreo: comprobar, supervisar, observar críticamente, o registrar el progreso de una actividad, acción o sistema en forma sistemática para identificar cambios.

1.3.22 Organización: una compañía, firma, empresa o asociación, u otra entidad legal o parte de ella, sea o no incorporada, pública o privada, que tiene sus propias funciones y administración.

1.3.23 Pérdida: cualquier consecuencia negativa, financiera o de otro tipo.

1.3.24 Probabilidad: la probabilidad de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación a la cantidad total de posibles eventos o resultados. La probabilidad se expresa como un número entre 0 y 1, donde 0 indica un evento o resultado imposible y 1 indica un evento o resultado cierto.

1.3.25 Probabilidad: utilizado como una descripción cualitativa de probabilidad o frecuencia.

1.3.26 Proceso de administración de riesgos: la aplicación sistemática de políticas, procedimientos y prácticas de administración a las tareas de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos.

1.3.27 Reducción de riesgos: una aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de una ocurrencia, o sus consecuencias, o ambas.

1.3.28 Retención de riesgos: intencionalmente o sin intención retener la responsabilidad por las pérdidas, o la carga financiera de las pérdidas dentro de la organización.

1.3.29 Riesgo residual: el nivel restante de riesgo luego de tomar medidas de tratamiento del riesgo.

1.3.30 Riesgo: la posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se lo mide en términos de consecuencias y probabilidades.

1.3.31 Transferir riesgos: cambiar la responsabilidad o carga por las pérdidas a una tercera parte mediante legislación, contrato, seguros u otros medios. Transferir riesgos también se puede referir a cambiar un riesgo físico, o parte el mismo a otro sitio.

1.3.32 Tratamiento de riesgos: selección e implementación de opciones apropiadas para tratar el riesgo.

2 Requerimientos de administración de riesgos

2.1 Propósito

El propósito de esta Sección es describir un proceso formal para establecer un programa sistemático de administración de riesgos.

Se necesita el desarrollo de una política organizacional de administración de riesgos y un mecanismo de soporte con objeto de proveer una estructura para llevar a cabo un programa de administración de riesgos más detallado a nivel sub-organizacional o de proyecto.

2.2 Política de administración de riesgos

El ejecutivo de la organización debe definir y documentar su política para administración de riesgos, incluyendo objetivos para, y su compromiso con, la administración de riesgos. La política de administración de riesgos debe ser relevante para el contexto estratégico de la organización y para sus metas, objetivos y la naturaleza de su negocio. La gerencia asegurará que esta política es comprendida, implementada y mantenida en todos los niveles de la organización.

2.3 Planeamiento y recursos

2.3.1 Compromiso gerencial

La organización debería asegurar que:

a) se ha establecido, implementado y mantenido un sistema de administración de riesgos, de acuerdo con este Estándar; y
b) se reporta el desempeño del sistema de administración de riesgos a la gerencia de la organización para revisión y como base para su mejora.

2.3.2 Responsabilidad y autoridad

Deberá definirse y documentarse la responsabilidad, autoridad e interrelaciones del personal que realiza y verifica el trabajo que afecta la administración de riesgos, particularmente para la gente que necesita la libertad y autoridad organizacional para realizar una o más de las siguientes acciones:

a) iniciar acciones para prevenir o reducir los efectos adversos de los riesgos;
b) controlar el tratamiento posterior de los riesgos hasta que el nivel de riesgo se haga aceptable;
c) identificar y registrar cualquier problema relativo a la administración de riesgos;
d) iniciar, recomendar o proveer soluciones a través de los canales asignados;
e) verificar la implementación de soluciones; y
f) comunicar y consultar interna y externamente según corresponda.

2.3.3 Recursos

La organización debe identificar los requerimientos de recursos y proveer recursos adecuados, incluyendo la asignación de personal entrenado para las actividades de administración, desempeño del trabajo, y verificación incluyendo la revisión interna.

2.4 Programa de implementación

Se requiere seguir una cantidad de pasos para implementar un sistema efectivo de administración de riesgos dentro de una organización. En el Apéndice B se proveen ejemplos. Dependiendo de la filosofía, cultura y estructura general de administración de riesgos de la organización, debería ser posible combinar u omitir ciertos pasos. Sin embargo, deberían considerarse todos los pasos.

2.5 Revisión gerencial

El ejecutivo de la organización debe asegurar que se lleve a cabo una revisión del sistema de administración de riesgos a intervalos especificados, suficiente para asegurar su continua conformidad y efectividad para satisfacer los requerimientos de este Estándar, y las políticas y objetivos de administración de riesgos establecidos en la organización (ver Cláusula 2.2). Deberá llevarse un registro de tales revisiones.

3 Vista general de la administración de riesgos

3.1 General

La administración de riesgos es una parte integral del proceso de administración. La administración de riesgos es un proceso multifacético, aspectos apropiados del cual son a menudo llevados a cabo mejor por un equipo multidisciplinario. Es un proceso iterativo de mejora continua.

3.2 Elementos principales

Los elementos principales del proceso de administración de riesgos, como se muestra en la figura Figura 3.1, son los siguientes:

a) Establecer el contexto

Establecer el contexto estratégico, organizacional y de administración de riesgos en el cual tendrá lugar el resto del proceso. Deberían establecerse criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.

b) Identificar riesgos

Identificar qué, por qué y cómo pueden surgir las cosas como base para análisis posterior.

c) Analizar riesgos

Determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que ocurran esas consecuencias. Consecuencias y probabilidades pueden ser combinadas para producir un nivel estimado de riesgo.

d) Evaluar riesgos

Comparar niveles estimados de riesgos contra los criterios preestablecidos.

Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de administración. Si los niveles de riesgo establecidos son bajos, los riesgos podrían caer en una categoría aceptable y no se requeriría un tratamiento.

e) Tratar riesgos

Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo.

f) Monitorear y revisar

Monitorear y revisar el desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.

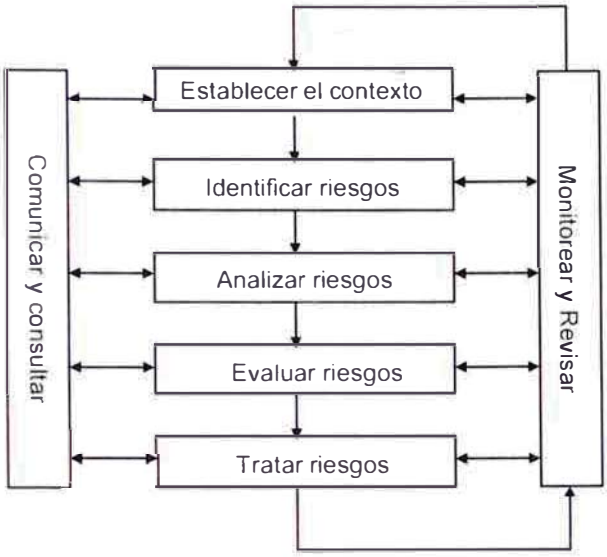
g) Comunicar y consultar

Comunicar y consultar con interesados internos y externos según corresponda en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.

La administración de riesgos se puede aplicar en una organización a muchos niveles. Se lo puede aplicar a nivel estratégico y a niveles operativos. Se lo puede aplicar a proyectos específicos, para asistir con decisiones específicas o para administrar áreas específicas reconocidas de riesgo.

La administración de riesgos es un proceso iterativo que puede contribuir a la mejora organizacional. Con cada ciclo, los criterios de riesgos se pueden fortalecer para alcanzar progresivamente mejores niveles de administración de riesgos.

Para cada etapa del proceso deberían llevarse registros adecuados, suficientes como para satisfacer a una auditoria independiente.



3.1 Vista General de la Administración de Riesgos

4 Proceso de administración de riesgos

4.1 Establecer el contexto

4.1.1 General

En la Figura 4.1 se muestran los detalles del proceso de administración de riesgos. El proceso ocurre dentro de la estructura del contexto estratégico, organizacional y de administración de riesgos de una organización. Esto necesita ser establecido para definir los parámetros básicos dentro de los cuales deben administrarse los riesgos y para proveer una guía para las decisiones dentro de estudios de administración de riesgos más detallados. Esto establece el alcance para el resto del proceso de administración de riesgos.

4.1.2 Establecer el contexto estratégico

Definir la relación entre la organización y su entorno, identificando las fortalezas, debilidades, oportunidades y amenazas de la organización. El contexto incluye los aspectos financieros, operativos, competitivos, políticos (percepciones públicas / imagen), sociales, de clientes, culturales y legales de las funciones de la organización.
Identificar los interesados internos y externos, y considerar sus objetivos, tomar en cuenta sus percepciones, y establecer políticas de comunicación con estas partes.

nota: El apéndice C establece una lista de interesados potenciales. Este paso está focalizado en el entorno en el cual opera la organización. La organización debería buscar determinar los elementos cruciales que podrían sustentar o dificultar su habilidad para administrar los riesgos que enfrenta. Puede llevarse a cabo un análisis estratégico. El mismo debería ser endosado al nivel ejecutivo, para que establezca los parámetros básicos y provea una guía en los procesos más detallados de administración de riesgos. Debería existir una estrecha relación entre la misión u objetivos estratégicos de una organización y la administración de todos los riesgos a los cuales está expuesta.

4.1.3 Establecer el contexto organizacional

Antes de comenzar un estudio de administración de riesgos, es necesario comprender la organización y sus capacidades, así como sus metas y objetivos y las estrategias que están vigentes para lograrlos.
Esto es importante por las siguientes razones:

a) La administración de riesgos tiene lugar en el contexto de las amplias metas, objetivos y estrategias de la organización;
b) La falla en lograr los objetivos de la organización, o de una actividad específica, o proyecto en consideración, es un conjunto de riesgos que debería ser administrado;
c) La política y metas de la organización ayudan a definir los criterios mediante los cuales se decide si un riesgo es aceptable o no, y constituye la base para las opciones de tratamientos.

4.1.4 Establecer el contexto de administración de riesgos

Deberían establecerse las metas, objetivos, estrategias, alcance y parámetros de la actividad, o parte de la organización a la cual se está aplicando el proceso de administración de riesgos. El proceso debería ser llevado a cabo con plena consideración de la necesidad de balancear costos, beneficios y oportunidades.

También deberían especificarse los recursos requeridos y los registros que se van a llevar.
Establecer el alcance y los límites de una aplicación del proceso de administración de riesgos involucra:

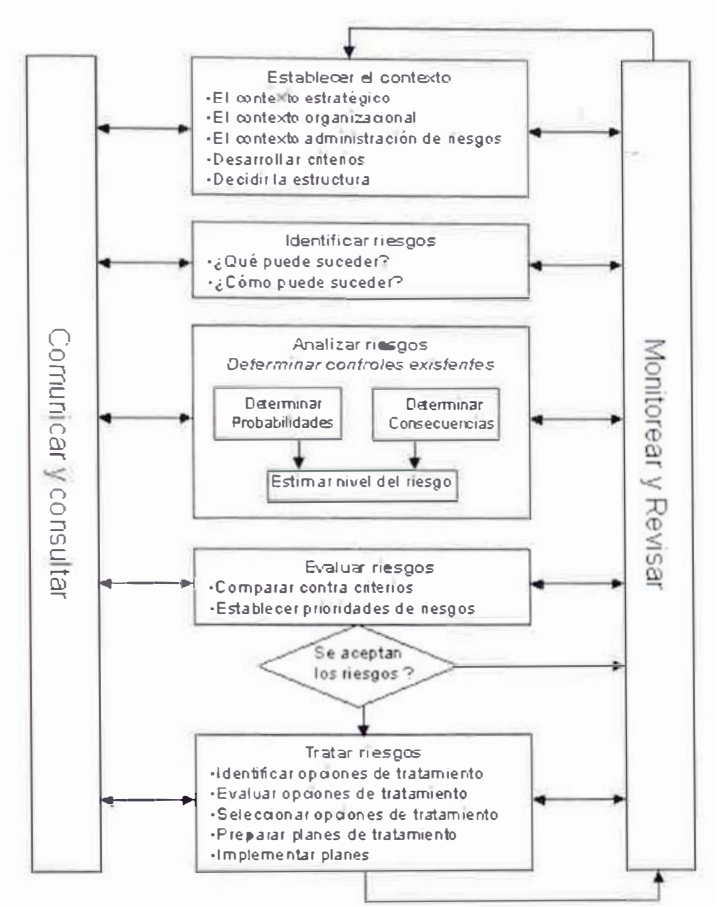
a) Definir el proyecto o actividad y establecer sus metas y objetivos;
b) Definir la extensión del proyecto en tiempo y ubicación;
c) Identificar cualquier estudio necesario y su alcance, objetivos y recursos requeridos. Pueden proveer una guía para esto las fuentes genéricas de riesgo y las áreas de impacto.
   nota: Para obtener ejemplos de fuentes genéricas de riesgo y sus áreas de impacto consultar el Apéndice D.
d) Definir el alcance y amplitud de las actividades de administración de riesgos a llevar a cabo.
   Los aspectos específicos que también podrían ser discutidos incluyen lo siguiente:
   i. Los roles y responsabilidades de las distintas partes de la organización que participan en la administración de riesgos;
   ii. Las relaciones entre el proyecto y otros proyectos o partes de la organización.

4.1.5 Desarrollar criterios de evaluación de riesgos

Decidir los criterios contra los cuales se va a evaluar el riesgo. Las decisiones concernientes a aceptabilidad de riesgos y tratamiento de riesgos pueden basarse en criterios operativos, técnicos, financieros, legales, sociales, humanitarios u otros. Esto a menudo depende de las políticas, metas y objetivos internos de la organización y de los intereses de las demás partes interesadas.
Los criterios pueden estar afectados por percepciones internas y externas y por requerimientos legales. Es importante que los criterios apropiados sean determinados al comienzo.
Aunque los criterios de riesgo son inicialmente desarrollados como parte del establecimiento del contexto de administración de riesgos, los mismos pueden ser posteriormente desarrollados y refinados a medida que se identifican riesgos particulares y se seleccionan técnicas de análisis de riesgos, ej: los criterios de riesgo deben corresponder al tipo de riesgos y a la forma en que se expresan los niveles de riesgo.

4.1.6 Definir la estructura

Esto involucra separar la actividad o proyecto en un conjunto de elementos.
Estos elementos proveen una estructura lógica para identificación y análisis lo cual ayuda a asegurar que no se pasen por alto riesgos significativos. La estructura seleccionada depende de la naturaleza de los riesgos y del alcance del proyecto o actividad.



4.1 Proceso de Administración de Riesgo

4.2 Identificación de riesgos

4.2.1 General

Este paso busca identificar los riesgos a administrar. Es crítica una identificación amplia utilizando un proceso sistemático bien estructurado, porque los riesgos potenciales que no se identifican en esta etapa son excluidos de un análisis posterior. La identificación debería incluir todos los riesgos, estén o no bajo control de la organización.

4.2.2 Qué puede suceder

La intención es generar una lista amplia de eventos que podrían afectar a cada elemento de la estructura referida en la Cláusula 4.1.6. Estos son luego considerados en mayor detalle para identificar lo que puede suceder.

nota: El apéndice D provee información sobre las fuentes genéricas de riesgo y sus áreas de impacto.

4.2.3 Cómo y por qué pueden suceder

Habiendo identificado una lista de eventos, es necesario considerar causas y escenarios posibles. Hay muchas formas en que se puede iniciar un evento. Es importante que no se omitan las causas significativas.

4.2.4 Herramientas y técnicas

Los enfoques utilizados para identificar riesgos incluyen "*checklists*", juicios basados en la experiencia y en los registros, diagramas de flujo, "*brainstorming*", análisis de sistemas, análisis de escenarios y técnicas de ingeniería de sistemas.
El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgos.

4.3 Análisis de riesgos

4.3.1 General

Los objetivos de análisis son separar los riesgos menores aceptables de los riesgos mayores, y proveer datos para asistir en la evaluación y tratamiento de los riesgos. El análisis de riesgos involucra prestar consideración a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias. Pueden identificarse los factores que afectan a las consecuencias y probabilidades. Se analiza el riesgo combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes.
Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se realizó un análisis de riesgos completo.

4.3.2 Determinar los controles existentes

Identificar la administración, sistemas técnicos y procedimientos existentes para controlar los riesgos y evaluar sus fortalezas y debilidades. Pueden ser apropiadas las herramientas utilizadas en 4.2.4, como asimismo los enfoques tales como inspecciones y técnicas de auto-evaluación de controles ('CSA').

4.3.3 Consecuencias y probabilidades

La magnitud de las consecuencias de un evento, si el mismo ocurriera, y la probabilidad del evento y sus consecuencias asociadas, se evalúan en el contexto de los controles existentes. Las consecuencias y probabilidades se combinan para producir un nivel de riesgo. Se pueden determinar las consecuencias y probabilidades utilizando análisis y cálculos estadísticos. Alternativamente cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular.
Para evitar prejuicios subjetivos cuando se analizan consecuencias y probabilidades, deberían utilizarse las mejores técnicas y fuentes de información disponibles.
Se pueden incluir las siguientes fuentes de información:

a) Registros anteriores;
b) Experiencia relevante;
c) Prácticas y experiencia de la industria;
d) Literatura relevante publicada;
e) Comprobaciones de *marketing* e investigaciones de mercado;
f) Experimentos y prototipos;
g) Modelos económicos, de ingeniería u otros;
h) Opiniones y juicios de especialistas y expertos.

Las técnicas incluyen:

i) entrevistas estructuradas con expertos en el área de interés·
ii) utilización de grupos multidisciplinarios de expertos;
iii) evaluaciones individuales utilizando cuestionarios·
iv) uso de modelos de computador u otros; y
v) uso de árboles de fallas y árboles de eventos.

Siempre que sea posible, debería incluirse el nivel de confianza asignado a las estimaciones de los niveles de riesgo.

4.3.4 Tipos de análisis

El análisis de riesgos pueden ser llevado con distintos grados de refinamiento dependiendo de la información de riesgos y datos disponibles. Dependiendo de las circunstancias, el análisis puede ser cualitativo, semi-cuantitativo o cuantitativo o una combinación de estos. El orden de complejidad y costos de estos análisis en orden ascendente, es cualitativo, semi-cuantitativo y cuantitativo. En la práctica, a menudo se utiliza primero el análisis cualitativo para obtener una indicación general del nivel de riesgo. Luego puede ser necesario llevar a cabo un análisis cuantitativo más específico. El detalle de los tipos de análisis es el siguiente:

a) Análisis cualitativo

El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran. Estas escalas se pueden modificar o ajustar para adaptarlas a las circunstancias, y se pueden utilizar distintas descripciones para riesgos diferentes.

nota: Las tablas E1 y E2 del Apéndice E muestran ejemplos de escalas simples cualitativas o descriptivas para probabilidades y consecuencias. La tabla E3 es un ejemplo de una matriz en la cual los riesgos están asignados a clases de prioridad mediante la combinación de su probabilidad y consecuencia. Se necesita adaptar estas tablas para satisfacer las necesidades de una organización individual o la materia particular de evaluación de riesgos.

El análisis cualitativo se utiliza:

i. como una actividad inicial de tamiz, para identificar los riesgos que requieren un análisis más detallado;
ii. cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo; o
iii. cuando los datos numéricos son inadecuados para un análisis cuantitativo.

b) Análisis semi-cuantitativo

En el análisis semi-cuantitativo, a las escalas cualitativas, tales como las descriptas arriba, se les asignan valores. El número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades. Los números pueden ser combinados en cualquier rango de fórmula dado que el sistema utilizado para priorizar confronta el sistema seleccionado para asignar números y combinarlos. El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo, y no sugerir valores realistas para los riesgos tales como los que se procuran en el análisis cuantitativo.

Se debe tener cuidado con el uso del análisis semi-cuantitativo porque los números seleccionados podrían no reflejar apropiadamente las relatividades, lo que podría conducir a resultados inconsistentes. El análisis semi-cuantitativo puede no diferenciar apropiadamente entre distintos riesgos, particularmente cuando las consecuencias o las probabilidades son extremas.

A veces es apropiado considerar la probabilidad compuesta de dos elementos, a los que se refiere generalmente como frecuencia de la exposición y probabilidad.
Frecuencia de la exposición es la extensión a la cual una fuente de riesgo existe, y probabilidad es la chance de que, cuando existe esa fuente de riesgo, le seguirán las consecuencias. Deberá ejercerse precaución en las situaciones en que las relaciones entre los dos elementos no es completamente independiente, ej. Cuando hay una fuerte relación entre frecuencia de la exposición y la probabilidad.
Este enfoque se puede aplicar en el análisis semi-cuantitativo y cuantitativo.

c) Análisis cuantitativo

El análisis cuantitativo utiliza valores numericos para las consecuencias y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos y semi-cuantitativos) utilizando datos de distintas fuentes (tales como las mencionadas en los sub-párrafos (a) a (h) de la Cláusula 4.3.3). La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados.
Las consecuencias pueden ser estimadas modelando los resultados de un evento o conjunto de eventos, o extrapolando a partir de estudios experimentales o datos del pasado. Las consecuencias pueden ser expresadas en términos de criterios monetarios, técnicos o humanos, o cualquier otro criterio referido en la Cláusula 4.1.5. En algunos casos se requiere más de un valor numérico para especificar las consecuencias para distintos momentos, lugares, grupos o situaciones.
La probabilidad es expresada generalmente como una probabilidad, una frecuencia, o una combinación de exposición y probabilidad.
La forma en que se expresan las probabilidades y las consecuencias y las formas en que las mismas son combinadas para proveer un nivel de riesgo variarán de acuerdo con el tipo de riesgo y el contexto en el cual se va a utilizar el nivel de riesgo.

nota: En el Apéndice F se brindan algunos ejemplos de expresiones de riesgo cuantitativo.

4.3.5 Análisis de sensibilidad

Dado que algunas de las estimaciones realizadas en el análisis cuantitativo son imprecisas, deberá llevarse a cabo un análisis de sensibilidad para comprobar el efecto de los cambios en los supuestos y en los datos.

4.4 Evaluación de riesgos

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.
El análisis de riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación de riesgos deberían considerarse sobre la misma base. En consecuencia, la evaluación cualitativa involucra la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y la evaluación cuantitativa involucra la comparación de un nivel numérico de riesgo contra criterios que pueden ser expresados como un número específico, tal como, un valor de fatalidad, frecuencia o monetario.
El producto de una evaluación de riesgo es una lista de riesgos con prioridades para una acción posterior.
Deberían considerarse los objetivos de la organización y el grado de oportunidad que podrían resultar de tomar el riesgo.
Las decisiones deben tener en cuenta el amplio contexto del riesgo e incluir consideración de la tolerabilidad de los riesgos sostenidos por las partes fuera de la organización que se benefician de ellos.

Si los riesgos resultantes caen dentro de las categorías de riesgos bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Los riesgos bajos y aceptados deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen aceptables.
Si los riesgos no caen dentro de la categoría de riesgos bajos o aceptables, deberían ser tratados utilizando una o más de las opciones consideradas en la Cláusula 4.5.

4.5 Tratamiento de los riesgos

El tratamiento de los riesgos involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

4.5.1 Identificar opciones para tratamiento de los riesgos

La Figura 4.2 ilustra el proceso de tratamiento de los riesgos. Las opciones, que no son necesariamente mutuamente exclusivas y apropiadas en todas las circunstancias, incluyen lo siguiente:

a) Evitar el riesgo decidiendo no proceder con la actividad que probablemente generaría el riesgo (cuando esto es practicable).
Evitar riesgos puede ocurrir inadecuadamente por una actitud de aversión al riesgo, que es una tendencia en mucha gente (a menudo influenciada por el sistema interno de una organización). Evitar inadecuadamente algunos riesgos puede aumentar la significación de otros.

La aversión a riesgos tiene como resultado:

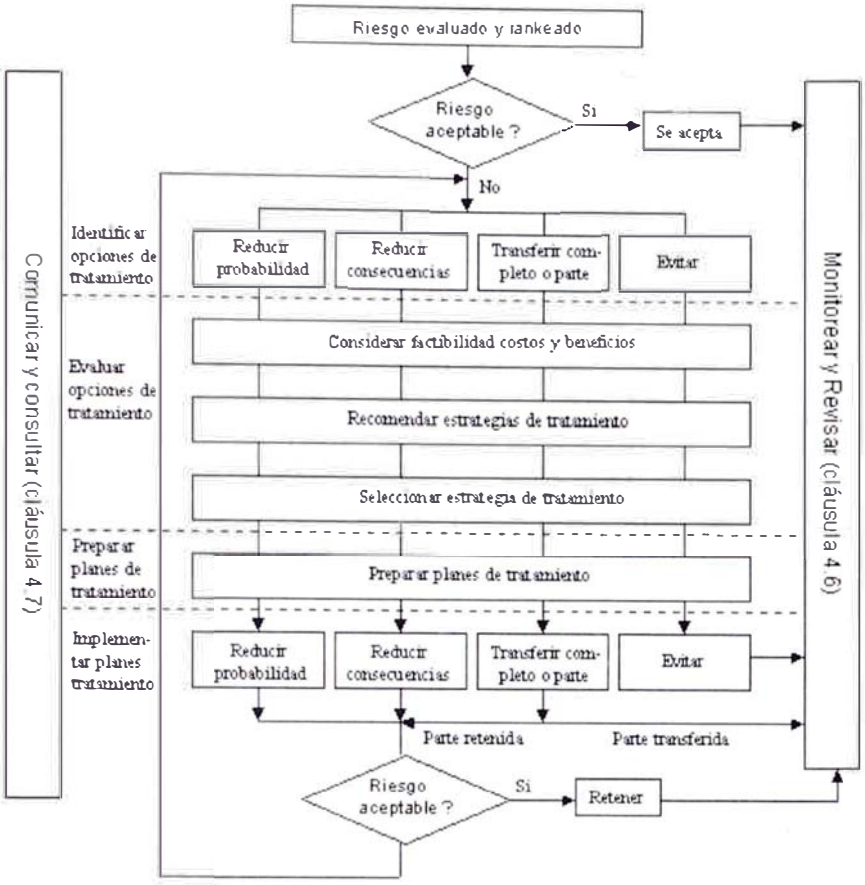
i) decisiones de evitar o ignorar riesgos independientemente de la información disponible y de los costos incurridos en el tratamiento de esos riesgos.
ii) fallas en tratar los riesgos;
iii) dejar las opciones críticas y/o decisiones en otras partes;
iv) diferir las decisiones que la organización no puede evitar; o
v) seleccionar una opción porque representa un riesgo potencial más bajo independientemente de los beneficios.

b) Reducir la probabilidad de la ocurrencia
nota: Se muestran ejemplos en el Apéndice G.

c) Reducir las consecuencias
nota: Se muestran ejemplos en el Apéndice G.

d) Transferir los riesgos
Esto involucra que otra parte soporte o comparta parte del riesgo. Los mecanismos incluyen el uso de contratos, arreglos de seguros y estructuras organizacionales tales como sociedades y *"joint ventures"*.
La transferencia de un riesgo a otras partes, o la transferencia física a otros lugares, reducirá el riesgo para la organización original, pero puede no disminuir el nivel general del riesgo para la sociedad.
Cuando los riesgos son total o parcialmente transferidos, la organización que transfiere los riesgos ha adquirido un nuevo riesgo, que la organización a la cual ha transferido el riesgo no pueda administrarlo efectivamente.

e) Retener los riesgos
Luego de que los riesgos hayan sido reducidos o transferidos, podría haber riesgos residuales que sean retenidos. Deberían ponerse en práctica planes para administrar las consecuencias de esos riesgos si los mismos ocurrieran, incluyendo identificar medios de financiar dichos riesgos. Los riesgos también pueden ser retenidos en forma predeterminada, ej. cuando hay una falla para identificar y/o transferir apropiadamente o de otro modo tratar los riesgos.

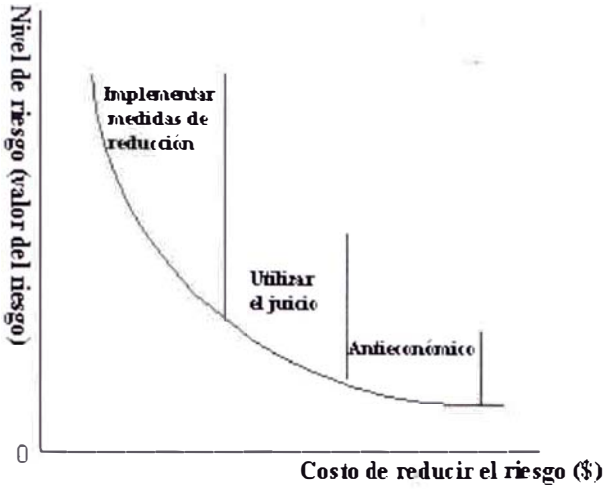


4.2 Proceso de Tratamiento de Riesgos

A la reducción de las consecuencias y probabilidades se las puede referir como control de riesgos. El control de riesgos involucra determinar el beneficio relativo de nuevos controles a la luz de la efectividad de los controles existentes. Los controles pueden involucrar políticas de efectividad, procedimientos o cambios físicos.

4.5.2 Evaluar opciones de tratamiento de los riesgos

Las opciones deberían ser evaluadas sobre la base del alcance de la reducción del riesgo, y el alcance de cualquier beneficio u oportunidad adicional creadas, tomando en cuenta los criterios desarrollados en la Cláusula 4.1.5. Pueden considerarse y aplicarse una cantidad de opciones ya sea individualmente o combinadas.
La selección de la opción más apropiada involucra balancear el costo de implementar cada opción contra los beneficios derivados de la misma. En general, el costo de administrar los riesgos necesita ser conmensurada con los beneficios obtenidos.
Cuando se pueden obtener grandes reducciones en el riesgo con un gasto relativamente bajo, tales opciones deberían implementarse. Otras opciones de mejoras pueden ser no económicas y necesita ejercerse el juicio para establecer si son justificables. Esto se ilustra en la Figura 4.3.
Las decisiones deberían tener en cuenta la necesidad de considerar cuidadosamente los riesgos raros pero severos, que podrían justificar medidas de seguridad que no son justificables por fundamentos estrictamente económicos.



4.3 Costo de las Medidas de Reducción de Riesgos

En general el impacto adverso de los riesgos debería hacerse tan bajo como sea razonablemente practicable, independientemente de cualquier criterio absoluto.
Si el nivel de riesgo es alto, pero podrían resultar oportunidades considerables si se lo asume, tal como el uso de una nueva tecnología, entonces la aceptación del riesgo necesita estar basada en una evaluación de los costos de tratamiento y los costos de rectificar las consecuencias potenciales versus las oportunidades que podrían depararse de tomar el riesgo.
En muchos casos, es improbable que cualquier opción de tratamiento del riesgo sea una solución completa para un problema particular. A menudo la organización se beneficiará sustancialmente mediante una combinación de opciones tales como reducir la probabilidad de los riesgos, reducir sus consecuencias, y transferir o retener algunos riesgos residuales. Un ejemplo es el uso efectivo de contratos y la financiación de riesgos sustentados por un programa de reducción de riesgos.
Cuando el costo acumulado de implementación de todos los tratamientos de riesgos excede el presupuesto disponible, el plan debería identificar claramente el orden de prioridad bajo el cual deberían implementarse los tratamientos individuales de los riesgos. El ordenamiento de prioridad puede establecerse utilizando distintas técnicas, incluyendo análisis de *"ranking"* de riesgos y de costo-beneficio. Los tratamientos de riesgos que no puedan ser implementados dentro de los límites del presupuesto disponible deben esperar la disponibilidad de recursos de financiamiento adicionales, o, si por cualquier razón todos o algunos de los tratamientos restantes son considerados importantes, debe plantearse el problema para conseguir el financiamiento adicional.
Las opciones de tratamiento de los riesgos deberían considerar cómo es percibido el riesgo por las partes afectadas y las formas más apropiadas de comunicárselo a dichas partes.

4.5.3 Preparar planes de tratamiento

Los planes deberían documentar cómo deben ser implementadas las opciones seleccionadas.
El plan de tratamiento debería identificar las responsabilidades, el programa, los resultados esperados de los tratamientos, el presupuesto, las medidas de desempeño y el proceso de revisión a establecer.
nota: Para mayores detalles consultar Parte H5, Apéndice H.
El plan también debería incluir un mecanismo para evaluar la implementación de las opciones contra criterios de desempeño, las responsabilidades individuales y otros objetivos, y para monitorear los mojones críticos de implementación.

Figura 4.3 Costo de las medidas de reducción de riesgos.

4.5.4 Implementar planes de tratamiento

Idealmente, la responsabilidad por el tratamiento del riesgo debería ser llevada a cabo por aquellos con mejor posibilidad de controlar el riesgo. Las responsabilidades deberían ser acordadas entre las partes en el momento más temprano posible.
La implementación exitosa del plan de tratamiento del riesgo requiere un sistema efectivo de administración que especifique los métodos seleccionados, asigne responsabilidades y compromisos individuales por las acciones, y los monitoree respecto de criterios especificados.
Si luego del tratamiento hay un riesgo residual, debería tomarse la decisión de si retener este riesgo o repetir el proceso de tratamiento.

4.6 Monitoreo y revisión

Es necesario monitorear los riesgos, la efectividad del plan de tratamiento de los riesgos, las estrategias y el sistema de administración que se establece para controlar la implementación. Los riesgos y la efectividad de las medidas de control necesitan ser monitoreadas para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos. Pocos riesgos permanecen estáticos.
Es esencial una revisión sobre la marcha para asegurar que el plan de administración se mantiene relevante. Pueden cambiar los factores que podrían afectar las probabilidades y consecuencias de un resultado, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos. La revisión es una parte integral del plan de tratamiento de la administración de riesgos.

4.7 Comunicación y consulta

La comunicación y consulta son una consideración importante en cada paso del proceso de administración de riesgos. Es importante desarrollar un plan de comunicación para los interesados internos y externos en la etapa más temprana del proceso. Este plan debería encarar aspectos relativos al riesgo en si mismo y al proceso para administrarlo.
La comunicación y consulta involucra un diálogo en ambas direcciones entre los interesados, con el esfuerzo focalizado en la consulta más que un flujo de información en un sólo sentido del tomador de decisión hacia los interesados.
Es importante la comunicación efectiva interna y externa para asegurar que aquellos responsables por implementar la administración de riesgos, y aquellos con intereses creados comprenden la base sobre la cual se toman las decisiones y por qué se requieren ciertas acciones en particular.
Las percepciones de los riesgos pueden variar debido a diferencias en los supuestos, conceptos, las necesidades, aspectos y preocupaciones de los interesados, según se relacionen con el riesgo o los aspectos bajo discusión. Los interesados probablemente harán juicios de aceptabilidad de los riesgos basados en su percepción de los mismos.
Dado que los interesados pueden tener un impacto significativo en las decisiones tomadas, es importante que sus percepciones de los riesgos, así como, sus percepciones de los beneficios, sean identificadas y documentadas y las razones subyacentes para las mismas comprendidas y tenidas en cuenta.

5 Documentación

5.1 General

Debería documentarse cada etapa del proceso de administración de riesgos.
La documentación debería incluir los supuestos, los métodos, las fuentes de datos y los resultados.

5.2 Razones para la documentación

Las razones para la documentación son las siguientes:

a) demostrar que el proceso es conducido apropiadamente;
b) proveer evidencia de un enfoque sistemático de identificación y análisis de riesgos;
c) proveer un registro de los riesgos y desarrollar la base de datos de conocimientos de la organización;
d) proveer a los tomadores de decisión relevantes de un plan de administración de riesgos para aprobación y subsiguiente implementación;
e) proveer un mecanismo y herramienta de responsabilidad;
f) facilitar el continuo monitoreo y revisión;
g) proveer una pista de auditoria; y
h) compartir y comunicar información.

Las decisiones concernientes al alcance de la documentación pueden involucrar costos y beneficios y deberían tomar en consideración los factores mencionados arriba.
Guía: Para asistir y dar alguna guía acerca de la documentación apropiada, se proveen ejemplos en el Apéndice H. Estos ejemplos son indicativos más que comprensivos.

Aplicaciones de la administración de riesgos

A1 Organizaciones

Este Estándar puede aplicarse a un rango muy amplio de organizaciones incluyendo:

a) públicas:
- nacionales, regionales, locales;

b) comerciales:
- compañías, "*joint ventures*", firmas, franquicias, prácticas exclusivas; y

c) voluntarias:
- de caridad, sociales, deportivas.

A2 Aplicaciones

El Estándar tiene un amplio rango de aplicaciones incluyendo, pero no circunscrito a:

i) administración de activos y planeamiento de recursos;
ii) interrupción del negocio;
iii) cambios: organizacionales, tecnológicos y políticos;
iv) actividad de construcción;
v) planeamiento de contingencia, para desastres y emergencias;
vi) responsabilidades de diseño y producto;
vii) responsabilidades de directores y funcionarios;
viii) procedimientos, entrenamiento, discriminación y acoso en empleos;
ix) aspectos ambientales;
x) aspectos éticos y de probidad;
xi) estudios de factibilidad;
xii) detección de incendios / prevención de incendios;
xiii) operaciones de cambio monetario;
xiv) prevención, detección y administración de fraudes;
xv) sanidad humana, animal y vegetal;
xvi) sistemas de información / redes de computación;
xvii) inversiones;
xviii) cumplimiento legislativo;
xix) salud y seguridad ocupacional;
xx) sistemas de operaciones y mantenimiento;
xxi) administración de proyectos;
xxii) riesgo público y responsabilidad general;
xxiii) administración de contratos de compra;
xxiv) asesoramiento profesional;
xxv) aspectos de reputación e imagen;
xxvi) seguridad;
xxvii) transporte incluyendo aire, mar, carretera, ferrocarril; y
xxviii) tesorería y finanzas.

B Pasos en el desarrollo e implementación de un programa de administración de riesgos

Paso 1: Respaldo de la alta gerencia

Desarrollar una filosofía de administración de riesgos organizacional y toma de conciencia sobre 'riesgos' a nivel de la alta gerencia. Esto podría ser facilitado mediante entrenamiento, educación y síntesis a la gerencia ejecutiva.

- Es necesario el apoyo permanentemente activo del Presidente (*CEO*) de la organización.
- Se necesita que patrocine la iniciativa un gerente ejecutivo principal o un "campeón" similar (o un grupo).
- Todos los ejecutivos principales deben dar pleno apoyo.

Paso 2: Desarrollar la política organizacional

Desarrollar y documentar una política y estructura corporativa para administrar los riesgos, a ser endosada por el ejecutivo de la organización e implementada en toda la organización. La política debe incluir información tal como:

- los objetivos de la política y explicación para administrar los riesgos;
- los vínculos entre la política y el plan estratégico / corporativo de la organización;
- el alcance, o el rango de aspectos a los cuales se aplica la política;
- guía de lo que puede ser considerado como riesgo aceptable;
- quién es responsable por administrar riesgos;
- el apoyo / capacidad disponibles para asistir a los responsables de administrar riesgos;
- el nivel de documentación requerido; y
- el plan para revisar el desempeño organizacional en relación con la política.

Paso 3: Comunicar la política

Desarrollar, establecer e implementar una infraestructura o medidas para asegurar que la administración de riesgos se convierte en una parte integral de los procesos de planeamiento y administración y de la cultura general de la organización. Esto puede incluir:

- establecer un equipo que comprenda personal de alta gerencia para ser responsable por las comunicaciones internas acerca de la política;
- procurar la toma de conciencia acerca de la administración de riesgos;
- comunicación / diálogo en toda la organización acerca de administración de riesgos y la política de la organización;
- adquirir pericia en administración de riesgos, ej: consultores, y desarrollar destrezas en el personal a través de la educación y capacitación;
- asegurar niveles apropiados de reconocimiento, recompensas y sanciones; y
- establecer procesos de administración de desempeño.

Paso 4: Administrar riesgos a nivel organizacional

Desarrollar y establecer un programa para administrar riesgos a nivel organizacional a través de la aplicación del sistema de administración de riesgos descrito en la Sección 2. El proceso de

administración de riesgos debería estar integrado con los procesos de planeamiento estratégico y administración de la organización. Esto involucrará documentar:

- el contexto de la organización y de la administracion de riesgos;
- los riesgos identificados para la organización;
- el análisis y evaluación de estos riesgos;
- las estrategias de tratamiento;
- los mecanismos para revisar el programa; y
- las estrategias para procurar la toma de conciencia, la adquisición de pericia, la capacitación y la educación.

Paso 5: Administrar riesgos a nivel de programa, proyecto y equipo

Desarrollar y establecer un programa para administrar los riesgos para cada área sub-organizacional, programa, proyecto o actividad de equipo a través de la aplicación del proceso de administración de riesgos descrito en la Sección 4. El proceso para administrar riesgos debería estar integrado con otras actividades de planeamiento y administración. Debería documentarse el proceso seguido, las decisiones tomadas y las acciones planeadas.

Paso 6: Monitorear y revisar

Desarrollar y aplicar mecanismos para asegurar revisiones de los riesgos sobre la marcha. Esto asegurará que la implementación y la política de administración de riesgos se mantenga relevante, dado que las circunstancias cambian todo el tiempo y se hace vital la revisión de las decisiones anteriores. Los riesgos no son estáticos. También debería monitorearse y revisarse la efectividad del proceso de administración de riesgos.

C Interesados

Interesados son aquellos individuos que están, o perciben estar, afectados por una decisión o actividad. Ellos pueden incluir:

- individuos dentro de la organización, tales como los empleados, la gerencia, la alta gerencia, y voluntarios;
- tomadores de decisiones;
- contrapartes de negocios o comerciales;
- grupos de empleados;
- grupos sindicales;
- instituciones financieras;
- organizaciones de seguros;
- reguladores y otras organizaciones gubernamentales que tienen autoridad sobre las actividades;
- políticos (a todos los niveles del gobierno) que pudieran tener un interés electoral o de cartera;
- organizaciones no-gubernamentales tales como grupos ambientales y grupos de interés público;
- clientes;
- proveedores, proveedores de servicios y contratistas para la actividad;
- los medios, que son interesados potenciales, como también, conductos de información a otros interesados;
- individuos o grupos que están interesados en aspectos relacionados con la propuesta;
- comunidades locales; y
- la sociedad como un todo.

La mezcla de interesados puede cambiar con el tiempo. Nuevos interesados pueden unirse y desear ser considerados, mientras que otros podrían quedar excluidos al no estar más involucrados en el proceso. Consecuentemente, el proceso de análisis de interesados debería ser continuo, y como tal, debería ser parte integrante del proceso de administración de riesgos.

El nivel de preocupación de los interesados puede cambiar en respuesta a nueva información, ya sea porque se han encarado las necesidades y preocupaciones de los interesados, o porque nueva información ha dado lugar a nuevas necesidades, aspectos o preocupaciones. Nótese también que distintos interesados podrían tener diferentes opiniones y diferentes niveles de conocimiento en relación a un aspecto en particular.

D Fuentes genéricas de riesgo y sus áreas de impacto

D1 General

La identificación de fuentes de riesgo y áreas de impacto provee una estructura para identificación y análisis de riesgos. A raíz de la gran cantidad potencial de fuentes e impactos, desarrollar una lista genérica focaliza las actividades de identificación de riesgos y contribuye a una administración más efectiva.
Las fuentes de riesgo y áreas de impacto genéricas son seleccionadas de acuerdo a su relevancia para la actividad bajo estudio (ver Cláusulas 4.1.4 y 4.2.2).
Los componentes de cada categoría genérica pueden formar la base para un estudio completo de riesgos.

D2 Fuentes de riesgo

Cada fuente genérica tiene numerosos componentes, cualquier de los cuales pueden dar lugar a un riesgo. Algunos componentes estarán bajo control de la organización que realiza el estudio, mientras que otros estarán fuera de su control. Cuando se identifican los riesgos se necesita considerar a ambos tipos. Las fuentes genéricas de riesgo incluyen:

a) Relaciones comerciales y legales
   Entre la organización y otras organizaciones, ej: proveedores, subcontratistas, arrendatarios.
b) Circunstancias económicas
   De la organización, país, internacionales, como asimismo factores que contribuyen a esas circunstancias ej: tipos de cambio.
c) Comportamiento humano
   Tanto de los involucrados en la organización como de los que no lo están.
d) Eventos naturales
e) Circunstancias políticas
   Incluyendo cambios legislativos y factores que pudieran influenciar a otras fuentes de riesgo.
f) Aspectos tecnológicos y técnicos
   Tanto internos como externos a la organización.
g) Actividades y controles gerenciales
h) Actividades individuales

D3 Áreas de impacto

El análisis de riesgo se puede concentrar en impactos en un área solamente o en varias áreas posibles de impacto.

Las áreas de impacto incluyen a las siguientes:

a) Base de activos y recursos de la organización, incluyendo al personal.
b) Ingresos y derechos
c) Costos de las actividades, tanto directos como indirectos.
d) Gente

e) Comunidad
f) Desempeño
g) Cronograma y programa de actividades
h) El ambiente
i) Intangibles tales como la reputación, gestos de buena voluntad, calidad de vida.
j) Comportamiento organizacional

D4 Identificación de riesgos

Un método de resumir la forma en la cual surgen los riesgos en una organización es utilizando una plantilla de identificación de riesgos del tipo que se muestra en la Tabla D1. Las entradas pueden realizarse con marcas para mostrar donde ocurren los riesgos, o con notas descriptivas más detalladas.

D5 Otras clasificaciones de riesgo

Distintas disciplinas a menudo categorizan las fuentes de riesgo de otra forma, utilizando términos tales como azares o exposiciones de riesgo. Estas clasificaciones pueden ser subconjuntos de las fuentes de riesgo listadas arriba en D2. Los siguientes son algunos ejemplos:

a) Enfermedades
ej: afectando a humanos, animales y plantas.
b) Económicos
ej: fluctuaciones en la moneda, tasas de interés, mercado accionario.
c) Ambientales
ej: ruidos, contaminación, polución.
d) Financieros
ej: riesgos contractuales, malversaciones de fondos, fraudes, multas.
e) Humanos
ej: motines, huelgas, sabotajes, errores.
f) Desastres naturales
ej: condiciones climáticas, terremotos, incendios de bosques, plagas, actividad volcánica.
g) Salubridad y seguridad ocupacional
ej: medidas de seguridad inadecuadas, administración de seguridad pobre.
h) Responsabilidad por productos
ej: errores de diseño, calidad bajo estándar, pruebas inadecuadas.
i) Responsabilidad profesional
ej: consejo equivocado, negligencia, error de diseño.
j) Daños a la propiedad
ej: fuego, inundaciones, terremotos, contaminación, error humano.
k) Responsabilidad pública
ej: acceso, egreso y seguridad públicas.
l) Seguridad
ej: desfalcos, vandalismo, robo, apropiación indebida de información, penetración ilegal.
m) Tecnológicos
ej: innovación, obsolescencia, explosiones y dependencia.

Tabla D1 Ejemplo de plantilla de identificación de riesgos.

Fuentes de Riesgo	Areas de Impacto				
	Seleccionar del Párrafo D3 según sea aplicable				
	*	*	*	*	*
Relaciones comerciales y legales					
Económicas					
Comportamiento humano					
Eventos naturales					
Circunstancias políticas					
Aspectos tecnológicos/técnicos					
Actividades y controles gerenciales					
Actividades individuales					

Las fuentes de riesgo y las áreas de impacto deberían adaptarse para la organización o actividad particular

E Ejemplos de definición y clasificación de riesgos.

Tabla E1 Medidas cualitativas de consecuencia o impacto.

Nivel	Descriptor	Ejemplo de descripción detallada
1	Insignificante	Sin perjuicios, baja pérdida financiera
2	Menor	Tratamiento de primeros auxilios, liberado localmente se contuvo inmediatamente, pérdida financiera media
3	Moderado	Requiere tratamiento médico, liberado localmente contenido con asistencia externa, pérdida financiera alta
4	Mayor	Perjuicios extensivos, pérdida de capacidad de producción, liberación externa, sin efectos nocivos, pérdida financiera mayor
5	Catastrófico	Muerte, liberación tóxica externa con efectos nocivos, enorme pérdida financiera

Las medidas utilizadas deberían reflejar las necesidades y naturaleza de la organización y actividad bajo estudio

Tabla E2 Medidas cualitativas de probabilidad.

Nivel	Descriptor	Descripción
A	Casi certeza	Se espera que ocurra en la mayoría de las circunstancias
B	Probable	Probablemente ocurrirá en la mayoría de las circunstancias
C	Posible	Podría ocurrir en algún momento
D	Improbable	Pudo ocurrir en algún momento
E	Raro	Puede ocurrir sólo en circunstancias excepcionales

Estas tablas necesitan ser adaptadas para satisfacer las necesidades de una organización en particular

Tabla E3 Matriz de análisis de riesgo cualitativo – nivel de riesgo.

Probabilidad	Consecuencias				
	Insignificantes 1	Menores 2	Moderadas 3	Mayores 4	Catastróficas 5
A (casi certeza)	H	H	E	E	E
B (probable)	M	H	H	E	E
C (moderado)	L	M	H	E	E
D (improbable)	L	L	M	H	E
E (raro)	L	L	M	H	H

La cantidad de categorías deberían reflejar las necesidades del estudio

Leyenda

E: riesgo extremo; requiere acción inmediata
H: riesgo alto; necesita atención de la alta gerencia
M: riesgo moderado; debe especificarse responsabilidad gerencial
L: riesgo bajo, administrar mediante procedimientos de rutina

F Ejemplos de expresiones cuantitativas de riesgo

F1 Riesgo de pérdida o ganancia financiera

La pérdida (o ganancia) financiera multiplicada por la frecuencia anual de la pérdida (o ganancia) da el valor esperado en dólares por año.

F2 Riesgo de fatalidad

El riesgo de fatalidad de una actividad.

F3 Desastres naturales o producidos por el hombre

Las consecuencias pueden ser modeladas utilizando simulaciones computarizadas y las probabilidades estimadas a partir de datos históricos, árboles de fallas u otras técnicas de ingeniería de sistemas.

F4 Riesgos de salubridad

Los riesgos de salubridad se expresan normalmente en alguna de las siguientes formas:

a) La cantidad de nuevos casos de enfermedad por año en una población expuesta comparado con el total de esa población, ej: 5 nuevos casos en una población expuesta de 100 000 es un riesgo de 5 x 10 -5 por persona expuesta, por año. Cantidad de muertes por año en la población expuesta a la actividad.
b) El coeficiente de probabilidad de muerte antes de cierta edad, con y sin exposición.
c) La cantidad de fatalidades por edad 70 que se espera resulte de una exposición, dividida por la cantidad de gente expuesta.

Los riesgos de salubridad pueden derivarse de datos epidemiológicos (censos de población de fatalidad o enfermedad) o de datos experimentales basados en estudios sobre animales.
nota: En lugar de calcular el valor promedio de un riesgo, la distribución de valores posibles se puede calcular reemplazando los valores promedio de las variables, de las cuales depende el resultado, por las distribuciones apropiadas de valores.

G Identificar opciones para tratamiento de riesgos

G1 Acciones para reducir o controlar la probabilidad

Estos pueden incluir:

i) programas de auditoria y cumplimiento;
ii) condiciones contractuales;
iii) revisiones formales de requerimientos, especificaciones, diseño, ingeniería y operaciones;
iv) inspecciones y controles de procesos;
v) administración de inversiones y cartera;
vi) administración de proyectos
vii) mantenimiento preventivo;
viii) aseguramiento de calidad, administración y estándares;
ix) investigación y desarrollo, desarrollo tecnológico;
x) capacitación estructurada y otros programas;
xi) supervisión;
xii) comprobaciones;
xiii) acuerdos organizacionales; y
xiv) controles técnicos.

G2 Procedimientos para reducir o controlar las consecuencias

Estos pueden incluir:

i) planeamiento de contingencia;
ii) arreglos contractuales;
iii) condiciones contractuales;
iv) características de diseño;
v) planes de recupero de desastres;
vi) barreras de ingeniería y estructurales;
vii) planeamiento de control de fraudes;
viii) minimizar la exposición a fuentes de riesgo;
ix) planeamiento de cartera;
x) política y controles de precios;
xi) separación o reubicación de una actividad y recursos;
xii) relaciones públicas; y
xiii) pagos *ex gratia*.

H Documentación de administración de riesgos

H1 General

Para administrar correctamente el riesgo, se requiere una documentación apropiada. Esto puede necesitar ser suficiente para satisfacer a una auditoria independiente. Las decisiones concernientes al alcance de la documentación puede involucrar costos y beneficios y debería tomar en cuenta los factores listados en la Cláusula 5.2. La declaración de la política de administración de riesgos debería definir la documentación necesaria.

En cada etapa del proceso, la documentación debería incluir:

a) objetivos;
b) fuentes de información;
c) supuestos; y
d) decisiones.

El Apéndice H incluye un ejemplo de un registro de riesgo, y un programa de tratamiento y plan de acción. Los planes para las áreas de alto riesgo pueden necesitar ser más específicos y detallados.

H2 Política

En el Apéndice B se dan ejemplos de la información que podría ser incluida en la declaración de política de una organización.

H3 Declaración de cumplimiento y diligencia debida

En algunas circunstancias puede requerirse una declaración de cumplimiento y diligencia debida, de forma tal que los gerentes tomen conocimiento formal de su responsabilidad por el cumplimiento de las políticas y procedimientos de administración de riesgos.

H4 Registro de riesgos *

Por cada riesgo identificado el registro de riesgo comprende:

a) fuente;
b) naturaleza;
c) controles existentes;
d) consecuencias y probabilidad;
e) puntaje inicial del riesgo; y
f) vulnerabilidad a factores externos / internos.

Consultar como guía la proforma de muestra.

H5 Programa de tratamiento de riesgos y plan de acción *

Un tratamiento de riesgos y plan de acción documenta los controles gerenciales a adoptar y lista la siguiente información:

a) Quién tiene responsabilidad por la implementación del plan;
b) Qué recursos se van a utilizar;
c) Asignación de presupuesto;
d) Calendario de implementación;
e) Detalles del mecanismo y frecuencia de la revisión de cumplimiento del plan de tratamiento.

H6 Monitorear y auditar documentos

Los registros de monitoreo y auditoria deberían documentar:

a) Detalles del mecanismo y frecuencia de la revisión de riesgos y del proceso de administración de riesgos como un todo;
b) Los resultados de las auditorias y de otros procedimientos de monitoreo;
c) Detalles de cómo son seguidas e implementadas las recomendaciones de las revisiones.

- Estos ejemplos son solo indicativos.

Registro de Riesgos

Fecha de revisión de riesgo.....
Compilado por..... Fecha.....
Revisado por..... Fecha.....

Función/actividad.....

Ref	Riesgo: qué puede suceder y cómo puede suceder	Las consecuencias de suceder un evento		Aptitud de los controles existentes	Puntaje de consecuencia	Puntaje de probabilidad	Nivel del riesgo	Prioridad del riesgo
		Consecuencias	Probabilidad					

Programa y plan de tratamiento de riesgos

Fecha de revisión de riesgo .....
Compilado por ..... Fecha. .....
Función/actividad ..... Revisado por ..... Fecha .....

El riesgo en orden de prioridad del Registro de Riesgo	Opciones posibles de tratamiento	Opciones preferidas	Puntaje de Riesgo luego del tratamiento	Resultado del análisis de costo/beneficio A. acepta B. rechaza	Persona responsable por implementación de la opción	Calendario de implementación	Cómo será monitoreado este riesgo y las opciones de tratamiento

Plan de acción de riesgos

Item Riesgo	Ref
Resumen – Respuesta e impacto recomendado	
Plan de acción 1 Acciones propuestas 2 Requerimientos de recursos 3 Responsabilidades 4 Programa de fechas 5 Monitoreo e informes requeridos	
Compilador.....Fecha..... Revisor.....Fecha.....	

DT/01/2005 SUPERINTENDENCIA DE BANCA, SEGUROS Y ADMINISTRADORAS PRIVADAS DE FONDOS DE PENSIONES

Examinando los riesgos macroeconómicos en Basilea II: propuestas de supervisión para economías emergentes

Juan José Marthans [1/]
Superintendente de Banca, Seguros y AFP

DICIEMBRE 2005

Resumen

El Nuevo Acuerdo de Capital (NAC) recomienda que los requerimientos de capital sean más sensibles a los riesgos que se enfrentan en el negocio bancario. Aun cuando el NAC constituye un gran avance, pues en su primer pilar reconoce la importancia del riesgo de mercado, crediticio y operacional, es cierto que existen riesgos materiales adicionales de impacto global, tales como el aumento del riesgo sistémico derivado de la concentración en los mercados financieros, el incremento del riesgo crediticio generado por la dolarización parcial de la economía, la importante participación del endeudamiento soberano en moneda extranjera y la presencia de ciclos crediticios más volátiles en las economías emergentes. Al respecto, el segundo pilar del NAC establece que aquellos riesgos bancarios no considerados en el primer pilar pueden incluirse como requerimientos adicionales de capital (a discreción del supervisor). Esta recomendación no es suficiente, ya que podría derivar en legislaciones disímiles entre países, las cuales --eventualmente- generarían alguna forma de arbitraje regulatorio; de ahí que surja la necesidad de establecer estándares mínimos y metodología objetivas similares a aquellas establecidas en el primer pilar. Al respecto, este documento recomienda el establecimiento de un requerimiento de capital adicional para las entidades activas internacionalmente que incrementen la concentración del sistema bancario nacional o internacional, un esquema de provisiones para el riesgo cambiario crediticio y un sistema de incentivos que implique exigencias de capital adicionales cuando la participación de un instrumento dentro de la cartera de inversiones es excesiva.

CLASIFICACION JEL: G21,G28

CLAVE: ***Basilea II, Riesgos macroeconómicos, Supervisión bancaria***

E-Mail del Autor(es): ***jmarthans@sbs.gob.pe***

[1/] El autor es el Superintendente de Banca, Seguros y AFP de Perú. Agradece los comentarios y sustanciales aportes de Michel Canta, Paul Collazos, Javier Nagamine, Javier Poggi, José Carlos Sánchez, Marco Shiva y Jakke Valakivi. Las opiniones expresadas en este artículo son del autor y no reflejan necesariamente las opiniones de la SBS. Las aclaraciones usuales también son pertinentes.

I. Introducción

El Nuevo Acuerdo de Capital (NAC) que recomienda el Comité de Basilea para la Supervisión Bancaria enfatiza la sensibilidad de los requerimientos de capital al riesgo inherente en los activos bancarios, permite que los intermediarios financieros puedan medir el grado de riesgo de sus negocios, y hace posible que el supervisor bancario pueda establecer una mejor diferenciación de los intermediarios financieros con portafolios más riesgosos, y así pueda distribuir adecuadamente los recursos disponibles para sus actividades de supervisión.

En esencia, el primer pilar del NAC presenta la medición cuantitativa del riesgo bancario, representado por los tres principales riesgos del negocio: riesgo crediticio, riesgo de mercado y riesgo operacional. A diferencia del Acuerdo de 1988, en el que se presentaba una metodología estandarizada y poco sensible al riesgo crediticio, el NAC enfatiza la medición de riesgos mediante el uso de modelos internos basados en la construcción estadística y muestral de las distribuciones de pérdidas de los portafolios de activos. El uso de modelos unifactoriales para la medición del riesgo crediticio y de mercado brinda una primera aproximación al cálculo de las pérdidas no esperadas, permitiendo la estimación del requerimiento de capital necesario para soportar dichas pérdidas y aliviando los problemas de riesgo moral que afectan a los accionistas en el sistema bancario.

No obstante el gran avance del NAC al reconocer el riesgo crediticio, de mercado y operacional que enfrentan los intermediarios financieros, se debe considerar una serie de riesgos materiales (adicionales y de carácter regional y global), entre los cuales destacan el riesgo sistémico que se deriva de una excesiva concentración, tanto en los sistemas financieros a nivel local como a nivel internacional; el incremento en el riesgo crediticio que se genera en economías altamente dolarizadas, donde los deudores que perciben ingresos en moneda local pueden tener obligaciones en moneda extranjera; el aumento del riesgo crediticio que se origina por la importante participación del endeudamiento soberano en moneda extranjera dentro del portafolio de inversiones de los bancos de países emergentes; y la aceleración del ciclo económico de las empresas ante la presencia de un canal crediticio.

Cabe resaltar que estos riesgos están relacionados, pues según las experiencias internacionales de los últimos años y dentro de la tendencia determinada por las grandes fusiones a nivel internacional, una crisis sistémica a nivel internacional -acrecentada por la elevada concentración de los sistemas financieros- podría generar un efecto recesivo sobre las economías emergentes, como producto de la globalización de los mercados financieros. Además, considerando los efectos de hoja de balance ocasionados por el canal crediticio y la dolarización presente en las economías en desarrollo, el impacto recesivo de las crisis financieras internacionales o la excesiva concentración de los mercados mundiales se podría traducir en una amplificación de los ciclos económicos, la cual se evidenciaría como un aumento de la volatilidad de los agregados macroeconómicos de estas economías.

La mayor volatilidad de los agregados macroeconómicos de economías emergentes retroalimenta el riesgo inherente en las operaciones de bancos internacionales con países en desarrollo, a la vez que genera un mayor requerimiento de capital y, posiblemente, un racionamiento crediticio hacia las economías consideradas más vulnerables. De ahí que la presencia de riesgos macroeconómicos, no solo ocasiona una amplificación del ciclo económico, sino también genera una mayor persistencia de impactos adversos sobre el desarrollo de los intermediarios financieros.

Aunque en el segundo pilar del NAC se establece que aquellos riesgos bancarios no considerados directamente pueden incluirse como requerimientos de capital adicionales –a discreción del supervisor- esto podría derivar en regulaciones disímiles, que eventualmente podrían generar alguna forma de

arbitraje regulatorio. De ahí que surja la necesidad de establecer estándares mínimos y metodologías objetivas similares a las establecidas en el Pilar I.

No obstante, el desarrollo de mecanismos objetivos para establecer requerimientos de capital por estos conceptos podría pertenecer a una agenda más ambiciosa del Comité de Basilea y resulta conveniente encontrar algunos lineamientos de políticas regulatorias que actúen como medidas temporales para enfrentar –sinceramente- estos riesgos, debido a que el establecimiento de regulaciones prudenciales se vuelve una inaplazable responsabilidad de los entes supervisores en todo el mundo.

En particular, este documento plantea que los supervisores bancarios a nivel mundial utilicen un requerimiento adicional de capital discrecional, que denominaremos "palanca en la sombra". El objetivo de este requerimiento adicional es doble. Por un lado, un mayor requerimiento de capital discrecional tendería también a desalentar estas sobre-exposiciones, generando incentivos para que los bancos sean más prudentes en sus operaciones crediticias. De otro lado, una exigencia adicional de capital aplicada sobre los bancos que elevan la concentración corregiría los incentivos de fusiones no competitivas. Asimismo, la propuesta podría reducir el carácter procíclico del NAC, puesto que esta reserva podría ser utilizada en recesión y acumulada durante las etapas expansivas del ciclo económico.

Además de este requerimiento de capital discrecional, este artículo propone otros instrumentos de regulación preventiva, tales como un esquema de provisiones para riesgo cambiario crediticio y un mecanismo de incentivos que implica requerimientos adicionales cuando la participación de un instrumento dentro de la cartera de inversiones supera determinados umbrales. Cabe precisar que estas medidas deben ser complementadas por factores de riesgo que deben ser necesariamente incorporados en modelos internos similares a los propuestos en el Pilar I del NAC, puesto que, de no incluirse, se incurriría en un sesgo en la estimación del riesgo bancario de consecuencias costosas para el sistema financiero.

Este artículo tiene la siguiente estructura: en la siguiente sección se analizan los riesgos sistémicos y macroeconómicos que se pueden derivar de la concentración del sistema bancario y se recomienda la utilización de un requerimiento prudencial adicional de capital. La tercera sección describe las consecuencias de la dolarización y sugiere algunas medidas regulatorias para aliviar su impacto acelerador sobre el ciclo económico. La cuarta sección aborda los efectos del endeudamiento soberano en moneda extranjera y propone algunas regulaciones para evitar sus consecuencias adversas sobre el sistema bancario. La quinta sección evalúa el canal crediticio que está detrás de los ciclos crediticios que afectan la evolución de los agregados macroeconómicos y las variables financieras y propone algunas políticas de supervisión bancaria para aliviar sus efectos perjudiciales. Finalmente, la sexta sección concluye el artículo.

II. Concentración bancaria, riesgo sistémico y el rol de los requerimientos de capital

Durante la década pasada, el sistema financiero mundial ha experimentado un proceso de concentración[2] producido por diversas causas entre las que destacan la salida de mercado de muchas instituciones financieras a nivel mundial y los procesos de fusión debido al crecimiento de las empresas o al redimensionamiento de los mercados internacionales. La globalización económica ha generado que poco

[2] Definimos como concentración a aquella situación en la que un número reducido de intermediarios financieros administran la mayor cantidad de activos o depósitos del sistema en donde operan. La medición de este tipo de concentración puede efectuarse a través del coeficiente de Gini, el índice de Hirschman-Herfindalh y los ratios de concentración de activos o de colocaciones (e.g el ratio C5).

más de un tercio de los activos totales del sistema bancario a nivel mundial esté concentrado en un reducido número de bancos de gran escala. Tal como se puede apreciar en el Cuadro N°1, los cinco primeros bancos a nivel internacional agrupan el 10.55% de los activos de los 1000 grupos bancarios más grandes del mundo, mientras que los 25 bancos más grandes agrupan el 37% de esos activos. Estos altos niveles de concentración justifican la magnitud del problema a discutir, así como la relevancia del problema de definir medidas regulatorias preventivas y de supervisión en un contexto de alta concentración en los mercados financieros y en una dimensión global.

Cuadro N° 1
25 Grupos bancarios más grandes según activos
(julio 2004)

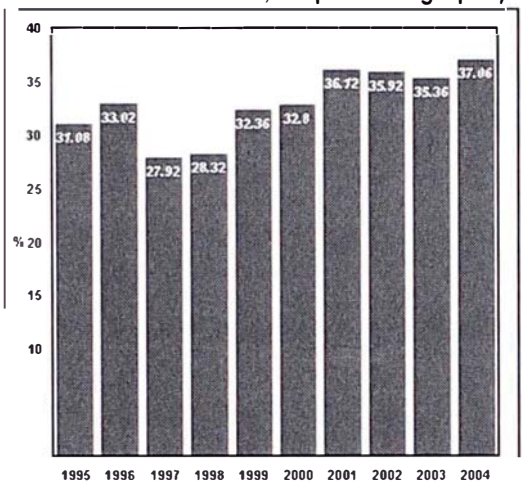
Orden actual	Nombre del grupo bancario	Activos (Millones de US $)	Participación en los 1000 primeros grupos (%)
1	Mizuho Financial Group, Tokio, Japon	1,285.471	2.33%
2	Citigroup, New York, EEUU.	1,264,032	2.29%
3	UBS Zurich, Suiza.	1,120,543	2.03%
4	Crédit Agricole Groupe, Paris, Francia.	1,105,378	2.01%
5	HSBC Holdings	1,034,218	1.88%
6	Deutsche Bank, Frankfurt, Alemania.	1,014,845	1.84%
7	BNP Paribas, Paris, Francia.	986,982	1.79%
8	Mitsubishi Tokyo Financial Group, Tokio, Japón.	974,950	1.77%
9	Sumitomo Mitsui Banking Corporation, Tokio, Japón.	950.448	1.73%
10	The Royal Bank of Scotland Group, Edinburgo, Reino Unido.	806,207	1.46%
11	Barclays, Londres, Reino Unido.	791,292	1.44%
12	Credit Suisse Group, Zurich, Suiza.	777,848	1.41%
13	JP Morgan Chase Bank, New York, EEUU.	770,912	1.40%
14	UFJ Bank, Tokio, Japón.	735,631	1.34%
15	Bank of America, Charlotte, EEUU.	736,445	1.34%
16	ING Bank , Amsterdam, Holanda.	684,004	1.24%
17	Société Générale, Paris, Francia.	681,218	1.24%
18	ABN AMRO Holding, Amsterdam, Holanda.	667,636	1.21%
19	HBOS, Londres, Reino Unido.	650,721	1.18%
20	Industrial & Commercial Bank of China, Beijing, China.	637,828	1.16%
21	Hypovereinsbank, Alemania.	605,525	1.10%
22	Dresdner Bank Group, Frankfurt, Alemania.	605,461	1.10%
23	Fortis Bank, Bélgica.	535.462	0.97%
24	Rabobank Group, Holanda.	509,352	0.92%
25	Commerzbank, Alemania.	481,921	0.87%
	Activos de los primeros 25	**20,414,330**	**37.06%**
	Activos de los primeros 1000	**55,084,539**	**100.00%**

Fuente: Ranking "Top 1000 World Banks" de la Revista "The Banker"

La tendencia mundial hacia sistemas financieros concentrados no se ha revertido desde 1995[3]. Tal como se aprecia en el Gráfico Nº 1, el grado de concentración de activos globales ha pasado de 31% en 1995 a casi 38% diez años después. También cabe resaltar que este fenómeno no solo tiene un carácter regional sino que tiene una envergadura mundial, constituyendo un fenómeno simultáneo al proceso de globalización que ha integrado los sistemas bancarios de todas las regiones del mundo. De este modo, la globalización ha permitido que el fenómeno de concentración global se replique en la escala regional y local.

A nivel mundial, los casos más notorios de concentración se presentaron en Holanda (con la fusión Deutsche Bank-BT), en Estados Unidos (con la fusión de instituciones financieras como Citicorp y Travelers, o la fusión entre el BankAmerica con NationsBank, o el Bank One con el banco First Bank), en Francia (donde se fusionaron BNP y Paribas), Japón (que subraya el caso del Sumitomo Bank y el Sakura Bank), España (con la fusión del Grupo Santander y el Banco Central o del grupo BBV con el grupo Argentaria), Suiza (con el caso del United Bank of Switzerland) o Canadá (con la fusión entre Royal Bank y el Bank of Montreal y el CIBC y el TD Bank). Adicionalmente todas estas fusiones de bancos en países desarrollados implicaron serios cambios en la estructura de los mercados financieros emergentes. Un caso ilustrativo de lo anterior se da en los países de nuestra región; en especial México, Argentina, Chile y Perú, donde se produjeron fusiones de instituciones bancarias locales como una consecuencia directa de las fusiones de los grupos bancarios europeos.

Gráfico N° 1
Evolución de la concentración de activos: 1996-2004
(Participación de los activos de los 25 grupos bancarios más grandes en los activos de los 1,000 primeros grupos)



Fuente: Ranking "Top 1000 World Banks" de la Revista "The Banker"

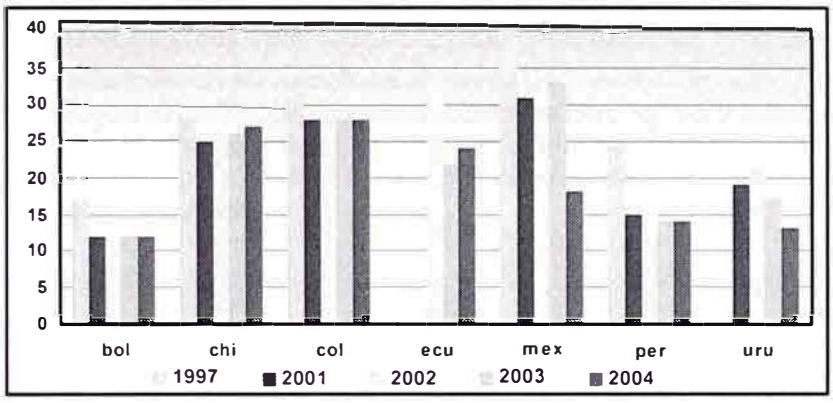
Adicionalmente, si tomamos en cuenta que los bancos internacionales más grandes son aquellos que intermedian una alta proporción de los flujos de capitales a nivel mundial, entonces, la concentración que

[3] Véase Berger & Strahan (1999), International Monetary Fund (2001) y Group of Ten (2001).

existe en los mercados financieros podria propiciar un incremento del riesgo sistémico internacional. Un ejemplo de lo anterior lo constituye la experiencia de varios bancos internacionales que sufrieron pérdidas durante las crisis rusa y asiática de la década pasada y que propiciaron el recorte de lineas de crédito hacia paises emergentes, con el consecuente aumento en la volatilidad de capitales financieros y la amplificación de los ciclos económicos en esos paises[4].

En América Latina, el fenómeno de concentración de los mercados financieros también es evidente. Tal como se muestra en el Gráfico N°2, la reducción en el número de entidades financieras ha sido generalizada y ha sido acompañada de un incremento en los indices de concentración del sistema. Los principales procesos de consolidación bancaria fueron generados a partir de crisis financieras, tanto en México como en Uruguay o Perú, siendo el cambio más dramático el ocurrido en México donde el número de bancos pasó de 40 en 1997 a tan solo 18 en el 2004. Uruguay, a consecuencia de las repercusiones que tuvo la crisis Argentina en su sistema financiero, pasó de tener 21 bancos en el 2002 a 13 en el 2004; y en Perú, entre 1997 y el 2004, el sistema bancario pasó de tener 24 bancos a solo 14.

Gráfico N°2
Evolución del número de bancos por países



Fuente: Bancos Centrales y Superintendencias de Bancos de los países citados.

El grado de concentración de los sistemas financieros latinoamericanos puede reflejarse en los indicadores C5[5] y el Herfindahl HHI[6]. Según el indicador de la participación en el mercado de

[4] Sobre este punto véase Tornell y Westerman (2002) y Chinn y Kletzer (2000). Este incremento de la volatilidad de los mercados financieros internacionales, asociado usualmente a procesos de crisis bancarias o cambiarias constituye un episodio de contagio financiero. Existen diversas explicaciones de porqué ocurre este fenómeno (i.e. porque las crisis se transmiten entre paises o regiones) que van desde problemas de información entre inversionistas y prestatarios internacionales (como en Calvo, 1999) hasta riesgo de liquidez (como en Valdés,1997). En nuestro caso nos interesa subrayar el canal de transmisión asociado a los problemas de liquidez, pues describe el proceso de propagación recurrente en las crisis sistémicas: una crisis bancaria o cambiaria genera pérdidas en un inversionista internacional, las cuales implican una reducción de sus activos y eventualmente una reducción de sus posiciones en otras plazas y, como consecuencia, se produce un recorte de financiamiento hacia otros paises o regiones.

[5] El ratio de concentración C5 mide la participación de las 5 empresas más grandes en un mercado determinado.

colocaciones de los 5 mayores bancos, paises como Uruguay, México y Perú presentan una alta concentración, pero es Uruguay el que presentó el cambio más drástico en los últimos años pues pasó de 53% a 75%.

Cuadro N°2
Concentración de las colocaciones: índice C5
(Participación porcentual en las colocaciones totales de los cinco mayores bancos)

País	1997	2001	2002	2003	2004
Colombia	43	43	40	41	41
Brasil	n.d.	n.d.	55	59	62
Chile	65	64	62	67	65
Ecuador	n.d.	n.d.	69	68	66
Bolivia	65	67	71	70	71
Uruguay	n.d.	n.d.	53	65	75
México	75	76	80	78	80
Perú	69	80	78	82	81

Fuente: Bancos Centrales y Superintendencias de Bancos de los paises citados.

El índice Hirschman-Herfindahl presenta resultados similares a los anteriores tanto para Uruguay, como para México y Perú[7]; pero en general, salvo Argentina[8] y Colombia todos los paises presentan niveles altos de concentración. A partir de este índice, se comprueba que -en los últimos años- el país que sufrió el cambio más severo fue Uruguay, que pasó de ser uno de los paises menos concentrados de la región a ser uno de los tres más concentrados.

Cuadro N°3
Concentración de las colocaciones: índice de Herfindahl

País	1997	1998	1999	2000	2001	2002	2003	2004
Colombia	572	699	730	673	626	587	594	599
Brasil	n.d.	n.d.	n.d.	1,076	879	777	872	1,050
Chile	1,060	1,061	1,028	1,003	1,019	981	1,235	1,073
Ecuador	n.d.	n.d.	n.d.	n.d.	n.d.	1,263	1,198	1,207
Bolivia	1,091	1,212	1,279	1,203	1,198	1,221	1,217	1,246
Uruguay	n.d.	n.d.	n.d.	n.d.	n.d.	806	1,090	1,363
México	1,456	1,494	1,432	1,751	1,745	1,672	1,516	1,588
Perú	1,259	1,163	1,361	1,446	1,614	1,563	1,863	1,856

Fuente: Bancos Centrales y Superintendencias de Bancos de los paises citados.

[6] El índice de Hirschman-Herfindahl está definido como la sumatoria de los cuadrados de la participación de mercado de cada institución.

[7] Analizando la cartera crediticia por tipo de crédito en el caso peruano, se puede precisar que no hay evidencia de una elevada concentración en los créditos de consumo, en los préstamos a las microempresas y en las colocaciones comerciales menores a 3 millones de Nuevos Soles (aproximadamente 1 millón de dólares americanos), sino que esta se presenta –fundamentalmente- en los grandes deudores del sistema bancario los cuales tienen acceso al financiamiento a través del mercado de capitales.

[8] No se cuenta con información para evaluar cómo evolucionó la concentración en Argentina después de la crisis del 2000.

Esta descripción de las tendencias mundiales y la situación latinoamericana acerca de la concentración bancaria es importante porque -desde el punto de vista de la supervisión y la regulación bancaria- es fundamental entender el vínculo entre la concentración en la banca y la estabilidad del sistema financiero. Al respecto se han generado una serie de estudios dedicados a evaluar el impacto de una mayor concentración sobre la estabilidad financiera, tanto en investigaciones teóricas como en estudios empíricos. Los trabajos teóricos se pueden clasificar en dos enfoques[9]: el enfoque de "concentración y fragilidad" y el enfoque de "concentración y estabilidad".

El enfoque de concentración y fragilidad[10] propone que mientras más grande sea un banco, mayores serán sus incentivos para tomar riesgos, ya que se considera "demasiado grande para quebrar". Asimismo, su mayor tamaño también deriva en una mayor complejidad de sus negocios, y en un incremento del riesgo operacional[11]. También se desprende de esta hipótesis que el incremento en la concentración de los mercados financieros mundiales implica un aumento de la volatilidad de los flujos de capitales y de la probabilidad de ocurrencia de una crisis financiera internacional, como consecuencia de la quiebra de un banco internacional de gran escala.

En contraste, el enfoque de concentración y estabilidad enfatiza la hipótesis de que una mayor concentración deriva en una mayor estabilidad del sistema financiero, debido al mayor nivel de diversificación que se alcanza al aumentar la escala del banco, o porque los bancos concentrados generan mayores ganancias, las cuales pueden constituir una reserva contra futuros impactos adversos[12], o simplemente porque resulta más fácil para el supervisor monitorear pocos bancos en el mercado, permitiéndole una mejor diferenciación entre instituciones a fin de poder reducir el efecto contagio en el evento de una crisis[13].

Respecto al análisis de la evidencia empírica, los trabajos han subrayado la relación positiva entre concentración y estabilidad financiera. En particular, Beck, Demirgüç-Kunt y Levine (2003), en base a una muestra de 70 países (incluyendo tanto países industrializados como economías en desarrollo), encuentran que la probabilidad de una crisis financiera es menor en los países con sistemas bancarios más concentrados, y que el aumento en la competencia o la existencia de instituciones que la promuevan disminuye la probabilidad de una crisis bancaria sistémica. En esa misma dirección, pero en otro estudio, Claessens and Laeven (2003) –utilizando una muestra de 50 países- no encuentran evidencia de una relación negativa entre concentración y competencia, y sostienen que -aún en sistemas concentrados- la

---

[9] Esta clasificación corresponde a Beck ,Demirgüç y Levine (2003).

[10] Al respecto se puede citar a Boyd y Graham (1991). También está presente en los recientes libros de Tirole (2002), Stiglitz y Greenwald (2003) y en el artículo de Stiglitz (2004).

[11] Existen varios casos que muestran la relevancia de este tipo de riesgo. Desde los recientes casos de Enron y el ataque al Wolrd Trade Center, que afectaron a numerosas empresas financieras y no financieras, o los famosos casos de fraude del Bank of Credit and Commerce Internacional (BCCI) en 1991 y el Long Term Capital Management en 1998, hasta casos de sobreexposición en operaciones de *trading* como el caso de la Corporación Sumitomo en 1996, las empresas del Grupo Prudential en 1994 o Barings en 1995.

[12] Esta reserva genera un aumento en el valor de la institución y reduce los incentivos para tomar mayores riesgos. Como un ejemplo de estos trabajos, los autores citan a Hellmann, Murdoch y Stiglitz (2000).

[13] Un ejemplo de este tipo de modelos se puede hallar en la sexta sección del artículo de Allen y Gale (2003), quienes consideran una economía en la cual la probabilidad de sufrir una crisis sistémica puede aumentar con el número de bancos debido a que los problemas de coordinación en el mercado interbancario se multiplican con el incremento del número de instituciones financieras.

posibilidad de entrada de nuevos bancos genera suficiente competencia en las instituciones bancarias establecidas.

Al respecto, cabe precisar la limitaciones de un análisis basado en datos de panel a partir de indicadores de estados financieros de entidades bancarias, en tanto se comparan experiencias distintas entre países que cuentan con planes contables, metodologías y regulaciones heterogéneas. De otro lado, y aún cuando estos hallazgos empíricos afirman que un sistema bancario concentrado no genera inestabilidad ni pérdida de competencia, los supervisores y reguladores bancarios deben observar que los sistemas financieros cada vez más concentrados pueden incrementar la probabilidad de sufrir crisis sistémicas, en caso de no tomar medidas complementarias.

Justamente este enfoque subraya la relación directa entre concentración y fragilidad. Para entender este punto de vista, nos podemos imaginar un sistema bancario muy poco concentrado, con numerosos bancos, cada uno de los cuales tiene asociada una probabilidad de quebrar muy pequeña y una correlación muy baja entre los eventos de quiebra de cada uno de ellos. En este escenario sumamente competitivo, la probabilidad de que la quiebra efectiva de una de estas instituciones derive en una crisis sistémica es extremadamente baja (debido a la casi nula correlación entre bancos).

En contraste, imaginemos un sistema bancario muy concentrado, con un banco muy grande que posee una gran porción de los activos del sistema, y que tiene asociada una probabilidad de quiebra incluso más baja que la correspondiente al escenario de los bancos pequeños. En este nuevo escenario, la probabilidad de una crisis sistémica es muy parecida a la probabilidad de quiebra de este banco, la cual es mucho mayor que la probabilidad de crisis sistémica del escenario anterior (i.e. la probabilidad conjunta de las crisis individuales).

Es importante resaltar que este proceso no solo se replica a nivel local, entre las instituciones que participan de un mercado interbancario doméstico, sino a nivel regional (a través del mercado de capitales entre los países de una región). Cuando esto ocurre, la crisis sistémica se convierte en una crisis de liquidez en la región que –eventualmente- puede desatar un episodio de contagio financiero internacional, de modo que los costos individuales se proyectan hacia costos regionales y estos, a su vez, se amplifican en costos globales (esencialmente por la naturaleza asimétrica de la información que poseen los inversionistas internacionales).

Debido a que un sistema concentrado implica un mayor riesgo sistémico, es necesario diseñar un mecanismo que provea incentivos para que los accionistas del sistema bancario adopten políticas de administración de riesgos más cautelosas en el contexto de un sistema más concentrado y, por lo tanto, más propenso a un crisis sistémica. Idealmente, se debería generar un método objetivo para medir la magnitud de este riesgo sistémico y proponer un mecanismo que genere incentivos para reducirlo, tal como se hace con los riesgos considerados en el Pilar I. Sin embargo, mientras se adecuen estos aspectos en el NAC, temporalmente se puede proponer la inclusión de un requerimiento de capital adicional aplicado sobre los bancos que generan este aumento en la concentración. Como se explicará a continuación, dicho requerimiento no solo cumple el rol de proveer incentivos para un manejo más cauteloso de los riesgos bancarios (dado que implica un crecimiento en la exposición de los propietarios del banco) sino que elimina -o al menos alivia- la tentación de fusiones que no incrementen la eficiencia.

En efecto, los mayores requerimientos de capital reducen los incentivos para la "concentración-no-competitiva" en un sistema financiero, constituyendo un instrumento de política para disuadir a los bancos en su búsqueda de un proceso de fusión como parte de una estrategia para convertirse en un banco "demasiado grande para quebrar". Este mecanismo actuaría haciendo más costosa la asignación de

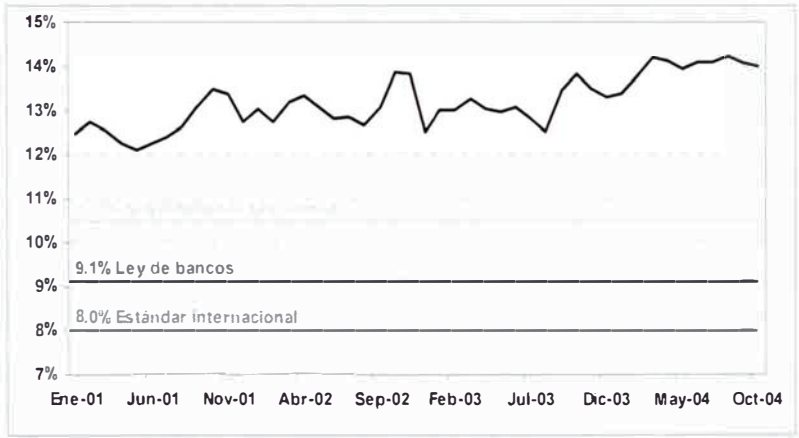
capital cuando los bancos no se fusionan por la búsqueda de mayor eficiencia[14]. En efecto, si un banco se fusiona por razones de eficiencia, las ganancias que obtenga producto de su reorganización y/o redimensionamiento compensarán el costo económico asociado al incremento del capital requerido. Sin embargo, si la fusión se genera como consecuencia de una estrategia para ser "demasiado grande para quebrar" el nuevo requerimiento de capital implicará un costo neto.

Esta recomendación de política se encuentra en línea con lo establecido en el NAC, el cual -en su segundo pilar- recomienda a los supervisores que requieran -por motivos discrecionales- una reserva de capital superior a la exigible a fin de contar con aquellos riesgos que no son explícitamente tratados en él. De esta forma, el supervisor bancario puede contar con una herramienta adicional que le permita mantener la estabilidad del sistema financiero, dentro de un marco coherente de administración de riesgos bancarios, como el propuesto por Basilea II.

La experiencia peruana es relevante en este sentido. Tal como se muestra en el siguiente gráfico, al mantenerse en los últimos años un requerimiento de capital adicional al mínimo establecido por la Ley de bancos, el sistema financiero peruano ha percibido los beneficios dinámicos de un esquema de incentivos que promueve una administración bancaria más cautelosa y se ha ubicado en una posición más sólida frente a los impactos adversos derivados de algunos episodios de crisis financieras en la región.

La propuesta presenta ventajas notorias respecto a las regulaciones sobre la concentración bancaria presente en otros países. Dichas legislaciones incluyen barreras a la fusión entre bancos si esta supera niveles de concentración predeterminados (entre 15% y 20%, por ejemplo), mayores requerimientos patrimoniales o, inclusive, la negación de autorización. Al respecto, la propuesta regulatoria peruana no establece umbrales *a priori* sobre el nivel de concentración, pero sí determina mayores requerimientos de capital, de modo que actúa como un mecanismo de revelación para distinguir las fusiones que incrementan o no la eficiencia.

Gráfico N° 3
Patrimonio efectivo sobre activos y créditos ponderados por riesgo
(En porcentajes)



Fuente: SBS.

[14] Nótese que si la fusión bancaria se da por motivos de eficiencia, el costo de este requerimiento adicional podría ser fácilmente absorbido por la mayor ganancia en eficiencia producto de la fusión.

El éxito de este mecanismo de autorregulación, por parte de los bancos locales, se comprueba al observar los niveles mostrados de patrimonio efectivo sobre activos y créditos ponderados por riesgo. Este ratio no solo se encuentra sistemáticamente por encima del estándar internacional, sino que esta diferencia positiva ha aumentado de 4 a casi 6 puntos porcentuales en los últimos 4 años, marcando una tendencia sobresaliente en la región. También cabe precisar que la Ley de Bancos peruana establece un requerimiento de 9.1% comparado con el nivel de 8% sugerido en la normativa internacional. El requerimiento prudencial que surge de un esquema coordinado entre el supervisor bancario y los bancos constituye la base para la autorregulación de estas entidades y ha contribuido al sostenimiento y tendencia creciente de este indicador.

Queda para la futura agenda de investigación definir la magnitud exacta de este incremento sobre el requerimiento de capital mínimo y establecer estándares mínimos similares a los sugeridos en el primer Pilar. Asimismo, se debe precisar que esta metodología debería aplicarse globalmente en el marco de una estrategia coordinada entre las agencias supervisoras de distintos países, a fin de evitar el arbitraje regulatorio o que los bancos internacionales de gran escala trasladen sus pérdidas a otras regiones y, de esta forma, reducir la volatilidad de los flujos de capitales y sus posibles efectos macroeconómicos adversos.

III. La dolarización de activos como acelerador del ciclo de las empresas

El uso de una moneda alternativa a la moneda local, tanto como medio de pago como depósito de valor, es común en economías emergentes, el primer caso se refiere a la sustitución monetaria, mientras que el segundo caso alude a la dolarización de activos. Ambos fenómenos definen usualmente el concepto de dolarización, un proceso cuyo origen radica en una serie de factores económicos tales como inestabilidad económica y la hiperinflación[15].

Uno de los problemas que genera el alto grado de dolarización y que recientemente viene siendo materia de continua preocupación en las economías emergentes, así como en los organismos internacionales, es el que origina el llamado riesgo crediticio cambiario. En una economía parcialmente dolarizada, gran parte de los fondos prestables se encuentran en moneda extranjera. A fin de evitar un descalce en sus exposiciones, los intermediarios financieros prestan recursos en moneda extranjera a empresas del sector real que no necesariamente generan ingresos en la misma moneda. De allí que, en la medida que exista este descalce de monedas en el deudor, un incremento en el tipo de cambio tiene un efecto de hoja de balance (que consiste en el incremento del monto de la deuda que éste mantiene con la entidad financiera expresada en la moneda local) y tiene un efecto sobre el flujo de caja del deudor (que posiblemente generaría el incumplimiento del pago del crédito). En consecuencia, el efecto final de una depreciación significativa del tipo de cambio puede ser una acumulación de cartera pesada en los intermediarios financieros y una expansión de la fase recesiva del ciclo económico.

De otro lado, cuando los bancos centrales de los países parcialmente dolarizados notan que una fluctuación brusca del tipo de cambio puede generar problemas, tanto en el sistema financiero como en el sector real, tienden a sufrir lo que se ha denominado "*fear of floating*" (es decir, no dejan flotar el tipo de cambio, a pesar que la regla establecida en el mercado es de flotación). Esto se debe a que la dolarización parcial de la economía y el correspondiente riesgo crediticio cambiario (cuando existe descalce en el deudor) limita el manejo de la política monetaria y no permite a esta actuar como

[15] Sobre las causas y consecuencias de la dolarización véase Levy Yeyati y Sturzenegger (2003)

estabilizador cuando la economía se encuentra en recesión[16]. No obstante, esta intervención del Banco Central en el mercado cambiario, a través de instrumentos monetarios en moneda extranjera[17], deriva en una reducción de la volatilidad del tipo de cambio y tiene como consecuencia una subestimación del riesgo de una depreciación cambiaria.

Teniendo en cuenta que los manuales de supervisión bancaria, así como las normas sobre provisiones y requerimientos de capital, consideran que se debe contar por los efectos del riesgo crediticio cambiario al momento de la evaluación del riesgo del portafolio bancario, esta subestimación del riesgo de una depreciación puede derivar en menores requerimientos de capital y de provisiones y, por lo tanto, es necesario tomar medidas complementarias que consideren este riesgo.

Una política a considerar es el establecimiento de categorías de riesgo asociadas a una probabilidad de incumplimiento que incorpore los efectos por descalce de monedas, tal como lo establecen los modelos internos propuestos en el primer pilar del NAC. En este sentido, un aumento del riesgo crediticio cambiario implicaría el reconocimiento implícito de una mayor probabilidad de incumplimiento debido a esa exposición, lo cual derivaría en un mayor nivel de provisiones y en mayores requerimientos de capital en los estados previos al deterioro de esta exposición.

Pero la incorporación del riesgo cambiario crediticio en un método avanzado se convierte en una meta necesaria pero desafiante, debido a los problemas que se enfrentarán al tratar de contrastar el modelo antes descrito; en particular, la dificultad en detectar criterios de discriminación que estén asociados a un mayor riesgo cambiario y que, a la vez, deriven en un aumento objetivo y verificable de la probabilidad de incumplimiento o la pérdida asociada a ese evento. Frente a esta limitación, se puede sugerir un esquema de incentivos establecidos por el supervisor a fin de fomentar –en las instituciones financieras- una evaluación cualitativa de los deudores, considerando aquellos factores que –a criterio del banco- incrementen el riesgo cambiario crediticio de los deudores. Cabe precisar que este tipo de evaluación se enmarca dentro del primer pilar del NAC (tanto en el método estandarizado como en los modelos avanzados) y se puede complementar con mecanismos que generen una penalidad adecuada cuando las entidades bancarias no efectúan sus evaluaciones considerando este riesgo.

Al respecto, la Superintendencia de Banca Seguros y AFP de Perú, siguiendo los procesos establecidos en el Pilar I respecto de la adecuada identificación y medición de riesgos, ha implementado una nueva normativa que establece estándares mínimos que buscan que los intermediarios financieros incluyan en su análisis de evaluación de cartera crediticia, la sensibilidad de sus posiciones ante variaciones en el tipo de cambio.

La regulación peruana que precisa el mecanismo prudencial frente al riesgo cambiario crediticio establece los principios generales y criterios mínimos para la adopción de un sistema de administración de riesgo cambiario crediticio y, a la vez, busca que las entidades financieras incorporen los costos asociados a este riesgo, ya sea mediante una reducción de su exposición ante este riesgo o la búsqueda de seguros como garantías o contratos derivados que transfieran el riesgo al cual están expuestas. En última

[16] Véase sobre este punto a Caballero y Krishnamurthy (2004) y a Eichengreen, Hausmann y Panizza (2003), así como la creciente bibliografía asociada a los efectos de variaciones del tipo de cambio en la exposición crediticia del sector real.

[17] En el caso peruano estos instrumentos son la tasa de encaje en moneda extranjera, los swaps en moneda extranjera, los créditos de corto plazo a las instituciones financieras (denominados "créditos de regulación"), la compra y venta de certificados de depósitos al banco central ajustados al dólar, las compras y ventas en la mesa de negociación tanto al sector público como a los bancos a través del mercado interbancario.

instancia, se plantea que aquellas entidades que no desarrollen una metodología de medición y control de riesgos, deberán asumir el costo a través de una mayor provisión sobre los créditos en moneda extranjera, que no solo reflejará el riesgo asumido, sino también la incertidumbre respecto a su magnitud (dado que no se ha cuantificado ni estudiado el riesgo que la entidad enfrenta). La provisión establecida es de 0.25%, 0.50% y 1.00% dependiendo del tipo de garantía existente.

De esta forma, se establece que si el riesgo crediticio cambiario de una posición acreedora es significativo, el intermediario financiero debe reconocerlo a través de la clasificación adecuada de esta exposición en un nivel de mayor riesgo. Asimismo, de incumplirse con esta nueva medida, la Superintendencia tiene la potestad de exigir al intermediario financiero una mayor provisión por aquellas exposiciones en las cuales no se ha considerado el efecto de riesgo crediticio cambiario[18]. Así, la política establecida funciona como un sistema de incentivos a las buenas prácticas y castigos a aquellas que involucren un mayor riesgo por falta de un adecuado reconocimiento del efecto del tipo de cambio sobre la posibilidad de pago de las obligaciones crediticias.

Este tipo de regulación no es frecuente y existen escasos ejemplos, uno de ellos corresponde al esquema de requerimientos mínimos para el otorgamiento y administración de los créditos en moneda extranjera similar al propuesto por *The Financial Market Authority* de Austria. Esta norma propone un sistema de requerimientos mínimos basados en cuatro consideraciones:

i. Las instituciones financieras que otorguen créditos en moneda extranjera deberán establecer límites cuantitativos que sean parte de la capacidad de repago del deudor una vez que se ha deducido el margen esperado de ganancia por el préstamo.
ii. Estos límites cuantitativos determinarán el monto del crédito.
iii. Las instituciones financieras deberán realizar ejercicios de *stress testing* para evaluar los límites cuantitativos.
iv. En caso que los límites superen la capacidad de pago del deudor como consecuencia de los ejercicios de *stress testing* entonces procederá un cambio en la clasificación del deudor.

No obstante, el esquema antes descrito impone un costo a los deudores, el cual se traduce en una restricción de liquidez basada en el límite cuantitativo a los préstamos. La aplicación de estos límites tiene como consecuencia la amplificación y la propagación de las fases recesivas del ciclo económico. La amplificación del ciclo se origina debido a que los prestatarios afrontan restricciones de liquidez debido a los límites máximos a sus créditos. Como consecuencia, cuando entran a la fase recesiva del ciclo los prestatarios no pueden cubrir sus requerimientos de liquidez a través de más créditos y deben liquidar parte de su negocio o reducir su escala, produciéndose una amplificación del impacto recesivo inicial. De otro lado, la propagación del ciclo sucede cuando los prestatarios liquidan sus activos cuando otros lo hacen y, por ello, el precio de venta es menor al esperado.

En resumen, las consecuencias de establecer un esquema de límites al otorgamiento de préstamos como un mecanismo de administración del riesgo crediticio cambiario tiene la ventaja de su sencilla aplicación, pero tiene como desventaja que implica un costo para el deudor, el cual sufrirá de una ampliación y una propagación de los impactos adversos que enfrente lo cual se traduce a nivel macroeconómico como una mayor duración de las recesiones. Cabe precisar que esta observación no resulta tan relevante en el caso

[18] Aunque lo ideal sería contar con una norma que implique mayores requerimientos de capital para enfrentar el riesgo cambiario crediticio, esto demandaría un cambio en la Ley de Bancos. Mientras tanto, la regulación peruana ha avanzado a través de un mecanismo que exige mayores provisiones si la clasificación cualitativa realizada por los banco no identifica si un deudor está expuesto o no al riesgo cambiario crediticio.

de la economia austriaca pues el porcentaje de préstamos en moneda extranjera no es considerable, sin embargo, sí lo es para el caso peruano debido a la dolarización de la cartera de colocaciones.

IV. El endeudamiento soberano en moneda extranjera y su implicancia sobre el riesgo país

Continuando con el análisis de las consecuencias de la presencia de moneda extranjera en las economías de los países emergentes, una de las características principales de estas economías es el endeudamiento del sector público en moneda extranjera. Generalmente para financiar las actividades del estado, el sector público utiliza la emisión de instrumentos soberanos, los cuales están dirigidos a inversionistas tanto locales como extranjeros. La importancia del financiamiento público como una porción considerable de la cartera de inversiones en los sistemas bancarios en Latinoamérica pone este tema en la agenda inmediata de los supervisores de la región.

A partir de la información publicada por las agencias supervisoras del sistema financiero de México, Colombia y Ecuador es posible mostrar el grado de importancia de los instrumentos emitidos por el gobierno sobre el total del portafolio de inversiones de las entidades bancarias. El siguiente cuadro presenta el grado de importancia de la deuda pública en los bancos para estos tres países. Se resalta el caso colombiano, donde el 71% de las inversiones totales corresponden a valores del gobierno[19]; en el caso mexicano, este porcentaje es de 63%, pero ha venido aumentando consecutivamente desde el año 2001, cuando este ratio alcanzaba apenas 27%. Para el caso de Ecuador, el porcentaje de inversiones públicas en el total de la cartera de valores de los bancos se ubica en casi 49%.

Cuadro N° 4
Inversión de bancos en instrumentos
del sector público en México, Colombia y Ecuador
(Diciembre 2004)

	Total títulos del Gobierno (A)	Inversiones en valores (B)	Ratio A/B (%)
México (Millones de pesos)	275 952	436 801	**63,2%**
Colombia (Millones Pesos)	23 514 465	33 012 000	**71,2%**
Ecuador (Millones dólares)	629	1 285	**48,9%**

Fuentes: Comisión Nacional Bancaria y de Valores de México, Superintendencia Bancaria de Colombia y Superintendencia de Banca y Seguros de Ecuador.

Adicionalmente a la información provista en el cuadro anterior, en Argentina se estima que el 50% del activo del sistema bancario está invertido en títulos del sector público. Más aún, el Banco Central de Argentina ha decidido aprobar una regulación que, en la práctica, limitará la tenencia de títulos públicos al 40% del activo, el exceso deberá computar a efectos de capital mínimo al 100% de su valor.

[19] Es importante destacar que, en el caso colombiano, las operaciones de mercado abierto, que regulan la liquidez del sistema financiero, se instrumentalizan mediante la compra-venta de bonos del Tesoro (TES) por parte del Banco de la República.

En el caso peruano, tal como se observa en el Cuadro N° 5, los bancos, los fondos mutuos, las administradoras de fondos de pensiones y las compañías de seguros constituyen los principales inversionistas locales. Esto implica que existe un riesgo soberano en el portafolio de inversión de los intermediarios financieros, el cual debe ser reconocido apropiadamente.

Cuadro N° 5
Inversión de bancos, AFPs y compañías de seguros en instrumentos del sector público peruano
(Diciembre 2004, miles de dólares)

	Sistema bancario (A)	Sistema de seguros (B)	Sistema privado de pensiones (C)	Total sistema financiero (D =A+B+C)	Total en circulación (E)	participación (F = D / E)
CDBCRP	1,502,951	2,254	821,006	2,326,211	2,515,235	92%
Bonos del gobierno central	526,972	371,911	942,669	1,841,551	8,183,635	23%
Bonos Bradys		55,576	150,537	206,113	1,239,871	17%
Letras del tesoro						
Total	**2,029,922**	**429,741**	**1,914,212**	**4,373,875**	**6,717,828**	**65%**

Fuente: SBS, MEF, BCRP.

Ningún mercado financiero emergente está ajeno a la participación del sector público como emisor de instrumentos de inversión, a fin de solventar su activa política de financiamiento interno. Esto es, el sector público utiliza la emisión de instrumentos de deuda, los cuales -en general- son considerados de bajo riesgo dentro de un mercado local. No obstante, si estos instrumentos se cotizaran en mercados internacionales, su precio debería reflejar el riesgo crediticio inherente de acuerdo al país emisor.

Sin embargo, para que los instrumentos soberanos reflejen el riesgo crediticio del emisor, estos tienen que ser emitidos en una moneda intercambiable internacionalmente. De allí que muchos gobiernos emitan instrumentos de deuda expresados en una moneda distinta a la local, lo cual no solo conlleva el riesgo crediticio inherente al deudor, sino también un potencial riesgo cambiario resultante de no poder conseguir moneda extranjera para redimir los bonos que han sido emitidos. Este tipo de problema se conoce en la discusión actual como la teoría del "pecado original" [20].

Por ello, si bien es necesario que los gobiernos administren adecuadamente sus finanzas públicas y que no se limite la inversión en instrumentos gubernamentales, no resulta prudente permitir una sobre-exposición de las entidades financieras con el Gobierno. En este sentido, es recomendable diseñar un instrumento de política bancaria que permita el desarrollo del mercado de renta fija gubernamental y sea prudencial en términos de asegurar que los intermediarios financieros asignen capital eficientemente, de acuerdo al grado de riesgo inherente en la compra de instrumentos soberanos.

Al respecto, la propuesta de Basilea II no considera la emisión soberana en moneda extranjera emitida por gobiernos de mercados emergentes como una deuda "de bajo riesgo". Esto representa un serio problema al momento de evaluar la correcta asignación de carga de capital a las exposiciones soberanas en moneda distinta a la local y colocada en el mercado interno, puesto que si bien conllevan un riesgo soberano, dado que el estado no genera recursos en moneda extranjera, el hecho de circular en el

[20] Véase al respecto Eichengreen, Hausmann y Paniza (2003)

mercado interno podría representar para los bancos inversionistas un bajo riesgo de incumplimiento en su portafolio[21]. Más aún, el establecimiento de un requerimiento de capital elevado para esta exposición podría afectar significativamente el mercado de deuda interna. Es por ello que se debe diseñar con mucho cuidado el requerimiento de capital para este tipo de exposiciones no consideradas explícitamente en el NAC, de modo que se pueda discriminar cuando esta exposición implica un riesgo crediticio mayor y cuando no, y así generar incentivos que fomenten un manejo prudencial de la política de inversión en instrumentos soberanos.

En general, un aumento en la exposición de deuda soberana en moneda extranjera, implica una menor diversificación del portafolio de inversiones (i.e. con la consecuente pérdida de granularidad). No obstante, el NAC no considera el caso de una alta concentración del portafolio de inversiones en un solo instrumento, puesto que el parámetro de correlación es fijo (debido a que Basilea considera un modelo unifactorial) y es relativamente bajo (dada la diversificación que caracteriza el portafolio de las mejores empresas de los bancos del G-10). En consecuencia, ante un aumento en la exposición de deuda soberana en moneda extranjera ocurre una subestimación del grado de correlación y de las reservas requeridas, de modo que surge un margen para requerir reservas adicionales que compensen esta subestimación.

Teniendo en cuenta lo anterior, la Superintendencia de Banca, Seguros y AFP de Perú viene evaluando un mecanismo de incentivos para reducir la sobre-exposición a las inversiones en deuda soberana a nivel local. Este mecanismo tendría el rol prudencial de evitar excesos de concentración en deuda soberana, tal como ocurrió con las exposiciones de la banca argentina en la deuda de su gobierno. El mecanismo considera que cualquier exceso sobre los límites prudenciales debería reflejarse en un incremento en el requerimiento de capital de los bancos, por ello –paralelamente- la SBS viene evaluando también el peso ponderado a aplicarse sobre las exposiciones soberanas locales denominadas en moneda extranjera, reconociendo el rol de "*benchmark*" que estas tienen en el desarrollo del mercado de capital doméstico y también el riesgo de descalce que implican al ser emitidas en moneda distinta a la local.

De esta forma, se estaría generando un mecanismo de política que no interferiría con el desarrollo de los mercados de capitales, a la vez que permitiría prudencialmente asignar un peso y requerimiento adecuado a las exposiciones soberanas en moneda extranjera, como una medida temporal hasta que se mejore el modelo interno a través de la introducción de una medida de la concentración del portafolio.

Mientras tanto, con la finalidad de reducir la probabilidad de sobreexposiciones en deuda del gobierno denominada en moneda extranjera, la SBS ha promovido, de manera temporal, el uso de un mecanismo autoregulatorio a través de un límite discrecional para este tipo de exposiciones, el cual ha sido asumido implícitamente por los bancos cuando operan con deuda soberana denominada en moneda extranjera. Este límite es igual a 75% del patrimonio efectivo de las instituciones financieras y es monitoreado mensualmente a través de un reporte preparado con la información provista por la entidades supervisadas. Como consecuencia de la aplicación de este límite implícito, el sistema bancario peruano mantiene al mes de abril de 2005, tenencias de bonos del gobierno denominados en moneda extranjera de solamente el 17% del patrimonio efectivo.

En el marco del enfoque de modelos internos propuesto por el Nuevo Acuerdo de Capital, la SBS también está evaluando la probabilidad de incumplimiento asociada a exposiciones soberanas. De esta forma se

[21] La baja probabilidad de incumplimiento se puede explicar, en el caso peruano, debido a que gran parte de la deuda soberana en moneda extranjera se compone de las obligaciones de encaje que mantienen los bancos en el Banco Central, las cuales se encuentran respaldadas por activos internacionales en bancos de primera categoría.

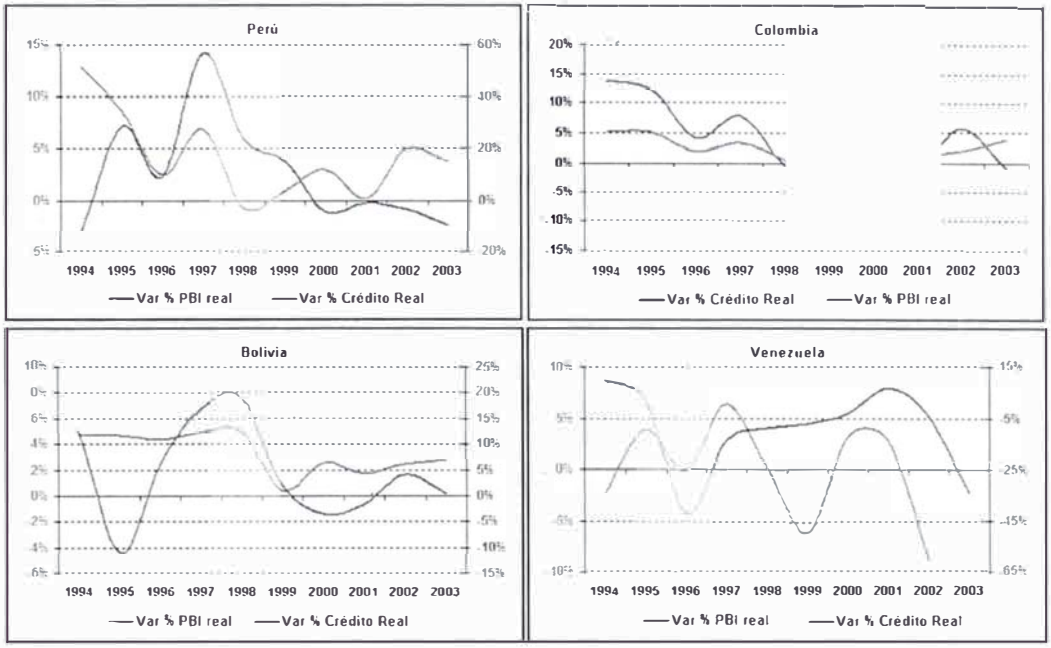
estableceria un límite inferior al requerimiento de capital por deuda soberana emitida en moneda extranjera y colocada en los mercados locales. Dicho límite afectaría el ponderador de riesgo de los activos bancarios según una regla que se determina en función del nivel de reservas, posición de cambio y el valor presente esperado de la cuenta corriente de nuestra economía. En consecuencia, se esperaría que el requerimiento de capital del Pilar I sobre deuda soberana no emitida en moneda local y colocada en el mercado interno sea menor al establecido por el NAC. Ambas políticas tienden a complementarse y, de esta forma, se reconoce todos los riesgos inherentes en una exposición soberana en moneda extranjera, a la vez que se minimizan los costos para las entidades reguladas.

V. El canal crediticio como amplificador del ciclo económico

La evidencia empírica describe recurrentes episodios de abruptas expansiones crediticias seguidas por crisis financieras severas. A nivel internacional se puede hacer referencia a los citados casos de la crisis mexicana en 1994, la recesión en Argentina en 1995, la crisis ecuatoriana de 1998, el episodio recesivo de Indonesia, Corea, Tailandia y Malasia en 1997, la crisis de Rusia en 1998 y de Turquía en 1994.

En Latinoamérica, los episodios de expansión en el crédito en periodos previos a abruptas y prolongadas recesiones son una historia recurrente. El siguiente gráfico muestra los comovimientos entre el nivel de actividad y el crédito doméstico hacia el sector privado de una muestra de 4 países de la región andina. Aunque los periodos no son los mismos, el patrón recurrente que anticipa las recesiones productivas y la contracción del crédito (subrayado en las áreas amarillas) es el de un fuerte crecimiento de las colocaciones correlacionado positivamente con el crecimiento del sector real de la economía.

Gráfico N°4
Comovimientos entre el producto bruto interno
y el crédito doméstico al sector privado en la región andina
(En tasas anuales de crecimiento)



Fuentes: International Financial Statistics (FMI) y Memoria Anual (BCRP).

La explicación de este hecho estilizado[22] es que estas expansiones crediticias podrían conducir a una mala asignación de recursos si los bancos (dispuestos a prestar sus fondos excedentes) relajan sus mecanismos de selección de préstamos, lo cual trae como consecuencia el posterior deterioro del portafolio bancario. Este relajamiento ocurre porque las expansiones crediticias están altamente correlacionadas con la fase expansiva del ciclo económico.

Precisamente, durante esa fase, los niveles de actividad de la economía crecen, los niveles de ahorro aumentan y la oferta de fondos prestables se incrementa. Además, las fases expansivas convierten a una pequeña economía abierta dependiente de capitales extranjeros en una alternativa más segura y rentable de inversión para los inversionistas extranjeros, lo que facilita que los intermediarios financieros locales accedan a financiamiento internacional de bajo costo, el cual se puede trasladar al sector real a través de menores tasas de interés. La posibilidad de mayor inversión y consumo a menores tasas de interés, el incremento en la oferta de fondos prestables y las mejoras en la actividad económica conducen a que los intermediarios financieros sean optimistas en su negocio, incrementando la oferta de créditos y reduciendo los límites al endeudamiento doméstico.

Este incremento no sería preocupante, si respondiese a fundamentos económicos. Sin embargo, si el incremento es excesivo y va acompañado del relajamiento de las condiciones para el otorgamiento de los préstamos, entonces se puede esperar que impactos negativos que afecten la actividad económica incrementen la fragilidad de los intermediarios financieros, debido a que afectan principalmente a aquellos clientes bancarios que son más riesgosos o que poseen proyectos más vulnerables. Por ello, un impacto adverso que revierta el ciclo económico hacia su fase recesiva deterioraría sustancialmente el portafolio

[22] Véase Tornell, Westerman y Martinez (2004) y Chinn y Kletzer (2000).

bancario de aquellos intermediarios que, al no considerar adecuadamente el riesgo de sus clientes, relajaron sus requerimientos para otorgar créditos.

Sin embargo, no se puede limitar el crecimiento del crédito puesto que se estaria amplificando la recesión dentro del ciclo económico. Debido a esto, la imposición de límites directos al crecimiento del crédito pueden tener un efecto perjudicial sobre el financiamiento de la actividad económica. Por ello, es conveniente buscar un instrumento de política regulatoria que no signifique un límite al crecimiento económico, sino más bien, un incentivo a que los intermediarios financieros puedan colocar adecuadamente sus recursos, tomando en cuenta los riesgos en cada fase del ciclo económico, a la vez que puedan amortiguar el efecto que el ciclo económico sobre la oferta de créditos bancarios. De esta forma, este mecanismo debería ayudar a suavizar el ciclo económico sin afectar el desarrollo de largo plazo de una economía.

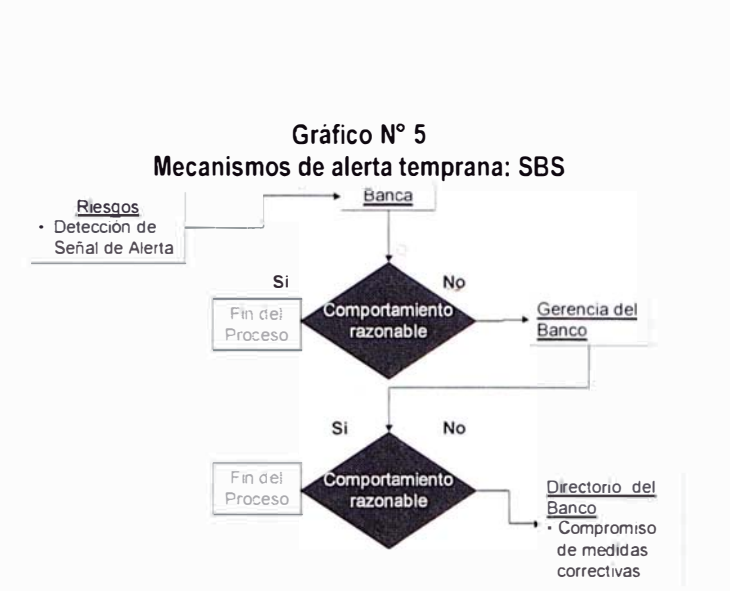
Al respecto, se debe precisar que en el caso de las economías emergentes, donde las fases de cada ciclo se amplifican pero con menor persistencia (i.e. son más volátiles), el requerimiento adicional de capital aplicado en periodos de relativa estabilidad macroeconómica permite reducir el efecto amplificador de los ciclos crediticios. Esto es así porque los requerimientos de capital que se extraen de las estimaciones de Basilea II consideran un horizonte muestral de 5 años, el cual no permite cubrir el espectro de un ciclo económico completo. En principio, esta observación no implica serios problemas para economías desarrolladas, donde los ciclos económicos no son tan volátiles[23] y, por lo tanto, las estimaciones pueden tener un pequeño sesgo positivo o negativo dependiendo si los cálculos fueron realizados durante una fase expansiva o recesiva. Sin embargo, en el caso de economías emergentes, este sesgo puede ser considerable dada la severa amplificación del ciclo económico. Para evitar este problema, se propone que la aplicación de un requerimiento de capital que proviene de estimaciones y calibraciones obtenidas durante fases expansivas del ciclo debería complementarse con un requerimiento adicional, el cual compensaría este sesgo.

En otras palabras, el requerimiento de capital constituye un estabilizador automático en estas economías, el cual puede ser usado para amortiguar los efectos de los ciclos económicos. En épocas de expansión económica, ese requerimiento adicional contribuye a suavizar cualquier incremento de créditos encima de lo requerido por los fundamentos de la economía. Por otro lado, en épocas de recesión, permite a los intermediarios financieros no amplificar el ciclo económico (profundizando la recesión), puesto que podría destinar el capital adicional a compensar efectos de pérdidas esperadas y no esperadas generadas por el ciclo recesivo.

Un sistema de monitoreo de la exposición crediticia según cada producto bancario constituye un mecanismo complementario a la reserva de capital adicional. Este sistema, desarrollado por la Superintendencia de Banca y Seguros del Perú, permite medir los efectos del ciclo crediticio. Por ejemplo, a partir de dicho sistema, el crecimiento abrupto por encima de un límite que no se encuentre respaldado por fundamentos económicos activaría un mecanismo de alerta, el cual motiva una recomendación para el banco o los bancos que incurran en este crecimiento excesivo.

[23] No obstante, incluso en economías desarrolladas, el tema de la prociclicidad del acuerdo ha sido discutido tanto empírica como teóricamente. Al respecto se puede citar los recientes estudios de Gordy y Howells (2004), Kashyap y Stein (2003) o Canta (2005).

Gráfico N° 5
Mecanismos de alerta temprana: SBS



El Cuadro No 5 presenta el sistema operativo de la alerta emitida por la SBS. Para entenderlo en detalle, se debe precisar que la SBS modificó su estructura orgánica y creó un área especializada en la supervisión de los riesgos de mercado, crediticio y operacional dentro de la institución (denotada como "Riesgos" en el gráfico). Esta modificación de la estructura orgánica y su adecuación a un esquema de supervisión basada en riesgos es una condición previa para una correcta aplicación del NAC.

Regresando al análisis del mecanismo de alerta propuesto por la SBS, el Gráfico No 5 señala que es el área de Riesgos la que emite una señal de alerta, la cual es reportada al área de supervisión bancaria (denotada como "Banca"). En esta área se evalúa si dicha alerta responde a un comportamiento razonable y, de no ser el caso, se reporta a la gerencia del Banco, la cual deberá justificar el comportamiento o informar al directorio de la empresa financiara a fin de que se adopten las medidas correctivas.

Asimismo, este sistema de monitoreo y alerta temprana activa la exigencia de un mayor requerimiento discrecional de capital, el cual disuade un mayor crecimiento de la oferta de crédito. En general, con ambas medidas se busca suavizar los efectos amplificadores de los ciclos económicos y establecer un requerimiento de capital promedio relativamente estable en el tiempo.

VI. Conclusiones

En este artículo se exponen una serie de riesgos materiales adicionales a los tres riesgos contemplados en el primer pilar del NAC (crediticio, de mercado y operacional): el riesgo sistemático derivado de una clara tendencia hacia sistemas bancarios más concentrados a nivel internacional, el riesgo crediticio generado por la dolarización de los préstamos otorgados a deudores que perciben ingresos en la moneda local, el aumento del riesgo soberano cuando esta deuda está denominada en moneda extranjera, y la amplificación de los ciclos económicos ante la presencia de un canal crediticio. El artículo sostiene que todos estos riesgos adicionales deberían ser incorporados en metodologías objetivas similares a las de los modelos internos considerados en el primer pilar, de modo que se eviten normas y políticas de supervisión disímiles entre países y que, eventualmente, podrían generar alguna forma de arbitraje regulatorio.

Asimismo, el artículo propone una serie de medidas complementarias que pueden ser aplicadas por las agencias gubernamentales supervisoras del sistema financiero para contrarrestar los efectos de los

riesgos adicionales antes mencionados, presentes en los mercados financieros internacionales, especialmente de los países emergentes. Estas medidas -en conjunto- tienen como objetivo reducir los impactos del incremento del riesgo sistémico debido a la concentración, y fomentar una mayor diversificación del portafolio bancario.

Tal como se revisó en la sección anterior, la ventaja del uso del requerimiento adicional de capital establecido en el segundo pilar del NAC radica en que, de ser aplicado -discrecionalmente- a bancos internacionales, este requerimiento evitaría que los bancos de gran escala con problemas trasladen sus pérdidas a otras regiones y, de esta forma, reduciría la volatilidad de los flujos de capitales y sus posibles efectos macroeconómicos adversos sobre los bancos de países emergentes, generaría incentivos para un manejo prudente de los riesgos bancarios y, a la vez, reduciría los incentivos para la "concentración-no-competitiva" en el sistema financiero. Así, este requerimiento discrecional se convierte en una herramienta importante para que el supervisor bancario pueda mantener la estabilidad del sistema financiero y, a la vez, reducir cualquier efecto negativo originado por eventos macroeconómicos adversos.

De otro lado, para contrarrestar el efecto de un descalce de monedas generado por la dolarización, así como el inherente riesgo crediticio cambiario que se genera cuando los bancos prestan a empresas del sector real que no generan ingresos en moneda extranjera, la Superintendencia de Banca, Seguros y AFP de Perú, siguiendo los procesos establecidos en el Pilar I respecto de la adecuada identificación y medición de riesgos, está evaluando complementar el requerimiento adicional de capital con el establecimiento de categorías de riesgo asociadas a una probabilidad de incumplimiento que incorpore los efectos por descalce de monedas.

Adicionalmente, con el objetivo de complementar el uso del requerimiento adicional y discrecional de capital, se viene evaluando la correcta aplicación del requerimiento de capital por deuda soberana emitida en moneda extranjera, a través de la incorporación de un esquema de incentivos que eviten excesos en la exposición soberana, de modo que toda sobre-exposición en estos instrumentos se traducirían en mayores requerimientos de capital.

Finalmente, debe advertirse que la aplicación del requerimiento adicional y discrecional, conjuntamente con las políticas complementarias establecidas en las secciones anteriores, constituye un grupo de opciones de política en línea con lo establecido en el Nuevo Acuerdo de Capital Basilea II. En general, todas las políticas pueden ser aplicadas con relación a una exigencia adicional de capital, sin embargo, definir una metodología que considere estos riesgos como parte del método avanzado es un objetivo desafiante que debe ser necesariamente parte de la agenda inmediata del Comité de Basilea; y -mientras tanto- corresponde a los supervisores bancarios sugerir –como lo hemos tratado de hacer en este trabajo- mecanismos regulatorios temporales que permitan aliviar el impacto adverso que se origina en estos riesgos macroeconómicos.

VII. Referencias

Allen, F. y D. Gale, 2003. *"Competition and Financial Stability."* En: Journal of Money, Credit, and Banking, Vol. 36 No. 3, Pág. 453-480.

Beck, T., Demirgüç-Kunt, A. y R. Levine, 2003. *"Bank concentration and crises"* NBER Working Paper No. 9921.

Berger, A., Demsetz, R y P. Strahan, 1999. *"The consolidation of the financial services industry: causes, consequences, and implications for the future"* En: Journal of Banking and Finance Vol. 23. Pág. 135-194.

Boyd, J. y S. Graham, 1991. *"Investigating the banking consolidation trend"* En: Federal Reserve of Minneapolis Quaterly Review Vol. 15 No. 2. Pág.3-12.

Caballero, R. y A. Krishnamurthy. 2004. *"Exchange rate volatility and Credit Channel in Emerging Markets"*. NBER Working Paper No. 10517.

Calvo, G. 1999. «Contagion In Emerging Markets: When Wall Street is a Carrier». Documento presentado en la Reunión AEA 1999, New York .

Canta, M. 2005. " Business Cycle Effects of the New capital accord in a DGE Model" En: The Macroeconomics of Banking Regulation. Disertación Doctoral, McGill University.

Chinn, M y K. Kletzer 2000. *"International capital inflows, domestic financial intermediation and financial crisis"*. NBER Working Paper No.7902.

Claessens, S. y L. Laeven, 2003. *"What Drives Bank Competition? Some International Evidence"* Manuscrito preparado para The World Bank and Federal Reserve Bank of Cleveland Conferences on Bank Competition.

Eichengreen, Barry; Hausmann, R. y U. Paniza, 2003. *"Currency Mismatch, debt intolerance and Original Sin"* NBER Working Paper No. 10036.

Gordy M. y B. Howells, 2004. "Prociclicality in Basel II: Can We Treat the Disease Without Killing the Patient? Board of Governors of the Federal Reserve System, Manuscrito.

Group of Ten, 2001. Report on Consolidation in the Financial Sector, Bank for International Settlements: Basel, Switzerland.

Hellmann, T. Murdoch K. y J. Stiglitz, 2000. *"Liberalization, Moral Hazard in Banking and Prudential Regulation: Are Capital Requirements Enough?"* En: American Economic Review, Vol. 90 No. 1, 147-165.

International Monetary Fund, 2001. Financial Sector Consolidation in Emerging Markets. International Capital Market Report.

Kashyap, A. y J. Stein, 2003. "Cyclical Implications of the Basel-II Capital Standard" En: Federal Reserve Bank of Chicago Economic Perspectives, Primer Trimestre 2004, Pág. 18–31.

Levy Yeyati E. y Sturzenegger, F. 2003. Dollarization: Debates and Policy Alternatives. MIT Press, Cambridge, Massachussets.

Stiglitz, J. 2004. "Capital Market Liberalization, Globalization and the IMF" En: Oxford Review of Economic Policy, Vol. 20 No. 1

Stiglitz, J. y B. Greenwald, 2003. Towards a New Paradigm in Monetary Economics. Cambridge University Press.

Tirole, J., 2002. Financial Crisis, Liquidity and the International Monetary System. Princeton University Press.

Tornell, A. y F. Westerman, 2002. "*Boom-Bust Cycles in Middle Income Countries*" NBER Working Paper No. 9219.

Tornell, A.; Westerman, F y L. Martinez, 2004. "*The positive link between financial liberalization, growth and crisis*" NBER Working Paper No. 10293.

Valdés, R. 1997. «Emerging Market Contagion: Evidence and Theory», Banco Central de Chile, Documento de Trabajo No 7.