



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

Desarrollo de una propuesta metodológica para la gestión del riesgo operacional en una entidad financiera

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Miguel Angel HUAROTO MANCO

Omar LÓPEZ TAPIA

ASESOR

César Augusto ALCÁNTARA LOAYZA

Lima, Perú

2011



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Huaroto, M. & López, T. (2012). *Desarrollo de una propuesta metodológica para la gestión del riesgo operacional en una entidad financiera*. [Tesina de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Académico Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA DE TITULACIÓN EXTRAORDINARIA 2011-1

Acta de Sustentación de Tesina

Siendo las... 8:15 del día ... 25 ... de Enero del 2012, se reunieron los docentes designados como miembros de Jurado de la Tesina; presidida por el Licenciado William Martin Enriquez Maguiña, la Doctora Nora Bertha La Serna Palomino (Miembro) y el Licenciado Cesar Augusto Alcántara Loayza (Miembro asesor) para la sustentación de la Tesina intitulada: **“DESARROLLO DE UNA PROPUESTA METODOLOGICA PARA LA GESTION DEL RIESGO OPERACIONAL EN UN ENTIDAD FINANCIERA”**, por el Sr. Omar López Tapia; para optar el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición de la Tesina, el Presidente invitó al graduando a dar respuesta a las preguntas establecidas por los Miembros de Jurado.

El graduando en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros de Jurado, el graduando obtuvo la nota de ... 14 ... (En letras) Calonce

A continuación el Presidente del Jurado, Lic. William Martin Enriquez Maguiña declara al graduando **Omar López Tapia, Ingeniero de Sistemas.**

Siendo las 21:15 horas, se levantó la sesión.

.....
Presidente

Lic. William Martin Enriquez Maguiña

.....
Miembro

Dra. Nora Bertha La Serna Palomino

.....
Miembro Asesor

Lic. Cesar Augusto Alcántara Loayza

El presente trabajo está dedicado a nuestras Familias, Profesores y Amigos que con su confianza, saber y apoyo incondicional nos han acompañado y guiado. Especialmente a nuestros Padres por su cariño y comprensión, bases fundamentales en nuestra formación profesional.

AGRADECIMIENTOS

Al profesor Lic. Cesar Augusto Alcántara Loayza, por su orientación y dedicación para que este trabajo cumpla con los objetivos trazados.

A los profesores de la Universidad Nacional Mayor de San Marcos, nuestro reconocimiento y agradecimiento, porque de ellos recibimos buenas enseñanzas que nos han servido de ejemplo para el desarrollo de nuestra vida profesional.

A nuestros amigos, pero una mención especial para Eisenhower Guillén Quijano, por el apoyo incondicional que nos brinda, por ser un buen amigo, por confiar en nosotros, por acompañarnos no solo en los momentos buenos, sino también en los malos, que es cuando verdaderamente llegas a conocer a tus amigos.

A todas aquellas personas que indirectamente nos ayudaron para la culminación de este trabajo y que muchas veces constituyen un gran apoyo moral.

RESUMEN

En la actualidad, las operaciones de las empresas del sistema financiero, particularmente de aquellas con procesos de alto volumen y/o diversidad de transacciones, conlleva la posibilidad de fallas o insuficiencias que pueden ocasionar pérdidas de eficacia operacional y recursos financieros. Es por ello la importancia de establecer una metodología y un sistema informático que contribuya a la mitigación y reducción de los riesgos operacionales críticos, buscando elevar el nivel de confiabilidad y disponibilidad de los procesos de negocio.

En este contexto, la presente investigación tiene como finalidad elaborar una metodología que permita a una institución financiera realizar una adecuada gestión de riesgos asociados a la tecnología de la información, relacionados a fallas de seguridad de información y continuidad operativa de los sistemas informáticos. En ese sentido, se ha implementado una política en el Banco de la Nación, basada en las buenas prácticas establecidas por el comité de Basilea II y reglamentadas por la Superintendencia de Banca, Seguros y AFP's, que establece procedimientos para la identificación, evaluación, monitoreo y control de riesgos operacionales, posibilitando la consolidación de eventos de pérdida por unidad de negocio de las posibles eventualidades o riesgos materializados presentados en los diferentes procesos que soporta la institución financiera.

ABSTRACT

Nowadays the finance system companies' deals, specially those with a high rate process/diversity procedures, leads to the possibility of failures and insufficient tasks that might cause losses of dealing efficacious and finance resources. It is for this reason the importance to set a methodology and a computer system that support the shortening and reduction of the dealing risks, trying for rising the rate of confidence and available in the process of business.

In this picture, the recent search has as an aim to elaborate a methodology that allows a finance undertaking to carry out a proper procedure of risk related to the computing technology, related to computer safety failure and a workable follow up of the computer systems.

This way, in the Banco de la Nación has been taken place a policy, based on the good trainings set by the comittee of Basilea II and the regulations by the insurance superintendency and AFP that set procedures to identify, evaluate, monitor and control of dealing risks, allowing the consolidation of event of loss per business unit of the posible downsides or risks materialized introduced in the different process that supports the finance company.

INDICE

INDICE DE FIGURAS	11
INTRODUCCION.....	12
1 CAPITULO I. PLANTEAMIENTO METODOLÓGICO	14
1.1 Antecedentes.....	14
1.2 Definición del problema	17
1.3 Objetivos	20
1.3.1 Objetivo General	20
1.3.2 Objetivos Específicos.....	20
1.4 Justificación.....	21
1.4.1 Justificación de carácter Teórico	21
1.4.2 Justificación de carácter Práctico	21
1.5 Propuesta Metodológica	23
1.6 Organización de la tesina	24
2 CAPITULO II.- MARCO TEORICO	26
2.1 Conceptos Inmersos en los Riesgos de Tecnología.....	26
2.1.1 Metodología.....	26
2.1.2 Riesgo.....	26
2.1.3 Calificación y cuantificación de un riesgo.....	27
2.1.4 Concepto de Riesgo de Tecnología de Información	29
2.1.5 Gestión Integral de Riesgos	30
2.1.6 Seguridad de Información	31
2.1.7 Plan de Continuidad de Negocios	32
2.1.8 Orígenes de la Administración de los Riesgos de Tecnología.....	33
2.1.9 Nuevo Acuerdo de Capital (NAC) - BASILEA II	34
2.1.10 Información y Sistema Informático	36
2.1.11 Confidencialidad	38
2.1.12 Integridad	38
2.1.13 Disponibilidad	39
2.1.14 Amenazas a la Información	40
2.1.15 Ataques Pasivos	41

2.1.16	Ataques Activos	41
2.1.17	Otros Aspectos Relacionados.....	42
3	CAPITULO III. ESTADO DEL ARTE METODOLÓGICO	44
3.1	Metodologías Similares	44
3.1.1	Metodología MAGERIT	44
3.1.2	Metodología OCTAVE	46
3.1.3	Metodología CRAMM	49
4	CAPITULO IV. DESARROLLO DE LA SOLUCIÓN O DEL ESTUDIO	50
4.1	Introducción	50
4.2	Objetivo General.....	51
4.3	Alcance.....	51
4.4	Base Legal o Administrativa.....	51
4.5	Definición de Términos	52
4.6	Disposiciones Generales	54
4.7	Disposiciones Específicas.....	55
4.7.1	Metodologías para la Gestión del Riesgo Operacional	55
4.7.2	Etapas de la Metodología para la Evaluación de Riesgos Operacionales	56
4.7.2.1	Identificación de Riesgos.....	56
4.7.2.1.1	Analizar el Contexto	56
4.7.2.1.2	Identificar Riesgos	57
4.7.2.2	Evaluación de Riesgos	59
4.7.2.2.1	Evaluar Riesgos.....	59
4.7.2.2.2	Identificar Controles.....	64
4.7.2.2.3	Evaluar la Efectividad de los Controles.....	64
4.7.2.3	Tratamiento de riesgos.....	69
4.7.2.3.1	Definir Tratamiento.....	69
4.7.2.3.2	Monitorear Planes de Acción	70
4.8	Responsabilidades.....	71
4.8.1	De la División Riesgos De Operación	71
4.8.2	De las Jefaturas de Departamento	72
4.8.3	De la División de Soporte Regional y Zonal Lima.....	73
4.8.4	Del Analista de Riesgos de Operación	74
4.8.5	Del Coordinador de Riesgos.....	74

4.8.6	Del Administrador de Sucursales y Agencias de Lima y Provincias	75
4.8.7	El Coordinador de Eventos de Perdida.....	76
4.8.8	Del Departamento de Auditoria.....	76
5	CAPÍTULO V. DESCRIPCIÓN DE LA SOLUCIÓN TECNOLÓGICA	83
5.1	Especificación de Requerimientos del Software (SRS)	84
5.1.1	Introducción.....	84
5.1.2	Propósito	84
5.1.3	Alcance	84
5.1.4	Definiciones	85
5.1.5	Referencias.....	85
5.1.6	Generalidades	85
5.1.7	Consideraciones y Dependencias	86
5.2	Requerimientos Funcionales.....	86
5.2.1	Funcionalidad	86
5.2.1.1	Registro de las cuentas Contables	86
5.2.1.2	Reporte Requerimiento de Pérdida por Riesgo Operacional por Riesgo Operacional	86
5.2.1.3	Almacenar Histórico del Requerimiento de Eventos de Pérdida por Riesgo Operacional	87
5.2.1.4	Reportes Estadísticos.....	87
5.2.1.5	Seguridad.....	87
5.2.1.6	Configuración y Mantenimiento	87
5.3	Modelo de Paquetes / Módulos	88
5.3.1	Paquete Configuración y Mantenimiento	88
5.3.2	Paquete Ingreso de Datos	88
5.3.3	Reportes y Estadísticas	88
5.4	Modelo de Casos de Uso	89
5.5	Resumen de Actores y Casos de Uso	90
5.6	Reporte de Requerimientos	92
5.6.1	Sistemas Operativos	92
5.6.2	Sistema de Gestión de Base de Datos.....	92
5.6.3	Servidor de Aplicaciones	92
5.6.4	Servidor Web	92

5.6.5	Otras Aplicaciones.....	92
5.7	Requerimientos No Funcionales	93
5.7.1	Facilidad de Uso.....	93
5.7.1.2	Facilidad de ingreso	93
5.7.1.3	Minimización del Error	93
5.7.1.4	Navegación	93
5.7.1.5	Entendimiento del aplicativo	93
5.8	Confiabilidad.....	94
5.8.1	Tiempo de Duración de Sesión del Usuario.....	94
5.9	Desempeño.....	94
5.9.1	Tiempo de Respuesta	94
5.9.2	Tiempo de espera	94
5.10	Facilidad de Soporte	94
5.10.1	Sobre el estándar para la codificación de los programas.....	94
5.10.2	Sobre el estándar para Diseño de la Base de Datos.....	94
5.11	Restricciones de Diseño	95
5.11.1	Restricciones sobre la Arquitectura	95
5.11.2	Estructura en Capas de la Arquitectura	95
5.11.2.2	Sobre el Lenguaje de Programación	95
5.11.3	Restricciones sobre los Componentes.....	95
5.12	Interfaces	96
5.12.1	Interfaces de Usuarios	96
5.12.2	Interfaces de Hardware	100
5.12.3	Interfaces de Software	100
5.12.4	Interfaces de Comunicación	100
5.13	Documentación en Línea y Requerimientos de Ayuda del Sistema	100
5.14	Requerimientos de Licencia.....	100
5.15	Metodología de Desarrollo	100
5.16	Componentes Adquiridos.....	100
5.17	Otros Estándares Aplicables.....	101
6.	CONCLUSIONES Y RECOMENDACIONES	102
7.	REFERENCIAS BIBLIOGRÁFICAS	104
8.	ANEXOS	105

INDICE DE FIGURAS

- Figura 1.1. Cronología de Avances en la Implementación de Acuerdos de Basilea II
- Figura 1.2. Análisis de Pérdidas debido a Eventos de Riesgo
- Figura 1.3. Pérdidas debido a Eventos de Riesgo Operacional
- Figura 1.4. Pérdidas Netas del Sistema Financiero debido a Eventos de Riesgo Operacional
- Figura 1.5. Pérdidas por Eventos de Riesgo Operacional en el Sistema Financiero Mundial
- Figura 1.6. Formato para Eventos de Pérdida por Riesgo Operacional de la SBS
- Figura 3.1. Pasos realizados por Magerit
- Figura 3.2. OCTAVE está impulsado por el riesgo operativo y prácticas de seguridad
- Figura 4.1. Committee of Sponsoring Organizations of Treadway Commision
- Figura 4.2. Etapas de la Metodología
- Figura 4.3. Pasos para identificar los riesgos.
- Figura 4.4. Inventario de Procesos, Subprocesos, y Actividades
- Figura 4.5. Pasos para proceso de evaluación
- Figura 4.6. Matriz de Evaluación del Nivel de Riesgo
- Figura 4.7. Pasos para tratamiento de riesgo
- Figura 4.8. Pasos para la Aplicación de la Metodología
- Figura 4.9. Ficha de Registro de Riesgos N° 1
- Figura 4.10. Ficha de Registro de Riesgos N° 2
- Figura 4.11. Formato de Autoevaluación de Riesgos
- Figura 4.12. Ficha de Plan de Acción

INTRODUCCION

En la actualidad a raíz de la reciente crisis financiera internacional, que evidenció la necesidad de fortalecer la regulación, supervisión y gestión de riesgos del sector bancario, el Comité de Basilea inició en el 2009 la reforma de Basilea II¹, actualmente llamada Basilea III. En este sentido, la SBS² actualmente está evaluando la implementación de estos cambios de acuerdo a la realidad peruana³. Para lo cual se ha normado mediante la Resolución SBS N° 2116 – 2009 para la Gestión del Riesgo Operacional y la Circular SBS N° 140 – 2009 para la Gestión de la Seguridad de la Información.

En este contexto, a nivel internacional se han desarrollado algunos sistemas relacionados a la administración de riesgos operacional como son el ObjectRisk, sistema de Administración de Riesgo Operativo que posibilita la creación de programas integrados de Gestión de Riesgo para cumplir el Nuevo Acuerdo de Basilea II, de la empresa Microsoft. Así también, el sistema Accelerate de la empresa Chase Cooper, que permite facilitar la labor de análisis, evaluación, registro y comunicación de riesgos identificados. Cabe mencionar que ambos sistemas utilizan una arquitectura cliente servidor lo que genera grandes costos operativos (licencias, soporte, instalación, hardware) y dependencia de la empresa propietaria del software.

¹ Comités de Basilea: Organización mundial constituida por los presidentes de los bancos centrales de los once países miembros del Grupo de los Diez (G-10) que reúne a las autoridades de supervisión bancaria, cuya función es fortalecer la solidez de los sistemas financieros.

² SBS : Superintendencia de Banca, Seguro y AFP

³ Portal SBS

Sin embargo, el presente trabajo está alineado y personalizado a los lineamientos establecidos en la regulación peruana mediante la resolución SBS 2116-2009 y la circular SBS G-140-2009, mencionadas anteriormente. En tal sentido, la metodología implementada permitirá establecer una guía para el tratamiento de los riesgos operacionales presentes en las tecnologías de información, identificando sus posibles amenazas y vulnerabilidades. Estos lineamientos deben permitir establecer todos los mecanismos necesarios para cuantificar y calificar los niveles de riesgos operacionales, además de determinar los diversos controles para minimizarlos. Así mismo mediante el desarrollo e implementación de esta metodología, se estaría facilitando a las entidades financieras, cumplir con lo normado por la SBS respecto al tema de Evaluación de Riesgos de Tecnología de Información. Asimismo, se constituye un avance fundamental que el soporte a esta metodología sea un sistema con arquitectura web, a diferencia de los sistemas de tipo cliente servidor, mencionados en el párrafo anterior, toda vez que ello contribuirá al despliegue de la metodología en toda la organización.

1 CAPITULO I. PLANTEAMIENTO METODOLÓGICO

1.1 Antecedentes

El Comité de Basilea fue establecido en 1975 por los presidentes de los bancos centrales de los once países miembros del Grupo de los Diez (G-10) y desde un inicio se constituyó en un foro de discusión para fomentar la mejora y la convergencia de las prácticas y normativas de supervisión bancaria, buscando perfeccionar las herramientas de fiscalización internacional, a través de acercamientos y de estándares comunes.

En 1988, el Comité aprobó el denominado Acuerdo de Capital de Basilea (Basilea I), que introducía un requerimiento de patrimonio (recursos propios) del 8% en función de los riesgos asumidos, principalmente de crédito⁴.

En junio de 2004 se publica los acuerdos de Basilea II cuyo principal propósito es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

Posteriormente como se señala en la siguiente cronología los países a través de sus entes reguladores del sistema financiero empiezan a adoptar los acuerdos y recomendaciones propuestos en Basilea II.

⁴ http://www.sbs.gob.pe/repositorioaps/0/0/jer/REGUL_PROYIMP_BASIL_FUNSBS/ASBANK.pdf

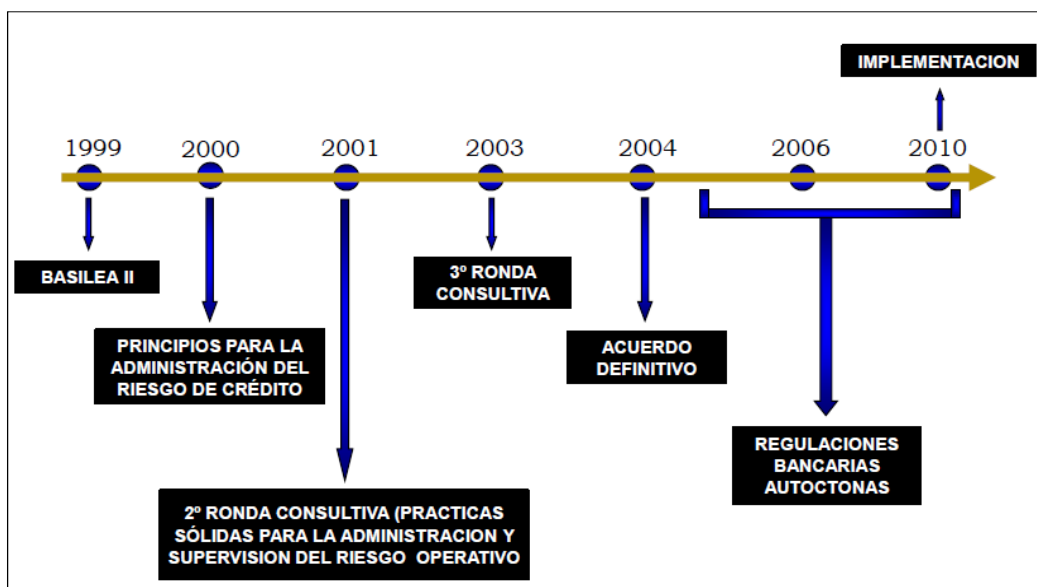


Figura 1.1. Cronología de Avances en la Implementación de Acuerdos de Basilea II

En el Perú, la Superintendencia de Banca y Seguros (SBS), ha implementado un proceso de estandarización de procesos de control que las entidades del sistema financiero deben cumplir para adecuarse a los estándares internacionales y a las mejores prácticas con relación a la administración de estos riesgos.

La Superintendencia, emitió el año 2002, la Circular N° G-105-2002 la misma que estipula los puntos de partida que se debe considerar para la adecuada administración de los riesgos de tecnología de información y la elaboración de los respectivos documentos de apoyo el plan de seguridad de información y el plan de continuidad de negocio, a esto se suma la reciente Circular N° 37-2008 la cual establece la adecuación al nuevo enfoque de Administración Integral de Riesgos.

En junio de 2004, se aprobó un Nuevo Acuerdo de Capital, el cual establece una serie de principios y recomendaciones sobre Supervisión Bancaria, cuyo objetivo es propiciar la convergencia regulatoria hacia los estándares más eficaces y avanzados sobre medición y gestión de los principales riesgos en la industria bancaria. Cabe señalar que uno de los puntos que se desprende de los principios propuestos por el Comité de Basilea II (Nuevo Acuerdo de Capital - NAC), es que las entidades financieras deberán de establecer y asignar el capital necesario a posible materialización de los eventos de riesgos que pudieran generar una crisis bancaria.

Finalmente, en abril del 2009 se emitió la Resolución N° 2116-2009, Reglamento de la Gestión Integral de Riesgos, que establece que las empresas supervisadas deben contar con una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios. Esta resolución se complementa con la circular N° G-140-2009, Gestión de la seguridad de la información, con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información.

1.2 Definición del problema

Las entidades financieras tienen pérdidas directas e indirectas (recursos económicos, reputación, problemas legales, etc.) debido a que no administran o gestionan adecuadamente los riesgos operacionales relacionados a las TI⁵ y no contar con una metodología para ello.

La administración y tratamiento de los riesgos de tecnologías de información como un factor que origina riesgos operacionales⁶ es un requerimiento oficial en nuestro país. Su no implementación puede afectar el desarrollo de las operaciones y servicios que realiza una institución financiera al atentar contra la confidencialidad, integridad y disponibilidad de la información. Cuando empiezan a aparecer las normas y procedimientos de mejores prácticas, las regulaciones y los estándares relacionados a riesgos de operación, es que el proceso de administración de riesgos adopta realmente la dimensión que tiene ahora.

Debido a la falta de implementación de estas normas las entidades financieras tienen pérdidas directas e indirectas (recursos económicos, reputación, problemas legales, etc.) debido a que no administran o gestionan adecuadamente los riesgos operacionales relacionados a las TI y SI⁷.

⁵Tecnología de Información

⁶ Entre los riesgos que enfrentan las empresas supervisadas en el desarrollo de sus actividades se encuentra el riesgo operacional, el cual puede generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos. Reglamento para la Gestión del Riesgo Operacional - Resolución SBS N° 2116-2009.

⁷ Formato de Eventos de pérdida por Riesgo Operacional

https://extranet.sbs.gob.pe/docs-igro/Cuestionario_aspectos_cualitativos_BD_Eventos_Perdida_Rop.xls

Asimismo, considerando la necesidad de cumplir con las exigencias de la Resolución N° 2116-2009 relacionada a la adecuada implementación de políticas y procedimientos para administrar los riesgos operativos, el Banco debe someterse a los requerimientos regulatorios con el claro objetivo de salvaguardar la información que administra sobre todo destinada a satisfacer a sus clientes.



Información empleada en el análisis

Información de eventos de pérdida:

- Provenientes de 15 bancos del sistema financiero*
- Registrados contablemente en el periodo comprendido entre enero 2010 y abril 2011 (16 meses de data disponible)
- Mayores a 3mil NS (para casi la totalidad del análisis)

(*) Dos bancos fueron excluidos del análisis

Figura 1.2 Análisis de Pérdidas debido a Eventos de Riesgo Operacional

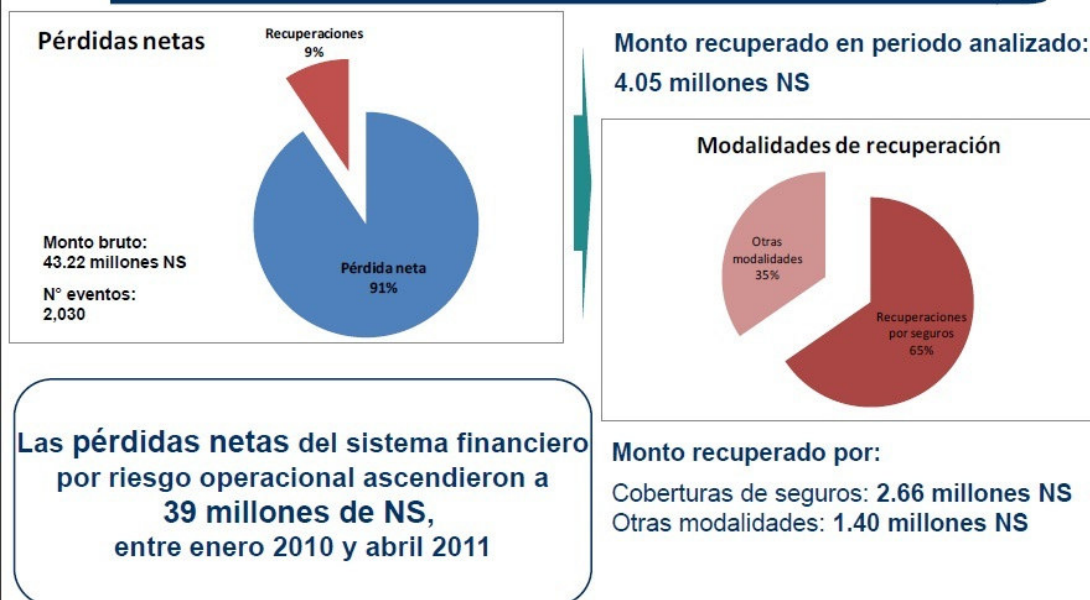


Entre 2010 y 2011, los Bancos han alcanzado un monto bruto de pérdidas de 48M de NS debido a eventos de riesgo operacional

	Pérdidas totales		Pérdidas >= S/. 3,000		Pérdidas promedio por banco >= S/. 3,000	
	N° eventos	Monto bruto (Millones NS)	N° eventos	Monto bruto (Millones NS)	N° eventos	Monto bruto (NS)
Total (15 bancos del SFP)	12,489	48.37	2,030	43.22	135	21,280

Figura 1.3. Pérdidas debido a Eventos de Riesgo Operacional

**Sólo 9% de las pérdidas son recuperadas;
siendo la principal modalidad de
recuperación las coberturas por seguros**



Información de enero 2010 a abril 2011, de acuerdo a fecha de registro contable del evento

17

Figura 1.4. Pérdidas Netas del Sistema Financiero debido a Eventos de Riesgo Operacional

⁸ Documento de presentación de la SBS ante el comité de Riesgo Operacional ASBANC,
PresentaciónDSRO_versiónAsbanc_Nov2011

1.3 Objetivos

1.3.1 Objetivo General

Diseñar una metodología que se utilice como política en una institución financiera para realizar una adecuada gestión de riesgo operacional, el cual incluye los relacionados a tecnologías de la información como fallas de seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo de la implementación de dichos sistemas y la compatibilidad e integración de los mismos así como problemas de calidad de la información. Con estos parámetros y lineamientos se desarrollará e implementará un sistema de información de riesgos, este aplicativo web permitirá la medición, gestión y control del riesgo operacional posibilitando la consolidación de eventos de pérdida por unidad de negocio de las posibles eventualidades o riesgos materializados presentados en los diferentes procesos que soporta la institución financiera.

1.3.2 Objetivos Específicos

- Contribuir al cumplimiento de la Resolución SBS N° 2116-2009 “Reglamento para la Gestión del Riesgo Operacional” y la circular SBS G-140-2009, “Gestión de la Seguridad de la Información.
- Brindar a la alta dirección información clara y fácil de comprender mediante una visión consolidada de los riesgos operacionales, a través del establecimiento de procedimientos concisos que permitan identificar, evaluar y calificar este tipo de riesgos, relacionándolos con los procesos, controles, planes de acción e indicadores necesarios para un adecuado tratamiento.

- A través de la implementación de la herramienta informática, se logrará la descentralización de la captura y registro de eventos de riesgo operacional con la finalidad de mejorar el seguimiento y cumplimiento de la metodología propuesta.

1.4 Justificación

1.4.1 Justificación de carácter Teórico

Debido a la importancia de su rol en el desarrollo económico de un país, las instituciones financieras están sujetas a una regulación. Ejemplos de estas son: los marcos Basilea I y II, y en Perú las Resoluciones SBS N° 037-2008 “Gestión Integral de Riesgos”, SBS N° 2116-2009 “Reglamento de la gestión de Riesgo Operacional” y la Circular SBS N° G- 140-2009 Gestión de la Seguridad de la Información. Dichas regulaciones buscan mitigar los diferentes tipos de riesgos inherentes a las operaciones financieras y entre otros efectos han tenido una repercusión importante sobre la madurez de este tipo de compañías en lo que respecta a la gestión de riesgos. Es importante para las instituciones financieras determinar, controlar y minimizar los riesgos operacionales, es por eso que éstas medidas sirven para supervisarlos y cómo los entes reguladores garantizan la efectividad de las mismas.

1.4.2 Justificación de carácter Práctico

En la actualidad los riesgos operacionales presentan dificultades en su gestión puesto que la alta dirección no participa activamente. Esta problemática genera la necesidad de una metodología que establezca procedimientos que generen información eficaz y eficiente en lo que concierne al riesgo operacional en las entidades financieras.

Para lograr lo anterior, se elaborará una política con soporte en un sistema informático, permitiendo registrar y teniendo actualizado los eventos de riesgos operacionales.

En el siguiente cuadro de la Operational Risk Data Exchange Association (ORX)⁹ se muestra las pérdidas por riesgo operacional que tienen las entidades financieras a nivel mundial debido a una inadecuada gestión de los riesgos de este tipo.¹⁰

	Internal Fraud	External Fraud	Employment Practices	Clients, Products & Business Practices	Disasters & Public Safety	Technology & Infrastructure	Execution Delivery & Process Management	Malicious Damage	Total % by Business Line
Corporate Finance	0.02%	0.09%	0.11%	0.24%	0.00%	0.00%	0.23%	0.00%	0.70%
Trading & Sales	0.08%	0.05%	0.32%	0.59%	0.02%	0.51%	8.26%	0.00%	9.84%
Retail Banking	3.66%	32.39%	7.53%	5.60%	0.67%	1.01%	13.25%	0.10%	64.21%
Commercial Banking	0.15%	3.07%	0.34%	1.21%	0.03%	0.20%	3.73%	0.00%	8.74%
Clearing	0.05%	0.48%	0.12%	0.12%	0.00%	0.13%	1.56%	0.00%	2.45%
Agency Services	0.01%	0.02%	0.07%	0.14%	0.00%	0.04%	1.41%	0.00%	1.70%
Asset Management	0.05%	0.11%	0.14%	0.51%	0.01%	0.07%	1.79%	0.00%	2.67%
Retail Brokerage	0.09%	0.12%	0.48%	1.72%	0.01%	0.04%	0.97%	0.00%	3.43%
Private Banking	0.21%	0.34%	0.14%	1.36%	0.02%	0.04%	2.01%	0.00%	4.12%
Corporate Items	0.04%	0.16%	0.58%	0.30%	0.20%	0.05%	0.80%	0.01%	2.14%
Total % by Event Type	4.36%	36.84%	9.83%	11.77%	0.97%	2.09%	34.02%	0.12%	100.00%

Key > 1% - 5% 5% - 10% >10%

Figura 1.5. Pérdidas por Eventos de Riesgo Operacional en el Sistema Financiero Mundial

⁹ Organización dedicada al avance de la industria de la medición y gestión del riesgo operacional en la industria de servicios financieros globales y que agrupa a los principales bancos del mundo. <http://www.orx.org/orx-members>

¹⁰ Fuente: Operational Risk Data Exchange Association (ORX), 2002-2007, www.orx.org.

La SBS también cuenta con formatos para eventos de pérdida por riesgo operacional, como consta en su portal web.¹¹



Información Consolidada de la Base de Datos de Eventos de Pérdida
Montos en Nuevos Soles (S/.)

Tipo de Evento	Finanzas corporativas						Negociación y ventas						Banca		
	N° de eventos	Monto Total Bruto	Pérdida mínima	Pérdida máxima	Monto recuperado por seguros	Monto Total Recuperado	N° de eventos	Monto Total Bruto	Pérdida mínima	Pérdida máxima	Monto recuperado por seguros	Monto Total Recuperado	N° de eventos	Monto Total Bruto	Pérdida mínima
FRAUDE INTERNO	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Actividades no autorizadas															
Robo y fraude															
FRAUDE EXTERNO	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Robo y fraude															
Seguridad de los sistemas															
RELACIONES LABORALES Y SEGURIDAD EN EL PUESTO DE TRABAJO	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Relaciones laborales															
Higiene y seguridad en el trabajo															
Diversidad y discriminación															
CLIENTES, PRODUCTOS Y PRÁCTICAS EMPRESARIALES	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Adecuación, divulgación de información y confianza															
Prácticas empresariales o de mercado improcedentes															

Figura 1.6 Formato para Eventos de Pérdida por Riesgo Operacional de la SBS

1.5 Propuesta Metodológica

El Banco de la Nación requiere una metodología para identificar, evaluar, tratar y monitorear los riesgos operacionales inmersos en los procesos del banco. Así mismo esta metodología contará con el apoyo de una aplicación tecnológica consistente, integrada y flexible que facilite la adopción de un proceso eficiente de Administración de Riesgos Operativos, generando reportes representativos de la Gestión del Riesgo Operacional en el Banco, con la finalidad de minimizar la posibilidad de que ocurran, evitándole pérdidas económicas.

¹¹ <https://extranet.sbs.gob.pe/app/login.jsp>

1.6 Organización de la tesina

Capítulo 1: Introducción

Está dedicado a la presentación del problema, los objetivos de la investigación, así como la justificación, propuesta y alcances

Capítulo 2: Marco Teórico

El propósito de este capítulo es de dar a la investigación un sistema coordinado y coherente de conceptos y proposiciones que permitan abordar el problema, describiendo detalladamente cual es el significado de los conceptos que se mencionaran durante todo el trabajo.

Capítulo 3: Estado del Arte

Se realiza una comparación con algunas metodologías y estándares ya existentes relacionada con la gestión de riesgos, con la finalidad de realizar una buena evaluación, gestión y administración de riesgos operacionales.

Capítulo 4: Resolución del problema aplicando la técnica seleccionada

Se detalla la metodología planteada indicando las bases científicas en que se basa y los resultados que se obtiene, con la finalidad de realizar una buena evaluación, gestión y administración de riesgos operacionales. Asimismo, se presenta el análisis y el prototipo del sistema que brinda el soporte a esta metodología con la finalidad de entender e interpretar todo lo sustentado.

Capítulo 5: Conclusiones y recomendaciones

Se detalla en forma resumida, la metodología planteada, incidiendo en los diversos beneficios que traería consigo su implementación en una entidad financiera peruana. Así mismo se indica algunas buenas prácticas que sería provechoso que la entidad financiera ejecutara, al momento de implementar la Evaluación de Riesgos Operacionales. Finalmente se plantea algunos temas de interés que se pueden desarrollar en base a este trabajo.

Referencias Bibliográficas

Se detalla las diversas fuentes bibliográficas (libros, páginas de internet, revistas, tesis, etc.), revisadas durante la realización del presente trabajo.

2 CAPITULO II.- MARCO TEORICO

2.1 Conceptos Inmersos en los Riesgos de Tecnología

2.1.1 Metodología

Metodología es el procedimiento o conjunto de procedimientos que se utilizan para obtener conocimientos. También se le puede entender como los pasos que se han seguido en:

- Una indagación determinada
- La designación de los modelos concretos de trabajo que se aplican en una determinada disciplina o especialidad.
- La referencia de procedimientos y recomendaciones que se desea a transmitir.

La metodología dependerá de los postulados que el investigador considere como válidos; de aquello que considere objeto de la ciencia y conocimiento científico; pues será a través de la acción metodológica, como recolecte, ordene y analice la realidad estudiada.

2.1.2 Riesgo

Existe una gran variedad de definiciones o conceptos asociados a lo que es un riesgo, este se puede definir como:

- La proximidad o posibilidad de que ocurra un daño o peligro.
- Cada uno de los imprevistos y/o hechos desafortunados que puede cubrirse con un seguro.

Asimismo, al hablar de riesgos comúnmente relacionamos este concepto con las siguientes palabras: amenaza, emergencia, urgencia, apuro, etc.

Sin embargo, es necesario que podamos tratar de obtener, utilizando las anteriores ideas, un concepto formal y tal vez uno de los más usados y que involucra tanto los hechos como las pérdidas que éstos podrían originar se adecua al siguiente: Un Riesgo es aquel evento que genera incertidumbre o pérdida en términos económicos, sociales, profesionales o de imagen.

2.1.3 Calificación y cuantificación de un riesgo

Son también variadas las formas y métodos para medir un riesgo, se presume que según el tipo de riesgo en análisis, existen distintas maneras de medir el nivel de riesgo al que está expuesto el proceso o servicio en evaluación.

Al hablar de calificación, se puede considerar los objetivos del negocio, por ejemplo para los clientes de una entidad financiera, la calificación de riesgo para acceder a un crédito se mide en términos de clasificar al cliente a quien se otorga un préstamo (por ejemplo, normal, deficiente, potencial pérdida, etc.).

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 pueden ser ajustables para adaptarlas a las circunstancias que el análisis establezca. El análisis cualitativo se utiliza:

- Como una actividad inicial de matiz, para identificar los riesgos que requieren de un análisis más detallado.
- Cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo y
- Cuando los datos numéricos son inadecuados para un análisis cuantitativo.

Al hablar de cuantificación, el objetivo es medir la probabilidad de que un evento de riesgo se concrete, asimismo se mide el impacto que generaría en términos monetarios, de imagen institucional, social hacia la organización, etc. Es necesario asimismo tener en cuenta las medidas que la organización adopte para mitigar en cualquier forma la ocurrencia de algún evento de riesgo.

En este contexto, es factible relacionar los niveles de calificación con la cuantificación de un riesgo a ello se denomina análisis semi cuantitativo, por ejemplo un riesgo que tiene una probabilidad de ocurrencia de 40 en 100 casos y que genera una pérdida de 200 nuevos soles cada vez que ocurre podría considerarse como un Riesgo Alto. Considerando el mismo ejemplo y conociendo que la organización ha implementado un mecanismo de control que reduce las pérdidas de 200 a 15 nuevos soles, y una ocurrencia de 12 en 100 casos, el riesgo puede adoptar un nivel de Riesgo Medio.

Este ejemplo muestra una de las maneras de tratar un riesgo y ese es uno de los retos de La Administración de Riesgos.

2.1.4 Concepto de Riesgo de Tecnología de Información

La definición de los riesgos de tecnología de información, está sustentado en dos pilares fundamentales, el primero de ellos enlazado a los riesgos de operación y el segundo a las definiciones internacionales de riesgo en SI.

En el primer pilar, los riesgos de tecnología de información son componentes de los riesgos de operación, entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.

Esta primera definición, está sustentada en la declaración de Basilea II, la misma que propone diez principios para una adecuada administración de los riesgos de operación, estos principios incluyen la adecuada estructura organizacional, la participación de la alta gerencia, la sujeción a revisión de auditoría, la generación de políticas de mitigación de riesgos y un proceso de gestión de los riesgos.

En el segundo pilar, los riesgos de tecnología de información se definen además como aquellos asociados a actividades con soporte en recursos de tecnología de información, sistemas informáticos y tecnología inherente a estos sistemas, los mismos que afectan el desarrollo de las actividades del negocio contra los principios de integridad, confidencialidad y disponibilidad de la información.

Como todo componente de riesgo, los asociados a tecnología de información están inmersos dentro de aquellos eventos que generan incertidumbre o pérdida en términos económicos, sociales, profesionales o de imagen.

2.1.5 Gestión Integral de Riesgos

Según el avance en las buenas prácticas para la administración de riesgos, este se ha ido incrementando en el alcance de su evaluación. En primer lugar, el riesgo tradicional que evaluaban las empresas financieras, se basó en el riesgo de créditos. El 15 de Julio de 1988 el Comité de Basilea publica el ACB ó Basilea I, el cual establecía el acuerdo de convergencia que uniforma medir la adecuación del capital en los bancos para asegurar su solvencia. Este ACB sólo tenía en cuenta el riesgo de crédito y no hacía ninguna referencia al riesgo de mercado.

En Enero de 1996 se efectuó la enmienda al ACB88 que incorpora el Riesgo de Mercado con lo cual la gestión de riesgos adopta un esquema financiero, de créditos y de mercado.

Posteriormente, a finales de la década de los noventa, Basilea II introduce novedades en el Riesgo Crediticio y además por primera vez tiene en cuenta el Riesgo de Operación que incluye los Riesgos de tecnología de información, aspecto que cada día tiene más importancia en la operatoria de las Instituciones Financieras. A partir de esa fecha, se inicia el tratamiento integral de Riesgos y su administración da origen a la Gestión Integral de Riesgos.

La Gestión Integral de Riesgos, ha dado origen al tratamiento de los riesgos estratégicos, los riesgos legales y morales que las empresas deben considerar.

2.1.6 Seguridad de Información

No existe una definición estricta de lo que se entiende por seguridad de información, puesto que ésta abarca múltiples y muy diversas áreas relacionadas con los procesos, su entorno y los sistemas de información. Consideraciones que van desde la protección física de las aplicaciones como componentes hardware, de su entorno, hasta la protección de la información que estos sistemas contienen o de las redes que lo comunican con el exterior.

Son muy diversos los tipos de amenazas contra los que debemos protegernos. Desde amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, el fraude interno, destrucción o modificación de la información.

No obstante, existen tres aspectos fundamentales que definen la seguridad de información: la confidencialidad, la integridad y la disponibilidad.

Sobre esta base, podemos definir a la seguridad de información como la adecuada interrelación de normas, procedimientos, cultura organizacional, mecanismos y recursos informáticos para garantizar los principios de confidencialidad, disponibilidad e integridad.

La seguridad de información, incluye en su análisis, un gran número de factores, por ejemplo, la British Estándar BS7799¹², establece 10 puntos clave en el control de la seguridad de información:

¹² BS 7799 : http://www.peopsoft.com/Servicio_Security.htm

- Documento de Política de Seguridad de Información.
- Asignación de Responsabilidades de Seguridad.
- Capacitación y Difusión en Seguridad de Información.
- Reporte de Incidentes de Seguridad.
- Controles Antivirus.
- Proceso de Planeación de Continuidad del Negocio.
- Control de copias Propietarias.
- Salvaguarda de los registros de la Empresa.
- Cumplimiento de la Legislación para la Protección de Datos.
- Cumplimiento de la Política de Seguridad.

2.1.7 Plan de Continuidad de Negocios

Un plan que direcciona la continuidad y el mantenimiento de todos los procesos del negocio requeridos para mantener un nivel aceptable de operación en el momento de ocurrencia de un evento de interrupción de los mismos y/o de los recursos que lo soportan.

Un plan de continuidad de negocios incluye los siguientes documentos como requerimiento mínimo de adecuación:

- Plan de Emergencias: Un mecanismo de respuesta centralizada que asegura la ejecución de las instrucciones y el control durante una interrupción operacional (Ej. Instrucciones y actividades manuales). Este plan incluye: identificación de incidentes, evaluación, escalamiento, declaración, plan de activación y desactivación inmediato y procedimientos iniciales de restauración.

- Plan de Contingencia: Un plan de ejecución y revisión constante que direcciona las acciones, personas, servicios y recursos informáticos o de comunicación disponibles para la atención de un evento de interrupción de los servicios con base en la evaluación de riesgos, disponibilidad de recursos y capacidad de respuesta.
- Plan de Recuperación: Un plan que direcciona la restauración de las aplicaciones de sistemas, software, datos e infraestructura de las mismas y procesos operativos del negocio (por ejemplo, hardware, comunicaciones, redes, servicios bancarios, etc.) después que la contingencia o desastre ha ocurrido.

2.1.8 Orígenes de la Administración de los Riesgos de Tecnología

- Requerimientos legales, regulatorios, contractuales
- Acelerados avances tecnológicos
- Incidentes de seguridad (comunicaciones divulgadas)
- Preocupación de los usuarios
- Pérdidas económicas
- Crecimiento generalizado de procesos de negocio soportados en tecnología de información.

2.1.9 Nuevo Acuerdo de Capital (NAC) - BASILEA II

A mediados de los años 90 y finalmente, en junio de 2004, se aprobó un Nuevo Acuerdo de Capital (Basilea II), cuyo objetivo es propiciar la convergencia regulatoria hacia los estándares más eficaces y avanzados sobre medición y gestión de los principales riesgos en la industria bancaria. El Comité de Basilea forma parte del Banco Internacional de Pagos (BIS) y fue creado por acuerdo de los representantes de los Bancos Centrales de los 10 países más industrializados con el propósito de formular una serie principios y estándares de supervisión bancaria, los que han sido acogidos no solo por los países miembros, sino por la mayoría de países en el mundo. Se indica que los países pertenecientes al G10, deberán de comenzar a implementar a partir del 2007 todo lo definido en Basilea II en sus versiones más simples y a partir de 2008 en sus versiones más avanzadas.

Más allá de proponer metodologías más sensibles al riesgo para el cálculo del capital regulatorio, Basilea II plantea reglas prudenciales específicas para las instituciones de crédito, apuntando a incentivar la estabilidad del sistema financiero dando mayor importancia a los sistemas de control interno, a la administración de los bancos y a la disciplina de mercado. Es así que Basilea II se puede definir como un marco global de supervisión bancaria, basado en tres pilares:

- Los Requerimientos Mínimos de Capital
- El Proceso de Examen del Supervisor
- La Disciplina de Mercado.

Cabe señalar que uno de los puntos que se desprende de los principios propuestos por el Comité de Basilea II (Nuevo Acuerdo de Capital - NAC), es que las entidades financieras deberán de establecer y asignar el capital necesario a la protección de los activos de Tecnología que pudieran generar una crisis bancaria.

En abril de 2003, la SBS decidió asumir el reto de la implementación y adecuación de lo propuesto por el comité de Basilea y estableció el Comité Especial Basilea II (CEB), en el cual se encuentran representadas las diversas áreas de la Superintendencia involucradas en este proyecto.

Entre las principales labores que viene realizando este Comité se encuentran las siguientes:

- Diseño de la supervisión según los principios de Basilea II.
- Adecuación estructura orgánica.
- Acceso a información nivel de operación: Nueva Central de Riesgos.
- El establecimiento de procedimientos de supervisión y mecanismos de alerta.
- Evaluación cuantitativa del impacto de la implementación del NAC en el sistema financiero peruano.
- Identificación de los principales cambios en la regulación y estudio de nuevas normas.
- Diseño del marco de transparencia ajustado a Basilea II.

Como se podrá apreciar los objetivos de la emisión de los documentos (normas, resoluciones, circulares, buenas prácticas, etc.) son:

- Las empresas supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, controlar y reportar los riesgos de tecnología de información que estas enfrentan.
- Incidir en la identificación de riesgos de tecnología, de los Procesos Críticos de la entidad financiera.
- Tener un control adecuado de los Activos de TI.
- Asignar el capital necesario, para la protección de los activos, ante el posible desenlace de un riesgo.

Finalmente indicamos que en el presente trabajo, se buscará plantear una metodología adecuada, la cual deberá de englobar los diversos documentos descritos en este capítulo.

2.1.10 Información y Sistema Informático

Entendemos por información el conjunto de datos que sirven para tomar una decisión. En consecuencia, su necesidad es evidente tanto en la planificación estratégica a largo plazo como en la fijación de estándares para la planificación a corto. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un componente vital para el Control.

En cuanto a su implantación, se puede hablar de:

- Subsistema formalizado: Normas, procedimientos e información de negocio.
- Subsistema no formalizado: Flujos de información que no pasan por el sistema de información formalizado (rumores, charlas informales, llamadas telefónicas, etc.).

El sistema informático es un subconjunto del subsistema formalizado, con distinto grado de cobertura. Por otra parte, se puede ver el sistema informático como el conjunto de los recursos técnicos (máquinas y utensilios), financieros (ingresos, gastos y patrimonio) y humanos (plantilla de informáticos y personal auxiliar), cuyo objetivo consiste en el almacenamiento, procesamiento y transmisión de la información de la empresa.

Los aspectos clave en la seguridad de información, están asociados a dos niveles:

- Aspectos de Negocio (Procesos de negocio y Organización)
- Aspectos tecnológicos (soluciones e Infraestructura)

Adicionado a esto, los riesgos fundamentales asociados con la incorrecta protección de la información como la revelación a personas no autorizadas, la inexactitud de los datos. La dificultad en el acceso a la información cuando se necesita, el fraude interno y externo, el costo financiero y social como los más importantes. Estos aspectos se relacionan con las tres características que debe cubrir un sistema de información seguro: *confidencialidad, integridad y disponibilidad*.

2.1.11 Confidencialidad

Se entiende por confidencialidad el servicio o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc. Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

2.1.12 Integridad

Se entiende por integridad el servicio que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Esta modificación debe ser permisible a revisiones o controles de auditoría que permitan identificar a los responsables de su modificación.

Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad:

- *Precisión accuracy,*
- *Integridad integrity,*
- *Autenticidad authenticity.*

El concepto de integridad asimismo, significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho el problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados.

En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los Bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos.

2.1.13 Disponibilidad

Se entiende por disponibilidad el grado en que la información está en el lugar, momento y forma en que es requerido por el usuario autorizado. Asimismo en términos de Sistema de Información cuando se puede acceder a un SI en un periodo de tiempo considerado aceptable.

Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo. Lógicamente, la información debe estar en los formatos adecuados para los usuarios al momento de encontrarse disponible para su uso.

Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio" (*denial of service*). Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados.

2.1.14 Amenazas a la Información

Una amenaza es cualquier elemento que afecta a los sistemas de información y a todo lo que involucra dicha información (procesos, eventos, etc.), el efecto de una amenaza es un daño, el mismo que no sólo incluye el efecto en si de la amenaza, sino también el hecho de no tomar acciones correctivas necesarias.

Una amenaza es también una condición del entorno del sistema de información (persona, máquina, suceso o idea), que dada una oportunidad, podría dar lugar a que se produzca una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). El análisis de riesgos identificará las amenazas que han de ser contrarrestadas.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- Interrupción: Se produce cuando un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad.
- Interceptación: Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora.
- Modificación: Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad.
- Fabricación: Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

2.1.15 Ataques Pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o controla, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico.

2.1.16 Ataques Activos

Los ataques activos implican algún tipo de modificación del flujo de datos transmitido, o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- 1.- Suplantación de Identidad: El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo.

2.- Repetición Indeterminada: Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

3.- Modificación de Mensajes: Una porción del mensaje legítimo es alterado, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.

4.- Degradación fraudulenta del servicio: Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones.

2.1.17 Otros Aspectos Relacionados

Existen otros aspectos considerados en el tratamiento de los riesgos de tecnología de información y que son especialmente importantes en el entorno bancario y en el uso del comercio digital, aunque pueden asimilarse a uno de los tres aspectos fundamentales, es necesario considerarlos con especial énfasis debido a su importancia en el negocio, entre ellos tenemos:

a) AUTENTICIDAD: Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser.

b) IMPOSIBILIDAD DE RECHAZO (no-repudio): Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió.

c) CONSISTENCIA: Asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados.

d) AISLAMIENTO: Regula el acceso al sistema, impidiendo que personas no autorizadas entren en él.

e) AUDITORÍA: Capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, y quién y cuándo las han llevado a cabo.

f) RECUPERACIÓN: En caso de emergencia o pérdida de información, deben existir los mecanismos necesarios para recuperar la información.

g) CUSTODIA Y PROPIEDAD: Es necesario tener identificado a quien custodia la información y establecer sólidamente las características de propiedad y depositario de la información.

3 CAPITULO III. ESTADO DEL ARTE METODOLÓGICO

3.1 Metodologías Similares

3.1.1 Metodología MAGERIT

La Metodología de Análisis y Gestión de Riesgos de Sistemas de Información MAGERIT, fue desarrollada por el Consejo Superior de Administración Electrónica de España, con la finalidad de administrar los sistemas de información de las entidades públicas; esta metodología fue emitida el año de 1997 y recoge las recomendaciones de las directivas de la Unión Europea en materia de seguridad de sistemas de información.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios. MAGERIT desarrolla el concepto de control de riesgos en las guías de procedimientos, técnicas, desarrollo de aplicaciones, personal y cumplimiento de normas legales.

Esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo.

Objetivos de MAGERIT:

Directos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

Cabe mencionar, que el análisis de riesgos propuesto por Magerit es una aproximación metódica que permite determinar el riesgo siguiendo unos pasos (Ver Figura N° 2)

- Determinar los activos relevantes para la Organización
- Determinar a que amenazas están expuestos aquellos activos
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Valorar dichos activos en función del coste que supondría para la Organización recuperarse ante un problema de disponibilidad, integridad, confidencialidad o autenticidad
- Valorar las amenazas potenciales.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza.



Figura 3.1. Pasos realizados por Magerit

3.1.2 Metodología OCTAVE

La Metodología OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) fue encargado por el CERT¹³ al SEI o Instituto de Ingeniería de Software de la Universidad estadounidense de Carnegie Mellon. Se liberó en el segundo trimestre de 2002 y desde entonces se han producido varias revisiones. Es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo.

-
- ¹³ CERT (Computer Emergency Response Team): considerado como autoridad mundial para la seguridad de Internet. Fue creado por DARPA (Defense Advanced Research Projects Agency) en 1988, en respuesta a las necesidades

Es un método operativo, orientado a resultados: después de la primera iteración (2-3 meses) se obtiene un plan a corto plazo y un plan estratégico a largo plazo para mitigar los riesgos detectados.

Objetivos de OCTAVE:

- Especificar los elementos del riesgo organizacional y los riesgos tecnológicos relativos a la estrategia y a la práctica.
- Fomentar el trabajo en equipo desde los sectores operativos o de negocios hasta los departamentos de tecnología de la información (IT), trabajarán juntos direccionados a las necesidades de seguridad, balanceando los tres aspectos: RIESGOS OPERATIVOS, PRACTICAS DE SEGURIDAD Y TECNOLOGIA. (Figura Nro 3)

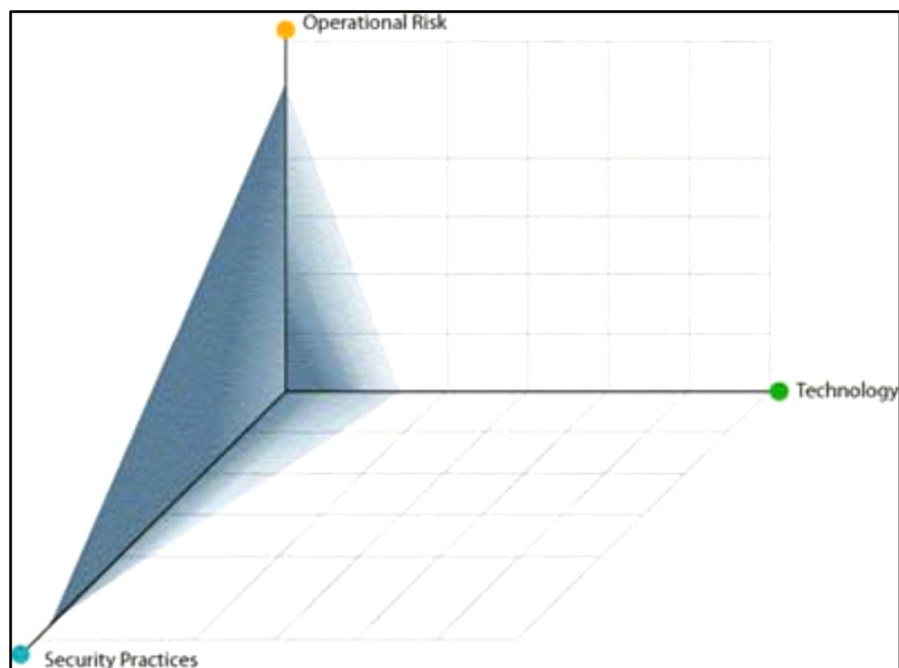


Figura 3.2. OCTAVE está impulsado por el riesgo operativo y prácticas de seguridad

- Se dirige de los servicios a los sistemas y no al revés, proponiendo un equipo de trabajo mixto entre personal encargado de la gestión de los servicios y personal técnico informático de sistemas. Está así pensado porque son las técnicas y gestoras de los servicios y proyectos las que conocen los riesgos de las entidades y de su tratamiento de la información.
- Propone una metodología muy bien detallada, con unos pasos muy claros y definidos, proporcionando el suficiente material de soporte (plantillas, ejemplos, etc.), y asumiendo todas las buenas prácticas de las normas y estándares actuales.

La aproximación de OCTAVE apunta a dos aspectos diferentes: riesgos operativos y prácticas de seguridad. La tecnología es examinada en relación a las prácticas de seguridad, permitiendo a las compañías tomar decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica.

3.1.3 Metodología CRAMM

La Metodología CRAMM (CCTA Risk Analysis Management Methodology), fue desarrollada en 1985 por la Agencia Central de Computación y Telecomunicaciones del Gobierno del Reino Unido, que utiliza técnicas cualitativas para el análisis y gestión de riesgos, se desarrolla en tres etapas distintas, a las que se asocian una serie de cuestionarios, objetivos y guías.

- Identificación de Riesgos.
- Análisis de Riesgos.
- Evaluación de Riesgos.

Objetivos de CRAMM:

- Proveer un marco conceptual genérico para el establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo.
- Especificar los elementos del proceso de administración de riesgos, sin forzar a la uniformidad en el sistema de administración del riesgo. Cabe señalar que este sistema de administración es influenciada necesariamente por las necesidades de la organización, sus objetivos particulares, sus productos y servicios, y los procesos y prácticas específicas empleadas.

4 CAPITULO IV. DESARROLLO DE LA SOLUCIÓN O DEL ESTUDIO

4.1 Introducción

La necesidad de entender y administrar los diferentes tipos de riesgos, que puedan afectar los objetivos empresariales de las entidades financieras, se ha convertido en un tema particularmente relevante para el desarrollo y funcionamiento de las empresas.

Durante la década anterior, un gran número de entidades financieras y no financieras han implementado procesos de administración de riesgo, principalmente para la gestión de los riesgos de crédito y de mercado.

Actualmente, las entidades financieras han enfocado su atención en el manejo del riesgo operativo, un tipo de riesgo que había sido considerado por muchas instituciones como no cuantificable, pero que, de acuerdo con el Comité de Basilea y teniendo en cuenta algunos eventos de pérdida significativos asociados a este tipo de riesgo, también puede representar peligros sustanciales para la solidez y seguridad del sistema bancario.

En consecuencia, dada la presencia del riesgo en el sistema bancario, su correcta administración contribuye sin duda alguna a la creación de valor para la empresa en el tiempo y constituye un elemento diferenciador que forma parte de una ventaja competitiva basada en la administración de los riesgos inherentes a la actividad bancaria.

4.2 Objetivo General

En el presente trabajo de investigación, se desarrolla una Metodología de Gestión de Riesgo Operacional, que tiene el objetivo de informar y comunicar, políticas, responsabilidades, procedimientos y herramientas dentro del marco de trabajo para la gestión de los riesgos operacionales. Este marco de trabajo incluye procedimientos como la identificación, evaluación, tratamiento y monitoreo de eventos de riesgo, registro de eventos de pérdida, definición y monitoreo de indicadores de riesgo.

4.3 Alcance

Lo establecido en la presente metodología, debe ser cumplido por todas las unidades orgánicas y trabajadores del Banco que intervienen en los procesos y servicios.

4.4 Base Legal o Administrativa

Resolución de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones N° 2116-2009, que aprueba el Reglamento para la Gestión del Riesgo Operacional.

Resolución de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones N° 37-2008 del 10 de enero del 2008, que aprueba el Reglamento de la Gestión Integral de Riesgos.

4.5 Definición de Términos¹⁴

a. Apetito por el Riesgo

Nivel de riesgo que el Banco está dispuesto a asumir en su búsqueda de rentabilidad y valor.

b. Evento o Incidencia

Suceso o serie de sucesos causados por factores internos o externos al Banco y que afectan a la consecución de algún objetivo. El evento o incidencia es la materialización de un riesgo que puede estar identificado o no.

c. Evento de pérdida por riesgo operacional

Evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.

d. Impacto

Consecuencia de la materialización de un riesgo, expresado en términos monetarios, como pérdidas financieras, mediante métodos cualitativos o cuantitativos.

e. Línea de Negocio

Son las categorías en las que se pueden clasificar las actividades realizadas por un banco. La Superintendencia a definido seis líneas de negocio: finanzas corporativas, negociación y ventas, liquidación y pagos, otros servicios, banca comercial y banca minorista.

f. Frecuencia

Probabilidad de ocurrencia de la materialización de un riesgo. Puede determinarse con base en información histórica o, en su defecto, con base en la experiencia y los conocimientos del personal involucrado en los procesos analizados.

¹⁴ La sección Definición de Términos, hace referencia al Capítulo 1 Artículo 2° de la Resolución S.B.S. 2116-2009 Gestión de Riesgo Operacional, y al Capítulo 1 Artículo 2° de la Resolución S.B.S. 37-2008 Gestión Integral de Riesgos.

g. Proceso crítico

Proceso considerado indispensable para la continuidad de las operaciones y servicios del Banco o cuya paralización o interrupción perjudica la consecución de los objetivos de la institución.

h. Riesgo

La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos del Banco.

i. Tolerancia al riesgo

Son los niveles de desviación de los objetivos trazados que el Banco está dispuesto a asumir.

Su definición busca asegurar que la entidad permanezca dentro del riesgo aceptado.

j. Riesgo Estratégico

Posibilidad de pérdidas por decisiones de alto nivel asociadas a la creación de ventajas competitivas sostenibles. Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias claves de la empresa y en el proceso de generación e innovación de valor.

k. Riesgo Operacional

Posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

l. Riesgo de Reputación

Posibilidad de pérdidas por la disminución de la confianza en la integridad de la institución que surge cuando el buen nombre de la empresa es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una organización.

m. Nivel de Riesgo Absoluto

Es aquel al que se enfrenta una entidad en ausencia de acciones de control para reducir su frecuencia y/o impacto.

n. Nivel de Riesgo Residual

Es el riesgo al que se enfrenta una entidad, considerando el efecto que tienen los controles existentes y/o los planes de acción sobre el riesgo absoluto.

o. Coordinador de Riesgo

Personal encargado por cada Jefatura de Departamento o División, para apoyar en la gestión de riesgos.

p. Riesgo Aceptado

Nivel de riesgo que el Banco está dispuesto a asumir para realizar su misión o visión.

4.6 Disposiciones Generales

La gestión del riesgo operacional se encuentra alineada a la visión, misión y objetivos estratégicos del Banco. La metodología de gestión del riesgo operacional debe ser aplicada a nivel de procesos, por lo que se requiere el análisis y entendimiento de los mismos.

La metodología de gestión del riesgo operacional permitirá administrar los riesgos operacionales que pueden tener un impacto negativo en el logro de los objetivos del Banco para que, a través de la implementación de planes de acción, mantenga el nivel de riesgo dentro del aceptado en la institución.

La metodología de gestión del riesgo operacional debe ser aplicada por todas las dependencias, siendo la División de Riesgos de Operación la encargada de apoyar y asistir en su aplicación.

4.7 Disposiciones Específicas

4.7.1 Metodologías para la Gestión del Riesgo Operacional

La metodología propuesta comprende las etapas de identificación, evaluación y tratamiento de los riesgos. La evaluación del riesgo comprende la determinación del impacto y la probabilidad de ocurrencia de cada uno de los riesgos identificados. El tratamiento se refiere a aquellas medidas o acciones que se toman con la finalidad de prevenir la ocurrencia o minimizar el impacto del riesgo.

Los etapas de la metodología, están basadas en componentes del modelo COSO-ERM¹⁵, documento marco utilizado como mejores prácticas para la gestión de riesgos empresariales.

Componente de la gestión de riesgos empresariales:

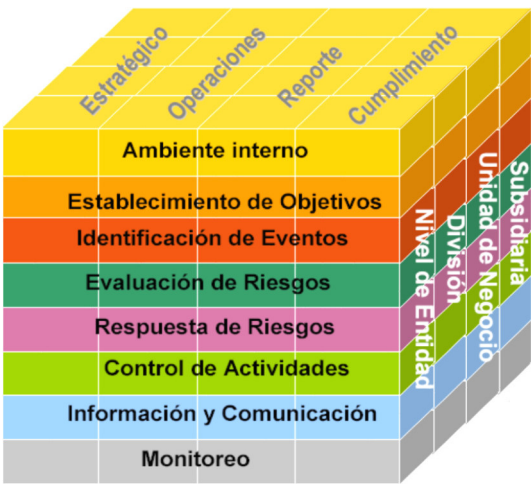


Figura 4.1. Committee of Sponsoring Organizations of Treadway Commission

¹⁵ COSO-ERM (Committee of Sponsoring Organizations of Treadway Commission), Marco integrado para la Gestión de Riesgos Corporativos

4.7.2 Etapas de la Metodología para la Evaluación de Riesgos Operacionales

La estructura de la metodología comprende las siguientes etapas:

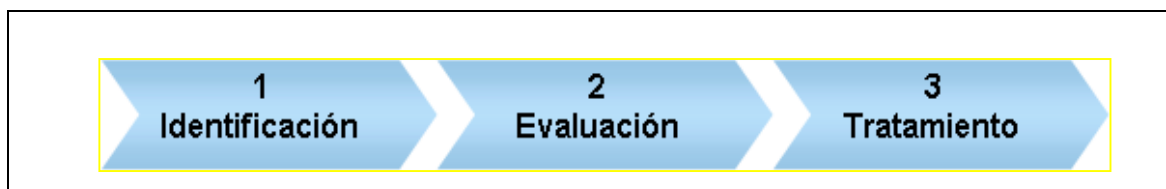


Figura 4.2. Etapas de la Metodología

4.7.2.1 Identificación de Riesgos

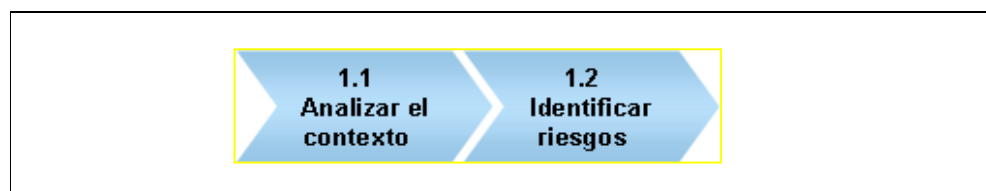


Figura 4.3. Pasos para identificar los riesgos

4.7.2.1.1 Analizar el Contexto

Fase que comprende el entendimiento del ambiente interno y externo donde opera el proceso o entidad sujeto a análisis, y sus herramientas, entre ellas:

Análisis de flujos de procesos

Representación esquemática de un proceso, que identifica las entradas, actividades, responsabilidades y salidas de los procesos. Ayuda gráficamente a identificar riesgos que pueden afectar los objetivos del proceso.

Entrevistas

El propósito es averiguar los conocimientos y puntos de vista sinceros del entrevistado, en relación con los acontecimientos pasados y los posibles acontecimientos futuros.

Cuestionarios y/o encuestas

Permite entender el contexto global o específico a partir de preguntas estructuradas.

4.7.2.1.2 Identificar Riesgos

Fase que comprende la identificación de los riesgos asociados a los procesos o productos, desde dos puntos de vista, el primero como riesgos asociados a las actividades y el segundo como riesgos asociados a las áreas de soporte que intervienen en el proceso.

A partir de esta fase, se utilizará como herramienta, los **Talleres de Trabajo**, que consisten en reuniones dirigidas, que congregan habitualmente a personal de muy diversas funciones o niveles, con el propósito de aprovechar el conocimiento colectivo del grupo. El registro de los riesgos se realizará en la matriz de riesgos.

Implementación de los Talleres de Trabajo

El Analista de Riesgos a cargo convoca al personal clave del proceso/subproceso, con la finalidad de verificar con los participantes la operatividad del proceso/subproceso evaluado.

En esta etapa, se debe contar con un inventario de procesos, subprocesos, y actividades; así como los responsables de cada una de ellas. Ver ejemplo:

PROCESO	SUB PROCESO	TAREAS	RESPONSABLE
Nombre del Macroproceso /	Nombre del Sub Proceso	actividades que comprende el proceso.	Se detalla el responsable de la ejecución del
Colocaciones / Préstamos Multired	Pre – Calificación	Actividades del Sub Proceso	Servicios Financieros / Div. Banca Personal.
	Evaluación	Actividades del Sub Proceso	Servicios Financieros / Div. Banca Personal.
	Aprobación	Actividades del Sub Proceso	Servicios Financieros / Div. Banca Personal.
	Desembolso	Actividades del Sub Proceso	Servicios Financieros / Div. Banca Personal.

Figura 4.4. Inventario de Procesos, Subprocesos, y Actividades

El Analista de Riesgos será quien lidere todas las fases del taller, contemplando una o más fases en una sola fecha, de acuerdo a la complejidad del proceso/subproceso. A continuación las fases a considerar:

1ra Fase: Identificación y categorización del riesgo, en el FORMATO N° 01 Ficha de Registro de Riesgos se registra para cada riesgo, la descripción del riesgo, las principales causas que lo originan y los controles existentes, además se determinan la línea de negocio (Anexo N° 02) a la pertenece el proceso/Subproceso evaluado, el objetivo estratégico y tipo de evento de pérdida (Anexo N° 03) relacionado, y el Departamento / División responsable; cada causa es asociada a uno de los factores que originan el riesgo.

2da Fase: Calificación de los riesgos, el Analista de Riesgos distribuirá el FORMATO N° 02 Ficha de Calificación de Riesgos, para que los participantes procedan a calificar los riesgos. Mayor detalle en el numeral 4.1.3 Evaluación de Riesgos y Controles.

El Departamento de Riesgos evaluará la necesidad de realizar nuevos talleres de trabajo por cada proceso, de acuerdo a la dinámica en su gestión (evolución de riesgos, implementación de planes de acción, variaciones en la efectividad de los controles, entre otros).

Validación de Riesgos

El Analista de Riesgos, a fin de validar los riesgos identificados, entrevistará a los responsables de las tareas y subprocesos involucrados. Estas entrevistas pueden realizarse posteriormente a la realización de un taller de trabajo, o cuando el analista lo crea oportuno.

Los riesgos identificados y evaluados se resumen en el FORMATO N° 03 Formato de Autoevaluación de Riesgos, y deben ser validados por los jefes de las áreas involucradas en el proceso, en particular por el dueño del proceso.

4.7.2.2 Evaluación de Riesgos

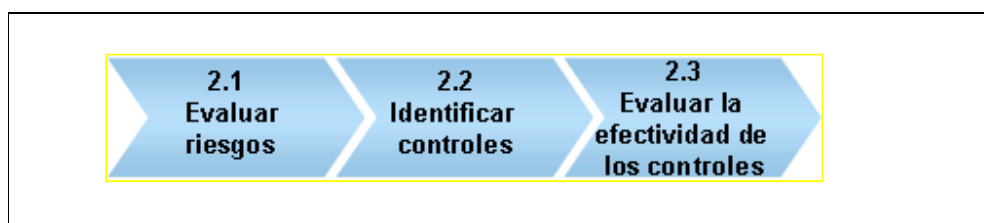


Figura 4.5. Pasos para proceso de evaluación

4.7.2.2.1 Evaluar Riesgos

Fase que comprende la determinación del impacto y la probabilidad de ocurrencia de cada uno de los riesgos identificados, para lo cual se han determinado rangos de valoración, detallados a continuación:

4.7.2.2.1.1 Niveles de Frecuencia

Para realizar el cálculo de la frecuencia se utilizan criterios de ocurrencia de los riesgos, así como estimaciones subjetivas. Los niveles de frecuencia definidos se muestran en la TABLA N° 01 Niveles de Frecuencia.

TABLA N° 01: NIVELES DE FRECUENCIA

Nivel	Descripción	Valor
Rara vez	Improbable. Ninguna incidencia al año. Uno de incidencia histórica. No es probable que se repita. Extremadamente raro. No haya ocurrido.	20% (1)
Ocasional	1 incidencia al año. Incidentes aislados.	40% (2)
Poco Frecuente	Entre 1 y 3 eventos al mes, máximo 12 al año. Evidencias de tendencias en crecimiento.	60% (3)
Frecuente	Altamente probable. Entre 3 y 10 eventos al mes. Recurrencia frecuente.	80% (4)
Muy Frecuente	Más de 10 eventos al mes. Alta frecuencia de recurrencia.	100% (5)

4.7.2.2.1.2 Niveles de Impacto

El impacto de un riesgo puede ser expresado cualitativa o cuantitativamente, en la medida que ocasione pérdidas económicas o interfiera en el desarrollo de las labores operativas del Banco.

Los niveles de impacto definidos se muestran en la TABLA N° 02 Niveles de Impacto.

TABLA N° 02: NIVELES DE IMPACTO

Nivel	Descripción	Valor
Insignificante	Menor o igual a S/. 3,000. Inconvenientes menores	20% (1)
Menor	Pérdida potencial o real mayores a S/. 3,000 y menores o iguales a S/. 30,000. Exposición a sanciones regulatorias menores. Los reclamos de los clientes están en los niveles esperados.	40% (2)
Moderado	Pérdida potencial o real mayores a S/. 3,000 y menores o iguales a S/. 200,000. Exposición a sanciones regulatorias menores. Los reclamos de los clientes están en los niveles esperados.	60% (3)
Mayor	Pérdida potencial o real mayores a S/. 200,000 y menores o iguales a S/. 6,000,000. Exposición a sanciones regulatorias menores. Los reclamos de los clientes están en los niveles esperados.	80% (4)
Catastrófico	Mayor o potencial catástrofe o actual impacto al grupo. Pérdida potencial o real superior a S/. 6, 000,000. Serias implicancias reguladoras.	100% (5)

Al momento de realizar la valoración de los eventos, si el rango del impacto se encuentre entre dos valores diferentes, se elegirá el de mayor valor. Para el caso de la probabilidad, se debe considerar el valor que indica una mayor frecuencia en un menor rango de tiempo.

Matriz de Evaluación del Nivel de Riesgo*

De la combinación de los niveles de impacto y probabilidad, se establece el nivel de RIESGO ABSOLUTO

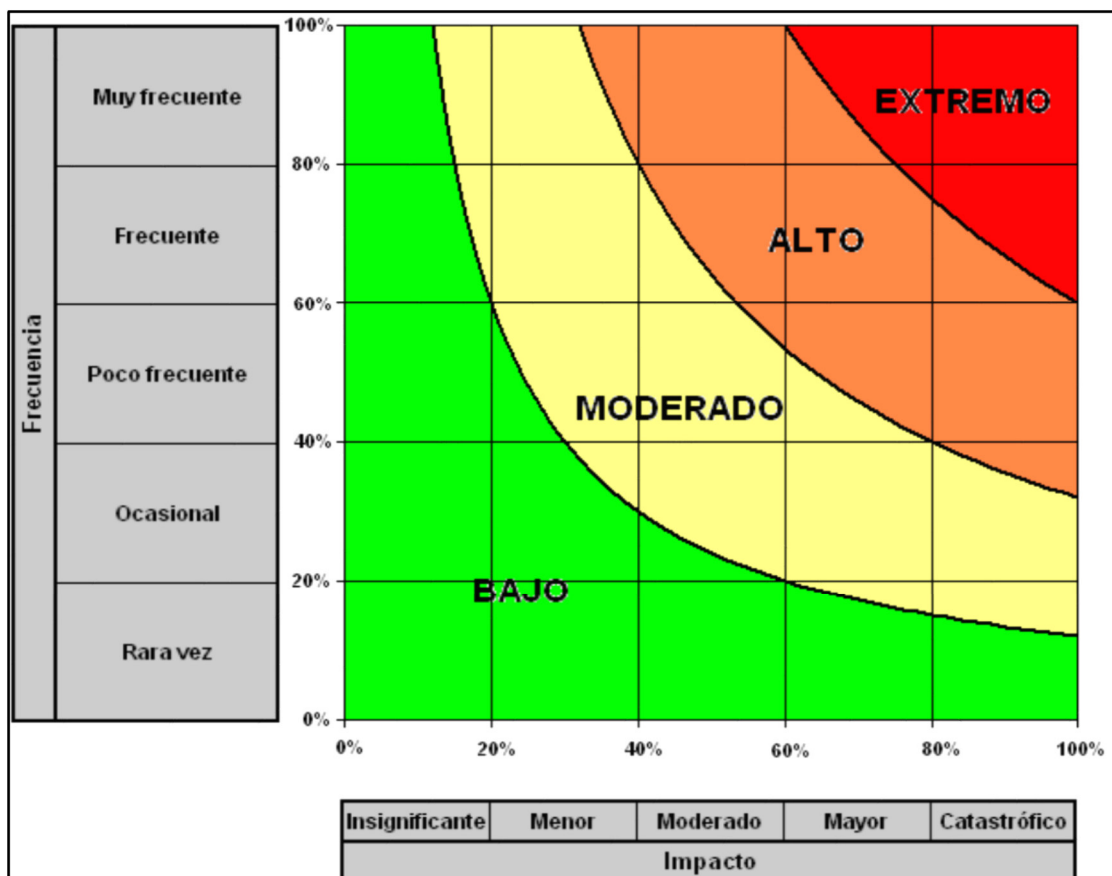


Figura 4.6. Matriz de Evaluación del Nivel de Riesgo

* Válida para los niveles de riesgo absoluto, y residual. El Nivel de Riesgo Aceptado es menor o igual a 24%.

El nivel de riesgo se clasifica en cuatro niveles:

TABLA Nº 03: TRATAMIENTO DE RIESGO OPERACIONAL

Apetito al riesgo	Nivel de riesgo	Tratamiento
No aceptable	Extremo	Requiere la definición inmediata de planes de acción, los que tienen alta prioridad de implementación. Rango de nivel de riesgo: de 60.01% a 100%.
	Alto	Requiere la definición de acciones prioritarias para la implementación de los planes de acción. Rango de nivel de riesgo: de 32.01% a 60%
Aceptable	Moderado	No se recomienda acciones de tratamiento; no obstante, en caso se considere pertinente, podría implementarse un plan de acción o indicador de riesgo a fin de reducir el riesgo y/o mejorar el ambiente de control interno. Rango de nivel de riesgo: de
	Bajo	Se acepta el riesgo, se gestiona mediante las acciones ya establecidas. Rango de nivel de riesgo: de 0% a 12%.

El nivel de riesgo aceptado es el igual o inferior al 24%; nivel que puede ser redefinido en función al apetito por el riesgo del Banco.

4.7.2.2.2 Identificar Controles

Fase que comprende la identificación de controles o mecanismos de mitigación existentes en el contexto actual para reducir un riesgo en particular.

4.7.2.2.3 Evaluar la Efectividad de los Controles

Fase que comprende la evaluación de la efectividad de las medidas existentes para mitigar el riesgo al que está asociado. La efectividad se evalúa en función a las diferentes características de los controles consideradas deseable, agrupadas en:

- a) Controles según el tipo
- b) Controles según su ejecución
- c) Controles según su documentación
- d) Controles según su periodicidad
- e) Controles según su responsabilidad

a) Controles según el tipo

Controles Preventivos: Actúan sobre la causa de los riesgos, con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa. Sirven para frenar ciertas transacciones antes de su ejecución. Ejemplos: Revisión de firmas y saldo antes de efectuar un pago.

Controles Detectivos: Sirven para supervisar la ejecución del proceso, ofrecen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear, o alertar a los trabajadores. Se diseñan para alertar sobre la presencia de los riesgos, permitiendo tomar acciones inmediatas. Ejemplo: sistema de alarma, doble verificación de cálculos, reportes periódicos.

Controles Correctivos: Identifica desviaciones cuando se han presentado los riesgos. Permiten el restablecimiento de la actividad después de ser detectado un evento no deseable y la modificación de las acciones que propiciaron su ocurrencia. Estos controles actúan cuando ya se han presentado hechos que implican pérdidas para la entidad. Ejemplo: la recuperación de un archivo dañado a partir de las copias de seguridad, planes de contingencia, los seguros.

b) Controles según su ejecución

Manual: Son ejecutados por el personal que interviene en el proceso.

Automatizada: Son aplicados a través de sistemas de información automatizados. Aseguran la correcta captación de la información y procedimientos de autorización y aprobación por parte de los responsables.

Combinada: Su aplicación es parcialmente automatizada.

c) Controles según documentación

Sin documentar: Los controles se realizan en base a la experiencia y al criterio del funcionario, no cuentan con documentación que lo sustente.

Desactualizada: Los controles cuentan con documentación que los sustente, pero esta se encuentra desfasada y no representa como se vienen ejecutando los controles en realidad.

Parcialmente documentado: Se cuenta con documentos normativos de respaldo a la aplicación de los controles, pero estos son parciales y no detalla en forma clara y precisa el procedimiento del control.

Documentado: Los controles están apoyados en documentos normativos actualizados (manuales de organización y funciones, manuales de procedimientos, circulares, directivas, etc.).

d) Controles según su periodicidad

Esporádico: Se aplican en forma ocasional, de acuerdo al criterio del funcionario responsable.

Periódicos: Pueden ser anuales, semestrales, mensuales, quincenales, semanales o diarios dependiendo de la ejecución de las operaciones, transacciones o actividades; se debe considerar además si es adecuado o no que el control sea periódico.

Continuos: Se aplica en forma constante cada vez que se ejecuta la transacción, operación o actividad; se debe considerar además si es adecuado o no que el control sea continuo.

e) Controles según la asignación de responsabilidad

No asignada: No se ha definido el responsable de la ejecución del control.

Asignada: Se ha definido el responsable de la ejecución del control, pero no cuenta con documento normativo que respalde la ejecución del control.

Asignada y formalizada: La responsabilidad del funcionario que ejecuta el control se encuentra definida y se sustenta en documentos normativos.

La TABLA N° 04 de Evaluación de Efectividad de Control, muestra la ponderación y valores de las características de los controles. Los valores asignados pueden ser de hasta el 100%. A cada característica se le ha asignado una ponderación de acuerdo a su importancia.

Para realizar el cálculo de la efectividad del control (Ec) ver Anexo N° 04.

TABLA N° 04 TABLA DE EVALUACIÓN DE EFECTIVIDAD DE CONTROL

Característica Efectividad del Control		Valores	Ponderación
Tipo	Correctivo	0.2	24%
	Detectivo	0.6	
	Preventivo	1	
Ejecución	Manual	0.2	23%
	Combinado	0.6	
	Automatizado	1	
Documentación	Sin documentar	0	15%
	Desactualizada	0.2	
	Parcialmente documentado	0.6	
	Documentado	1	
Periodicidad	No se aplica	0	15%
	Esporádico	0.2	
	Periódico inadecuado	0.6	
	Continuo inadecuado	0.6	
	Periódico adecuado	1	
	Continuo adecuado	1	
Responsabilidad	No asignada	0.2	23%
	Asignada no formalizada	0.6	
	Asignada y formalizada	1	
Puntaje máximo			100%

La efectividad del control se determina utilizando la siguiente tabla:

TABLA N° 05 TABLA DE VALORACION DE LA EFECTIVIDAD DE CONTROL

Efectividad	%min	%Max	Puntaje
Excelente	80%	100%	5
Buena	60%	79.99%	4
Media	40%	59.99%	3
Insatisfactoria	20%	39.99%	2
Pobre	0	19.99%	1

- **Excelente:** Los controles son adecuados y efectivos.
- **Buena:** Los controles son efectivos. Las debilidades del control son mínimas y no representan un riesgo significativo.
- **Media:** Los controles son adecuados, sin embargo existen algunas debilidades que pueden ser superadas.
- **Insatisfactoria:** Los controles no son efectivos ni aceptables.
- **Pobre:** No existen controles o estos son deficientes, no cumplen con su objetivo de mitigar los riesgos.

En el caso de existir más de un control se debe hallar la efectividad por cada uno de ellos.

Grado de Reducción del control sobre la Frecuencia y/o Impacto

TABLA N° 06 GRADO DE REDUCCION DEL CONTROL

Calificación	Grado en %
Bueno	90%
Medio	60%
Pobre	30%
Nulo	0%

En el caso de existir más de un control se debe calificar el grado de reducción por cada uno de ellos. Para realizar el cálculo del grado de Reducción del control en la Frecuencia o en el Impacto ver Anexo N° 04.

Después del análisis, se realiza nuevamente la combinación del nivel de impacto y probabilidad, considerando los controles existentes y su efectividad para hallar el nivel de RIESGO CONTROLADO

4.7.2.3 Tratamiento de riesgos



Figura 4.7. Pasos para tratamiento de riesgo

4.7.2.3.1 Definir Tratamiento

Fase que comprende la respuesta al riesgo en las siguientes categorías:

- Evitar la exposición
- Reducir
- Compartir
- Aceptar

En los casos que corresponda debe definirse un Plan de Acción, según el apetito de riesgo aprobado por el Directorio.

4.7.2.3.2 Monitorear Planes de Acción

Fase que comprende el seguimiento y control de los avances de los planes de acción comprometidos en la fase tratamiento. Este monitoreo es realizado hasta su implementación.

Para hallar el nivel de RIESGO RESIDUAL, se realiza nuevamente la combinación del nivel de impacto y probabilidad, considerando la culminación del Plan de Acción.

APLICACIÓN DE LA METODOLOGIA



Figura 4.8. Pasos para la Aplicación de la Metodología

4.8 Responsabilidades

Las responsabilidades del Directorio, Gerencia General, Comité de Riesgos, Jefes de las unidades orgánicas y del Departamento de Riesgos se encuentran incluidas en los Reglamentos de Políticas de la Gestión Integral de Riesgos, de Organización y Funciones del Banco y el del Comité de Riesgos.

4.8.1 De la División Riesgos De Operación

- a) Elaborar, proponer y desarrollar la metodología para la gestión del riesgo operacional.
- b) Apoyar y asistir a las dependencias del Banco para la aplicación de la metodología de gestión del riesgo operacional.
- c) Promover la cultura de gestión del riesgo operacional, identificando las necesidades de capacitación y difusión.
- d) Identificar y evaluar los riesgos operacionales a los que está expuesto el Banco.
- e) Proponer alternativas para reducir y/o controlar los riesgos operacionales que puedan afectar el cumplimiento de los objetivos del Banco, en coordinación con los dueños del proceso.
- f) Proponer los lineamientos para la gestión del fraude en el banco, en concordancia con las buenas prácticas y la normativa al respecto.
- g) Realizar la evaluación del riesgo operacional, de forma previa al lanzamiento de nuevos productos o servicios y ante cambios importantes en el ambiente operativo o informático.
- h) Proveer información, sobre la gestión de riesgos realizada, cuando esta sea requerida por los Departamentos, a fin de que realicen actividades para la continuidad de sus procesos.
- i) Emitir reportes e informes periódicos sobre la gestión del riesgo operacional.

4.8.2 De las Jefaturas de Departamento

- a) Designar a los coordinadores de riesgo que apoyarán en la gestión del riesgo operacional.
- b) Administrar integralmente los riesgos de los procesos de su competencia, a través de la identificación, tratamiento e implementación de los planes de acción de los mismos; considerando las políticas, límites y procedimientos establecidos para la Gestión Integral de Riesgos, así como el tratamiento de los riesgos involucrados en la gestión de continuidad.
- c) Brindar información del proceso/subproceso para la correcta identificación de sus riesgos.
- d) Validar los riesgos identificados y evaluados en los talleres.
- e) Liderar la definición e implementación de los planes de acción, a fin de mantener los riesgos identificados dentro de los niveles de riesgo aceptables, y coordinar con los corresponsables la consecución de las actividades establecidas en el plan.
- f) Remitir al Departamento de Riesgos las propuestas de nuevos productos o servicios, así como las de cambios significativos en los ambientes operativo o informático, identificando y evaluando los riesgos previos a su lanzamiento.
- g) Reportar los eventos de pérdida cuyo origen corresponde al riesgo operacional, así como ejecutar acciones inmediatas para mitigar los eventos de pérdida ocurridos.
- h) Evaluar las “acciones a seguir” para reducir los riesgos operacionales, considerando el análisis costo/beneficio, así como definir los responsables, recursos y plazos necesarios para su ejecución.
- i) Asumir ante el Gerente General los resultados de la gestión de riesgos correspondiente a su Departamento.

4.8.3 De la División de Soporte Regional y Zonal Lima

- a) Identificar y reportar los riesgos que puedan afectar negativamente la operatividad en la Región, de acuerdo a la metodología establecida por el Departamento de Riesgos; estableciendo, en el ámbito de su competencia, acciones para reducir o controlar el riesgo, en coordinación con las áreas competentes; así como el tratamiento de los riesgos involucrados en la gestión de continuidad.
- b) Reportar de manera oportuna los eventos de pérdida por riesgo operacional, recopilando y proporcionando información sobre dichos eventos.
- c) Impulsar a las Agencias dependientes a registrar las incidencias mediante el aplicativo Portal de Registro de Incidencias, inmediatamente después de detectada la incidencia, así como realizar el seguimiento de las mismas hasta la solución de los problemas, esto en coordinación con las áreas responsables.
- d) La Jefatura de la División Soporte Regional designará al(los) analista(s) que se encargarán de las funciones de Gestión de Riesgos:
- Realizar el seguimiento de las incidencias operativas reportadas por los administradores de las Sucursales / Agencias, a través del ReportCenter (herramienta de consulta de incidencias).
 - Informar y coordinar oportunamente, con las distintas áreas responsables en el ámbito de su responsabilidad, la solución de las incidencias operativas reportadas.

4.8.4 Del Analista de Riesgos de Operación

- a) Apoyar y asistir a las dependencias en la identificación de riesgos, causas, controles y en la definición de los planes de acción para los riesgos en los procesos, productos o servicios nuevos y proyectos.
- b) Evaluar el riesgo operacional de acuerdo a la metodología establecida.
- c) Realizar el seguimiento de los Planes de Acción.
- d) Desarrollar reportes sobre la Gestión del Riesgo Operacional.
- e) Proponer acciones para el tratamiento de los eventos de riesgo operacional.
- f) Promover la cultura de gestión del riesgo operacional.
- g) Actuar como agente facilitador de información de riesgos cuando ésta sea requerida por los Departamentos y/o el líder de la Gestión de la Continuidad del Negocio.

4.8.5 Del Coordinador de Riesgos

- a) Registrar en los formatos autorizados la información de los eventos o incidencias identificados.
- b) Representar a su dependencia en las labores de administración de riesgos (identificación, evaluación y reporte de los planes de mitigación), alineadas a la nueva metodología definida para la gestión del riesgo operacional.
- c) Reportar al Gerente de su Dependencia y al Departamento de Riesgos las situaciones relacionadas con la administración de riesgos, principalmente los riesgos que podrían generar pérdidas para el Banco, y las debilidades de control identificadas en los procesos inherentes de negocio.

- d) Coordinar e impulsar las actividades necesarias para la ejecución de los planes de acción.
- e) Identificar y reportar nuevos riesgos y eventos.
- f) Apoyar al Área de Riesgos en el desarrollo de la administración del riesgo operacional, así como brindar retroalimentación al respecto.
- g) Participar activamente en la gestión del Plan de Continuidad de Negocios (Mantenimiento, documentación, evaluación de riesgos, ejecución de pruebas).
- h) Mantener actualizada la información y documentación que se genere en la ejecución de sus actividades.
- i) El encargo de responsabilidades como Coordinador de Riesgo se realiza mediante memorando emitido por cada Jefatura de Departamento o División con línea de dependencia directa a la Gerencia General o Presidencia Ejecutiva; su revocatoria se hará por la misma vía.

4.8.6 Del Administrador de Sucursales y Agencias de Lima y Provincias

- a) Identificar y comunicar al Departamento de Riesgos, los riesgos que puedan afectar negativamente la operatividad de la oficina a su cargo; estableciendo, en el ámbito de su competencia, acciones para reducir o controlar el riesgo, en coordinación con las áreas competentes.
- b) Comunicar y coordinar con la Jefatura Regional / Zonal los eventos de pérdida por riesgo operacional y brindar la información que se le solicite al respecto.
- c) Registrar las incidencias relacionadas a sus oficinas mediante el aplicativo Portal de Registro de Incidencias, reportándolas inmediatamente después de ocurrido el evento.
- d) Realizar el seguimiento a través del portal; una vez atendida y solucionada la incidencia, el Administrador deberá cambiar el estado de la misma (cerrar ticket) en el Portal.

- e) Participar activamente en la gestión del Plan de Continuidad de Negocios (Mantenimiento, actualización, ejecución de pruebas).
- f) Administrar formatos de su dependencia a fin de mantener actualizados toda la documentación relacionada a la continuidad del negocio.
- g) Participar en los programas y simulacros que se desarrollan por temas de continuidad.

4.8.7 El Coordinador de Eventos de Pérdida

- a) Informar la ocurrencia de un evento de pérdida al Departamento de Riesgos - División Riesgos de Operación, con los documentos que sustenten el evento.
- b) Apoyar al área de riesgos en la recopilación de la información requerida sobre dichos eventos.

4.8.8 Del Departamento de Auditoría

- a) Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional, así como lo dispuesto en la Resolución SBS N° 2116-2009, de conformidad con lo establecido en el reglamento de Auditoría Interna.
- b) Auditoría Interna deberá coordinar con la Unidad de Riesgos mecanismos de retroalimentación de la información obtenida a través de los exámenes y evaluaciones realizadas.

FORMATOS

FORMATO N° 01: FICHA DE REGISTRO DE RIESGOS

INFORMACION DEL MACROPROCESO									
MP0001		Préstamo Multired							
Codigo		Detalle							
INFORMACION DEL PROCESO									
Codigo		Detalle							
MP0001-001		Colocación							
LINEA DE NEGOCIO									
Nivel 1		Nivel 2							
Banca Minorista		Banca Minorista (Préstamos de Libre Disponibilidad)							
Cod.	RIESGO Descripción	OBJETIVO ESTRATÉGICO RELACIONADO	CAUSAS		TIPO DE EVENTO DE PÉRDIDA	CONTROLES	RESPONSABLE		
			Descripción	Factor					
001	Impacto: Pérdida económica (cuota, comisión, intereses, costos operativos). mediante: generación errada de cronograma en las condiciones de prepago y/o cambio de tasa.	Brindar satisfacción al cliente	Ejecución errada de sistemas.		Interrupción del negocio y fallos en los sistemas	- Elaboración, modificación y revisión manual del cronograma. - Control dual en el sistema para aprobación (Asistente, Jefe de Sección, Jefe de Departamento). - La sección carteras solicita la instrucción solicitada por el cliente (persona natural) - La sección carteras confirma la instrucción del cliente con los funcionarios de la red de oficinas.	- Operaciones - Sección Cartera		
002	Impacto: Multa o Sanción. mediante: Errores en la información, equivocación al colocar código IBS, monto de la deuda errado, otros.	Brindar satisfacción al cliente	- Ejecución errada de sistemas. - Reportar indebidamente a la central de riesgos.	Tecnológico				Interrupción del negocio y fallos en los sistemas	- Operaciones - Sección Cartera

Figura 4.9. Ficha de Registro de Riesgos N° 1

FORMATO N° 02: FICHA DE REGISTRO DE RIESGOS

Taller N°	0001	Fecha	01/11/2011	Responsable:	M. Saavedra Huertas
Macroprocesos:	Préstamo Multired			Dependencia:	Operaciones
Procesos:	Colocación			Co-Responsables:	C. Rodríguez Choque
Sub Proceso:	Aprobación y generación de cronograma			Dependencias:	Red de Agencias

Cod Riesgo	Riesgo	Causas	Factor de Riesgo	Nivel Riesgo Absoluto		Controles	Efectividad del Control					Responsible de la ejecucion del control	Reduccion		
				Fa	la		Tipo Ejec ucion n	Documenta cion	Periorid ad	Respons abilidad	Reduce Fa, la o ambos		Grad o		
														RF	RI
001	Impacto: Pérdida económica (cuota, comisión, intereses, costos operativos). mediante: generación errada de cronograma en las condiciones de prepago y/o cambio de tasa.	Ejecución errada de sistemas.	Tecnológico	3	3	- Elaboración, modificación y revisión manual del cronograma. - Control dual en el sistema para aprobación (Asistente, Jefe de Sección, Jefe de Departamento).	Co	Ma	Pd	Pa	AN	-Operaciones - Sección Cartera	Fa	2	3
002	Impacto: Multa	- Ejecución	Tecnológico	4	3	- La sección carteras	Co	Ma	Pd	Pa	AN	-Operaciones	Fa	3	3

FORMATO N° 03: FORMATO DE AUTOEVALUACIÓN DE RIESGOS

Macroproceso	Proceso	Subproceso	Código del Riesgo	Descripción del Riesgo	Causas(s)	Factor de Riesgo	División / Sección	Riesgo Absoluto				Descripción del Control (s)	Efectividad del Control				Reducción			Riesgo Residual			Tratamiento	Plan de Mejora	
								Frecuencia (Fa)	Impacto (Ia)	NRA			Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	¿Reduce?	En Frecuencia	En Impacto	Frecuencia (Fr)	Impacto (Ir)		NRR	Situación
						- Selección										- Selección						- Selección			
						- Selección										- Selección						- Selección			
						- Selección										- Selección						- Selección			
						- Selección										- Selección						- Selección			
						- Selección										- Selección						- Selección			
						- Selección										- Selección						- Selección			

Figura 4.11. Formato de Autoevaluación de Riesgos

FORMATO N° 04: FICHA DE PLAN DE ACCIÓN

RIESGOS(S) TRATADOS				
001	Impacto: Multa o Sanción. mediante: Errores en la información, equivocación al colocar código IBS, monto de la deuda errado, otros.			
Codigo	Detalle	Nivel de riesgo (NRC)		
PLAN DE ACCIÓN				
Codigo	Descripción	Fecha Inicio	Fecha Fin	
001	Evaluar la posibilidad de crear un Tipo de categoría en el Sistema SaraWeb que contenga todos los tipos de empresas (incluidas SRL y EIRL), para permitir vincular la garantía con los otros créditos del cliente, con la finalidad que luego se visualice en el Saraweb al momento de la liberación de garantía o una opción en el Saraweb en el que muestre a detalle todos los créditos a la que está relacionada una garantía.	01/12/2011		31/01/2012
Responsable	Involucrados			
Operaciones	J. Saavedra Diaz			
CRONOGRAMA DE IMPLEMENTACIÓN				
Actividad	Responsable	Fecha Inicio	Fecha Fin	Avance
Reunión con personal de red de agencia, operaciones y sistemas para replicar el error identificado.	Operaciones	02/12/2011	30/12/2011	100%
Evaluación del impacto en el sistema Saraweb e informe de viabilidad técnica.	Sistemas	02/01/2012	31/01/2012	100%
				31/01/2012

Figura 4.12. Ficha de Plan de Acción

5 CAPÍTULO V. DESCRIPCIÓN DE LA SOLUCIÓN TECNOLÓGICA

**SIRO – Sistema Informático de Riesgo Operacional
(Modulo I: del proyecto SIRO: Requerimiento de Evento de Pérdida por Riesgo Operacional)**

Especificación de Requerimientos del Software (SRS)

Versión 1.1

5.1 Especificación de Requerimientos del Software (SRS)

5.1.1 Introducción

El presente documento describe los requerimientos funcionales y no funcionales del Modulo I del proyecto SIRO: Requerimiento de Evento de Pérdida por Riesgo Operacional. El documento está dividido en tres partes, la primera define el propósito, el alcance, definiciones, acrónimos y abreviaturas; referencias y generalidades. La segunda realiza una descripción global del producto así como consideraciones y dependencias. Finalmente la tercera describe los requerimientos específicos, de funcionalidad, de facilidad de uso, de confiabilidad, de desempeño, de facilidad de soporte, restricciones de diseño, interfaces, documentación en línea y componentes adquiridos.

5.1.2 Propósito

Describe de forma clara, despejando las dudas posibles sobre los requerimientos funcionales y no funcionales del producto de software, dejando un documento nítido al diseñador y al arquitecto para que definan la mejor implementación de la solución.

5.1.3 Alcance

Este documento detalla las características definidas en el Charter del Proyecto plasmándolas en requerimientos funcionales y no funcionales. Este documento especifica los requerimientos funcionales, de facilidad de uso, de confiabilidad, de facilidad de soporte, de restricciones de diseño, de interfaces, de documentación en línea y requerimientos de ayuda finalmente de componentes adquiridos.

5.1.4 Definiciones

Riesgo: Probabilidad que un evento ocurra e impacte negativamente sobre los objetivos del Banco.

Riesgo Operacional: Posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

Línea de Negocio: Servicios o productos agrupados según características similares y que buscan atender los requerimientos de un mismo segmento de mercado.

SBS: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

SUCAVE: Sub-Módulo de Captura y Validación Externa.

5.1.5 Referencias

- Charter del Proyecto.
- Cronograma del Proyecto.

5.1.6 Generalidades

El documento está dividido en tres partes. Además de la primera, la segunda parte realiza una descripción global del producto así como consideraciones y dependencias. Finalmente, la tercera describe los requerimientos específicos, de funcionalidad, de facilidad de uso, de confiabilidad, de desempeño, de facilidad de soporte, restricciones de diseño, interfaces, documentación en línea, componentes adquiridos, entre otros.

5.1.7 Consideraciones y Dependencias

Las principales consideraciones y dependencias de este producto software son las siguientes:

- El Sistema de Claves Host, con el cual se realiza el proceso de autenticación de los usuarios.
- Los reportes generados por el producto software sirven para evaluar y monitorear la evolución del Requerimiento de Eventos de Pérdida por Riesgo Operacional.

5.2 Requerimientos Funcionales

5.2.1 Funcionalidad

5.2.1.1 Registro de las cuentas Contables

Se debe registrar mensualmente las cuentas contables reportadas por el Dpto. de Contabilidad, mismo que se genera en formato TXT. Este archivo es el mismo que se envía al SUCAVE y al realizarse su ingreso deberá indicar el mes y el año al que corresponde el mencionado archivo.

5.2.1.2 Reporte Requerimiento de Pérdida por Riesgo Operacional por Riesgo Operacional

El sistema deberá realizar el cálculo de Pérdida por Riesgo Operacional para cubrir el riesgo operacional que enfrenta el Banco. Para el cálculo de dicho requerimiento de Eventos de Pérdida por Riesgo Operacional se debe formular de acuerdo a lo dispuesto por la SBS en la resolución N° 2115-2009.

5.2.1.3 Almacenar Histórico del Requerimiento de Eventos de Pérdida por Riesgo Operacional

Se requiere guardar la información generada por cálculo de dicho requerimiento de Eventos de Pérdida por Riesgo Operacional, para poder analizar su evolución.

5.2.1.4 Reportes Estadísticos

Se necesita analizar el requerimiento de Eventos de Pérdida por Riesgo Operacional por periodos de forma automática. Así también presentar esta información en forma gráfica.

5.2.1.5 Seguridad

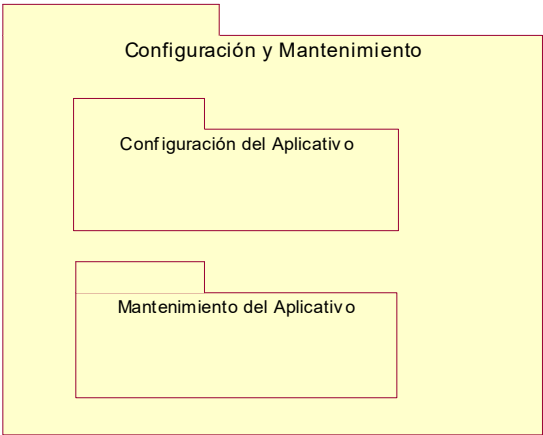
A través de un nombre de usuario y contraseña, se realizará el acceso al Sistema. Así también este usuario deberá estar asignado a un tipo de perfil para acceder a la funciones que esta autorizado a realizar.

5.2.1.6 Configuración y Mantenimiento

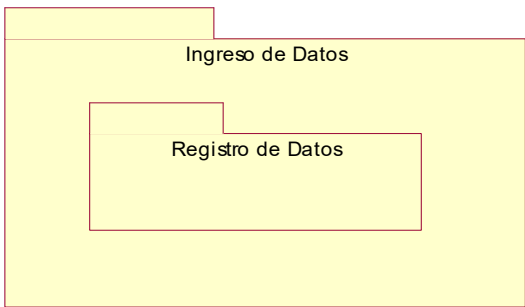
Se debe permitir realizar una configuración inicial para los parámetros establecidos en el cálculo del requerimiento de Eventos de Pérdida por Riesgo Operacional. Así también el mantenimiento de los principales tablas que conformaran el sistema.

5.3 Modelo de Paquetes / Módulos

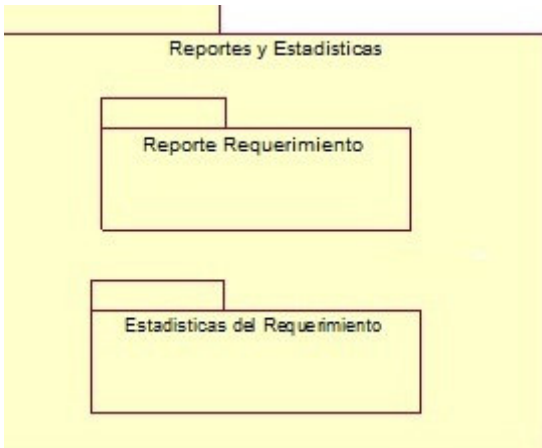
5.3.1 Paquete Configuración y Mantenimiento



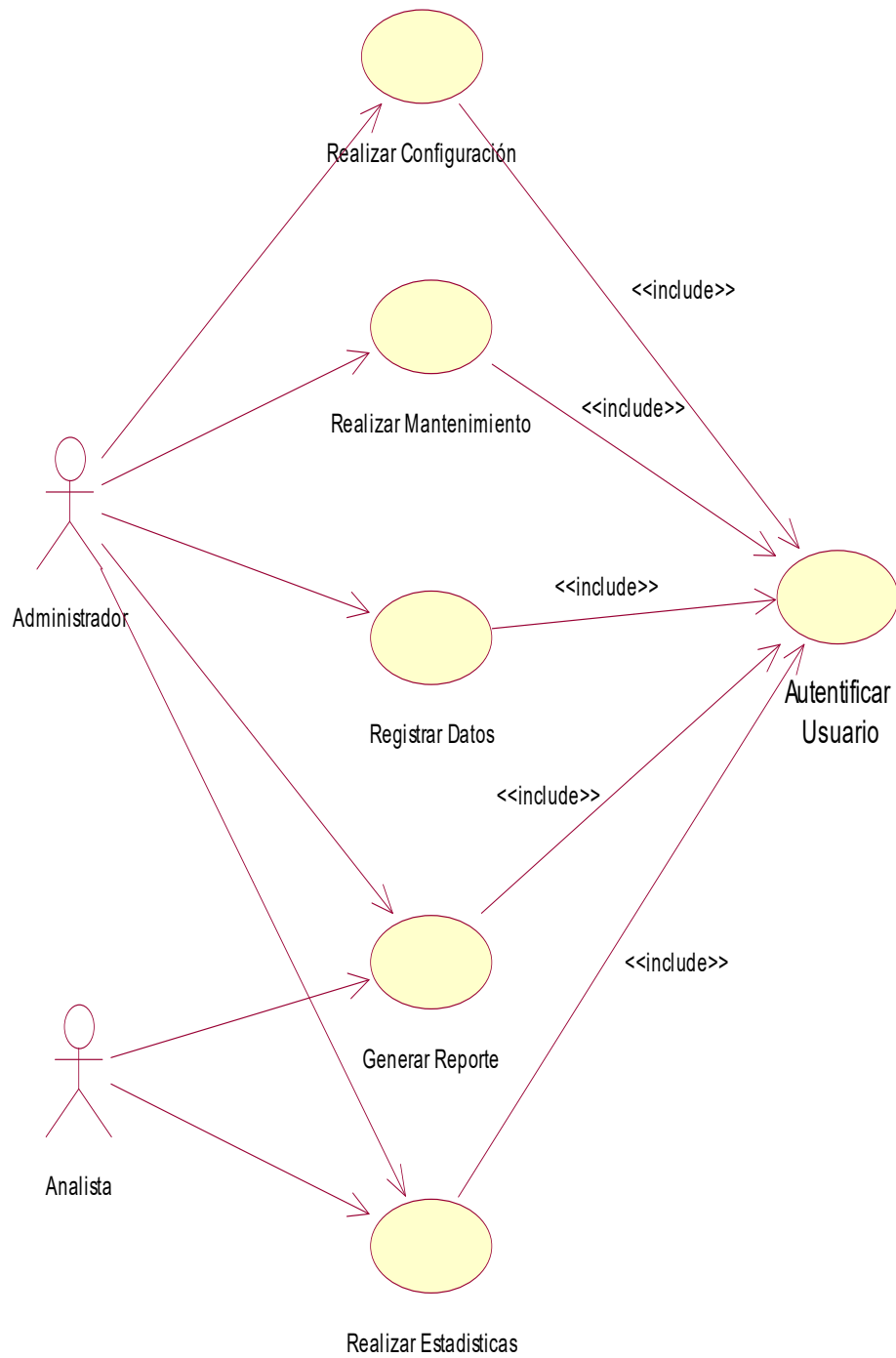
5.3.2 Paquete Ingreso de Datos



5.3.3 Reportes y Estadísticas



5.4 Modelo de Casos de Uso



5.5 Resumen de Actores y Casos de Uso

Actor	Descripción
Administrador	Es el actor que realiza las siguientes actividades: • Configuración de los parámetros del aplicativo. • Mantenimiento de las tablas principales del aplicativo. • Registrar los datos, por ejemplo cuentas contables, etc. • Genera Reporte de Requerimiento de Eventos de Pérdida por Riesgo Operacional. • Realiza las Estadísticas de la evolución del Requerimiento de Pérdida por Riesgo Operacional.
Analista	Es el actor que realiza las siguientes actividades: • Genera Reporte de Eventos de Pérdida por Riesgo Operacional. • Realiza las Estadísticas de la evolución del Requerimiento de Eventos de Pérdida por Riesgo Operacional.

Caso de Uso	Descripción
Autenticar Usuario	Esta actividad permite valida el acceso del usuario al sistema, así mismo visualiza las opciones del sistema, según el perfil asociado.
Realizar Configuración	Se realiza la configuración de los parámetros del sistema, como son: • Asignar el nombre o IP del Servidor. • Asignar el nombre o IP de la Base de Datos. • Asignar un Usuario Inicial. • Asignar el correo por el cual se realizará el envío automático de correos.
Realizar Mantenimiento	Este proceso permite actualizar las principales tablas del sistema, por consiguiente se modificara información como:

	• Registro de Usuarios. • Registro de Líneas de Negocios. • Registros de Cuentas Contables. • Registro de Métodos.
Registrar Datos	Esta actividad permite al administrador registrar las cuentas contables, las mismas que son emitidas por el Dpto. de Contabilidad.
Generar Reporte	Mediante este proceso, se realizara el Cálculo del Requerimiento de Eventos de Pérdida por Riesgo Operacional. Este cálculo se realiza a través de los métodos: • Met. del Indicador Básico. • Met. Estándar Alternativo
Realizar Estadísticas	Esta actividad consiste en visualizar la información histórica del requerimiento de Eventos de Pérdida por Riesgo Operacional, calculado por métodos anteriormente mencionados.

5.6 Reporte de Requerimientos

5.6.1 Sistemas Operativos

Servidor Central

- Windows 2003 Server SP1 o Windows XP SP2

Cientes Web

- Windows XP SP2 o Superior.

5.6.2 Sistema de Gestión de Base de Datos

- Ms. Sql Server 2005

5.6.3 Servidor de Aplicaciones

- COM 1.0 o COM 1.5

5.6.4 Servidor Web

- IIS 6.0 o Superior.

5.6.5 Otras Aplicaciones

- Ms .NET Framework 2.0
- Internet Explorer 6.0 o Superior.

5.7 Requerimientos No Funcionales

5.7.1 Facilidad de Uso

5.7.1.1 Facilidad de aprendizaje

Los usuarios podrán utilizar el sistema dentro de un corto plazo y con un entrenamiento básico.

5.7.1.2 Facilidad de ingreso

El aplicativo no requerirá a los usuarios realizar numerosos pasos antes de que puedan comenzar a usarlo.

5.7.1.3 Minimización del Error

El aplicativo permite a los usuarios realizar sus tareas sin errores, minimizándolos al dificultar y restringiendo el ingreso de un error humano.

5.7.1.4 Navegación

Las interfaces de usuario del aplicativo facilitan a los usuarios navegar por donde ellos quieran.

5.7.1.5 Entendimiento del aplicativo

Las interfaces de usuario del aplicativo son claras e intuitivas para los usuarios. Los mensajes del aplicativo son entendibles y comprensibles de acuerdo al tipo de acceso que disponga.

5.8 Confiabilidad

5.8.1 Tiempo de Duración de Sesión del Usuario

La duración de la sesión de trabajo del cliente será de 30 minutos, después del cuál expirará la sesión y se obligará al cliente a realizar nuevamente el ingreso al sistema. El software permite configurar el tiempo de expiración de la sesión.

5.9 Desempeño

5.9.1 Tiempo de Respuesta

El aplicativo tiene un tiempo de respuesta inferior a 8 segundos.

5.9.2 Tiempo de espera

El aplicativo tiene un tiempo de espera inferior a 4 segundos.

5.10 Facilidad de Soporte

5.10.1 Sobre el estándar para la codificación de los programas.

Se utilizará el estándar de codificación de los programas visuales proporcionado por el Departamento de Informática.

5.10.2 Sobre el estándar para Diseño de la Base de Datos

Se utilizará el estándar de creación de objetos de bases de datos proporcionado por el Departamento de Informática.

5.11 Restricciones de Diseño

5.11.1 Restricciones sobre la Arquitectura

5.11.2 Estructura en Capas de la Arquitectura

La arquitectura del producto está diseñada de acuerdo a la arquitectura en 3-capas.

5.11.2.2 Sobre el Lenguaje de Programación

El lenguaje de programación a emplear para el desarrollo de la capa de presentación será el Microsoft ASP.NET.

5.11.3 Restricciones sobre los Componentes

5.11.3.2 Sobre tipo de Browser

El software cliente sobre el que deberá operar el producto será:

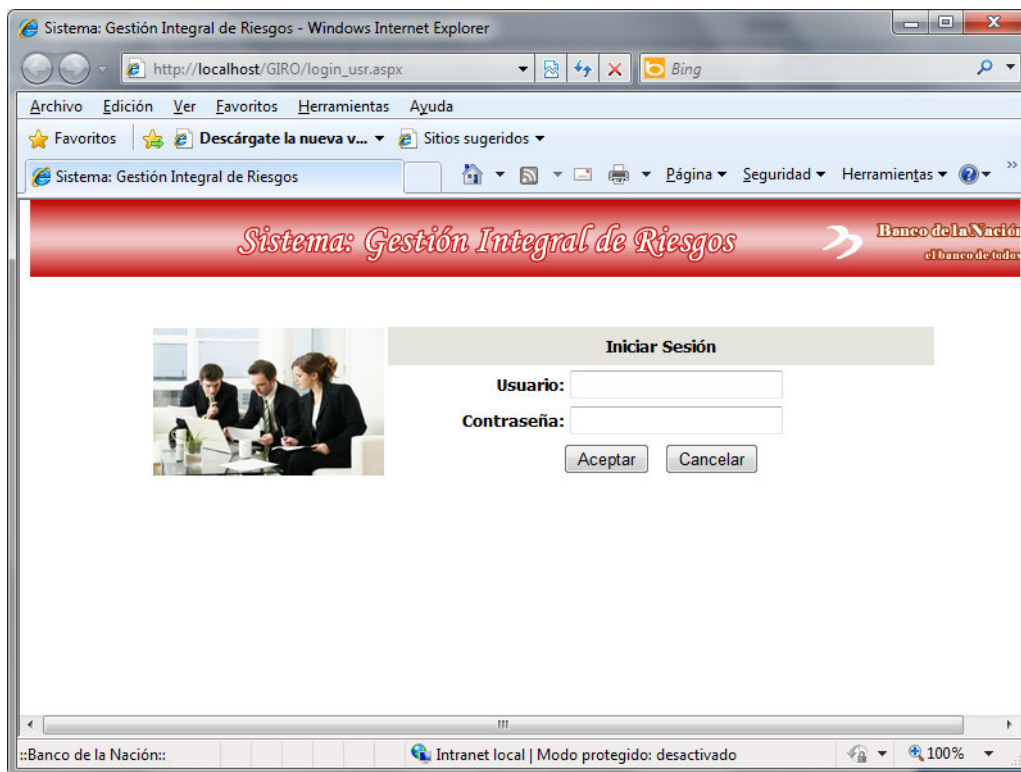
Microsoft Internet Explorer (5.0 ó superior).

El sistema ha sido probado en este navegador no encontrándose ningún inconveniente. Es posible que otros navegadores trabajen sin inconvenientes.

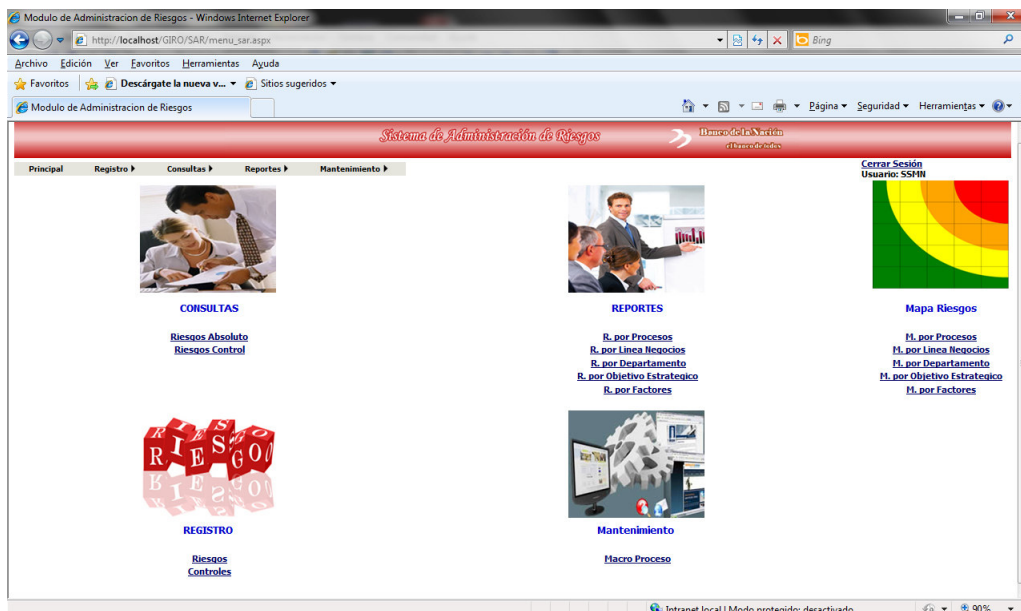
5.12 Interfaces

5.12.1 Interfaces de Usuarios

5.12.1.2 Prototipo de Ingreso de Usuarios



5.12.1.3 Prototipo Menú Principal



5.12.1.4 Prototipo Ingreso de Riesgos

Registro de Riesgo - Windows Internet Explorer

http://localhost:1080/SAR/registro_riesgos.aspx

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos Descárgate la nueva v... Sitios sugeridos

Registro de Riesgo

Sistema de Administración de Riesgos

Inicio de Sesión
Cerrar Sesión
Usuario: SSF/M

Principal Registro Consultas Reportes Mantenimiento

Registro de Riesgos

Nro. Riesgo: Fecha: 16/12/2011

Macro-Proceso: Captaciones Proceso: Apertura de Cuenta

Sub-Proceso: Cuentas Corrientes

Línea de Negocio: Otros Servicios

Error en el ingreso de información del cliente

Riesgo:

Obj. Estratégico: Brindar Satisfacción al Cliente Obj. Específico: Mejorar nuestro conocimiento del cliente

Evento: Ejecución, entrega y gestión de procesos Perdas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores

Perdida:

Causas	Descripción	Factor
1	Error de digitación.	Personal
2	Error en el control dual. Procesos Internos	Procesos Internos

Factor Principal: Personal

Relacionado a: ☐ Continuidad Neg. ☐ R. Estratégica ☐ R. Legal ☒ R. Reputacional

Responsable

Departamento: Departamento de Red de Agencias División: División Zonal Lima

Sección: -Selecione-

5.12.1.5 Prototipo de Sub Ingreso de las Causas de Eventos de Pérdida por Riesgo Operacional

Registro de Riesgo - Windows Internet Explorer

http://localhost/GIRO/SAR/registro_riesgos.aspx

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos Descárgate la nueva v... Sitios sugeridos

Registro de Riesgo

Página Seguridad Herramientas

Sistema de Administración de Riesgos Banco de la Nación

Principal Registro Consultas Reportes Mantenimiento

Cerrar Sesión
Usuario: SSHN

Registro de Riesgos

Macro: Riesgo:1
Fecha: 16/12/2011

Proceso: Captaciones
Sub-Proceso: Cuentas Corrientes
Linea de Negocio: Otros Servicios

Riesgo: Error en el ingreso de informacion del cliente

Obj. Brindar Satisfaccion al Cliente
Obj. Especifico: Ejecucion, entrega y gestion de procesos

Evento: Ejecucion, entrega y gestion de procesos
Perdida: Ejecucion, entrega y gestion de procesos

Causas: Error de digitacion.

Factor: Personal

Factor Principal: -Selecione-

Relacionado a: ☐ R. Continuidad Neg. ☐ R. Estrategico ☐ R. Legal ☐ R. Rep

Responsable: Departamento: -Selecione- Division: -Selecione- Sección: -Selecione-

Co-Responsable: Riesgo Absoluto

Intranet local | Modo protegido: desactivado 90%

5.12.1.6 Prototipo de Búsqueda de Riesgos e Ingreso de Controles

Consulta de Riesgo Absoluto - Windows Internet Explorer

http://localhost/GIRO/SAR/consulta_riesgos_absoluto.aspx

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos Descárgate la nueva v... Sitios sugeridos

Consulta de Riesgo Absoluto

Sistema de Administración de Riesgos Banco de la Nación

Principal Registro Consultas Reportes Mantenimiento

[Cerrar Sesión](#)
Usuario: SSMN

Consulta de Riesgos (Absoluto)

Macro-Proceso	Proceso	Sub-Proceso
Captaciones	Apertura de Cuenta	Depositos a plazo
Codigo	Riesgo	Fec. Inicio
Linea de Negocio	Obj. Estrategico	Factor Riesgo
Liquidacion y Pagos	Brindar Satisfaccion al Cliente	Personal
Riesgo Absoluto	Riesgo que Afecta	Responsable
Bajo	R. Estrategico	Area de Administracion

Buscar

Intranet local | Modo protegido: desactivado 90%

5.12.2 Interfaces de Hardware

No Aplica.

5.12.3 Interfaces de Software

No Aplica.

5.12.4 Interfaces de Comunicación

La comunicación entre el Browser y el servidor Web deberá realizarse sobre SSL (Secure Socket Layer).

5.13 Documentación en Línea y Requerimientos de Ayuda del Sistema

Se dispondrá de un manual de usuario, que estaría a disposición de todos los usuarios del sistema, a su vez se elaborará material visual explicando las principales operaciones del aplicativo, que estaría a disposición a través del portal del Departamento en Intranet.

5.14 Requerimientos de Licencia

No Aplica.

5.15 Metodología de Desarrollo

“Metodología de Ciclo de Vida de Software del Banco de la Nación”, que es una adaptación de la Norma Técnica Peruana NTP-ISO/IEC 12207.

5.16 Componentes Adquiridos

No Aplica.

5.17 Otros Estándares Aplicables

No Aplica.

5.18 Reglas de Negocio

Para el registro de datos, se requiere del archivo de cuentas contables, el cual es generado por el Dpto. de Contabilidad en formato TXT. Este archivo debe ser el mismo que es registrado en el SUCAVE y se emite en forma mensual.

El Cálculo del Requerimiento de Eventos de Pérdida por Riesgo Operacional se realiza según la Resolución de la S.B.S. N° 2115 – 2009.

Historia de las Revisiones

Fecha	Versión	Descripción	Autor
10/10/2011	1.0	Definición de los principales requerimientos del producto software	Omar López Tapia Miguel Huaroto Manco
30/11/2011	1.1	Modificación	Omar López Tapia Miguel Huaroto Manco

6. CONCLUSIONES Y RECOMENDACIONES

Quisiéramos concluir este trabajo destacando los aspectos que, a nuestro juicio, resume la situación actual del sector financiero peruano en la Gestión del Riesgo Operacional.

- Introducir de forma generalizada el Riesgo Operacional en la cultura de las organizaciones será el principal reto al que deberán enfrentarse las entidades que quieran implantar con éxito un marco completo de Gestión del Riesgo Operacional. Sin embargo la gestión correcta y completa de este riesgo no sólo les servirá para cumplir con la normativa y regulación vigente sino que les permitirá, además, reducir las pérdidas por fallos operacionales, los riesgos de control y mejorar la calidad de los servicios, lo que finalmente redundará en una mayor protección del accionista.
- Los datos sobre la experiencia histórica de pérdidas del banco, proporcionan información importante para evaluar la exposición al riesgo operacional del banco y son necesarios para el cálculo de los requerimientos de capital por este riesgo. Es importante que los supervisores provean orientación sobre cómo deben diseñarse los registros para la recopilación de estos datos.
- La gestión del riesgo operacional no debe estar desligada de la gestión de los otros riesgos inherentes a la actividad de intermediación financiera. Por el contrario, la gestión del riesgo operacional debe ser parte de un enfoque integral de gestión de riesgos.
- Se debe promover que los bancos divulguen información suficiente que permita a los participantes del mercado entender y evaluar la exposición al riesgo operacional del banco, la calidad de su gestión y las medidas adoptadas para mitigar dicha exposición.

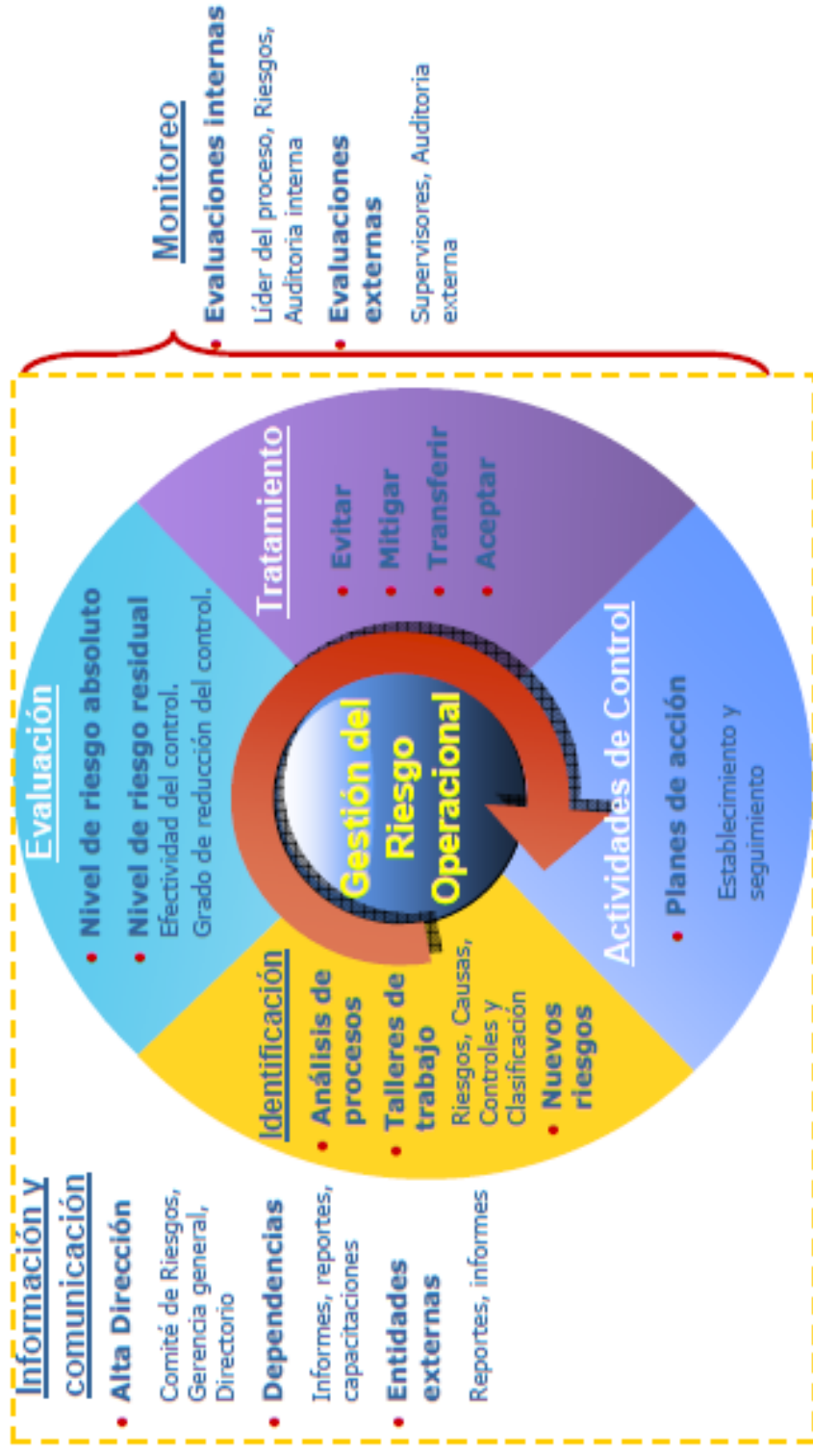
- Las instituciones financieras deben registrar y acumular información histórica por línea de negocios y tipo de evento, con el objeto de identificar:
 - Los riesgos de la unidad de negocio;
 - Las estimaciones de pérdidas esperadas;
 - Las estimaciones de pérdidas inesperadas;
 - La frecuencia de los eventos de pérdida;
 - La severidad de los eventos de pérdida;
 - La tendencia de los eventos de pérdida.
- Es importante entender que una vez identificadas las amenazas y las respectivas vulnerabilidades organizacionales, es fundamental establecer los respectivos controles para fortalecer las vulnerabilidades y minimizar la posibilidad de que el desastre penetre en la empresa y cause daño.
- La Metodología para la Identificación y Cuantificación del Riesgo Operativo diseñada en este trabajo consta de pasos que permiten, no sólo identificar las principales fuentes de riesgo operativo, sino también cuantificar la exposición al mismo y calcular las provisiones que debe realizar la entidad para cubrir cualquier evento de pérdida que se pueda presentar.

7. REFERENCIAS BIBLIOGRÁFICAS

- Comité de Basilea de Supervisión Bancaria: Sanas Prácticas para la Gestión y supervisión del Riesgo Operativo, febrero 2003, Banco de Pagos Internacionales
- The Operational Riskdata eXchange Association <http://www.orx.org/index.php>
- Committee of Sponsoring Organizations of the Treadway Commission <http://www.coso.org>
- Bank for International Settlements <http://www.bis.org/>
- Comité de Basilea de Supervisión Bancaria Convergencia Internacional de Medición de Capital y Estándares de Capital Un marco revisado, junio 2004, Banco de Pagos Internacionales.
- Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley 26702. Perú, Febrero 2004
- Risk-Based Capital Guidelines; Capital Adequacy Guidelines; Capital Maintenance: Domestic Capital Modifications - Joint advance notice of proposed rulemaking (ANPR). published in the Federal Register on October 20, 2005
- Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos y Seguros del Ecuador, Título VII, Subtítulo VI, Capítulo V “De la Gestión del Riesgo Operativo” (Resolución No. JB-2005-834)
Alexander, C. 2002. Advanced Risk Management. IFF.
- Neil, M. & Tranham E. 2002. Using Bayesian Networks to predict Op Risk. Operational Risk.

8. ANEXOS

ANEXO N° 01
ETAPAS DEL PROCESO DE LA GESTIÓN DEL RIESGO OPERACIONAL



ANEXO N° 2

LINEAS DE NEGOCIO GENÉRICAS PARA EMPRESAS DEL SISTEMA FINANCIERO

Nivel 1	Nivel 2	Definición
Finanzas corporativas	Finanzas corporativas	Realización de operaciones de financiamiento estructurado y participación en procesos de titulización; underwriting; asesoramiento financiero a empresas corporativas, grandes y medianas empresas, así como al gobierno central y entidades del sector público; entre otras actividades de naturaleza similar.
	Finanzas de administraciones públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Operaciones de tesorería; compra y venta de títulos, monedas y commodities por cuenta propia; entre otras actividades de naturaleza similar.
	Creación de mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Financiamiento a clientes minoristas incluyendo tarjetas de crédito, préstamo automotriz, entre otros.
Banca comercial	Banca comercial	Financiamiento a clientes no minoristas, incluyendo: factoring, descuento, arrendamiento financiero, entre otros.
Liquidación y pagos	Clientes externos	Actividades relacionadas con pagos y cobranzas, transferencia interbancaria de fondos, compensación y liquidación, entre otras actividades de naturaleza similar.
Otros servicios	Custodia	Servicios de custodia, fideicomisos, comisiones de confianza y otros servicios.
	Encargos de confianza	
	Fideicomisos	
	Otros servicios	

ANEXO N° 3

TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Tipo de evento (Nivel 1)	Definición	Tipo de evento (Nivel 2)	Ejemplos
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicado, al menos, un miembro de la empresa.	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones (intencional).
		Robo y fraude	Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional).
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	Robo y fraude	Robo, falsificación.
		Seguridad de los sistemas	Daños por ataques informáticos, robo de información.
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad o discriminación.	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
		Higiene y seguridad en el trabajo	Casos relacionados con las normas de higiene y seguridad en el trabajo; indemnización a los trabajadores.
		Diversidad y discriminación	Todo tipo de discriminación.
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información (conocimiento del cliente, etc.), quebrantamiento de la privacidad de información sobre clientes minoristas, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial.
		Prácticas empresariales	Prácticas restrictivas de la competencia, prácticas comerciales /

		o de mercado improcedentes	de mercado improcedentes, manipulación del mercado, abuso de información privilegiada (en favor de la empresa), lavado de dinero.
		Productos defectuosos	Defectos del producto (no autorizado, etc.), error de los modelos.
		Selección, patrocinio y riesgos	Ausencia de investigación a clientes conforme a las directrices, exceso de los límites de riesgo frente a clientes.
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento.
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Desastres y otros acontecimientos	Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo).
Interrupción del negocio y fallos en los sistemas	Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas	Sistemas	Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo (p.ej. en el Delivery vs. Payment).
		Seguimiento y presentación de informes	Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas).
		Aceptación de clientes y documentación	Inexistencia de autorizaciones / rechazos de clientes, documentos jurídicos inexistentes / incompletos.
		Gestión de cuentas de clientes	Acceso no autorizado a cuentas, registros incorrectos de clientes (con generación de pérdidas), pérdida o daño de activos de clientes por negligencia.
		Contrapartes comerciales	Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes.
		Distribuidores y proveedores	Subcontratación, litigios con proveedores.

ANEXO N° 04

CÁLCULOS PARA LA EVALUACIÓN DE LOS NIVELES DE RIESGO ABSOLUTO Y RESIDUAL

1. CÁLCULO DEL NIVEL DE RIESGO ABSOLUTO

$$NRA = Fa * Ia$$

Donde:

Fa: Frecuencia absoluta

Ia: Impacto Absoluto

2. CÁLCULO DEL NIVEL DEL RIESGO RESIDUAL

2.1 La efectividad del control

De acuerdo a los valores asignados para cada características de la Tabla de Evaluación de Efectividad de Control por su respectiva ponderación (tabla N° 4), se halla el puntaje por cada uno de los controles evaluados.

$$Ec_i = \sum_{c=5} V_c \times P_c$$

Donde:

Vc: Valor asignado para la característica c del control i

Pc: Ponderación asignada para la característica c

Eci: Efectividad del control evaluado (Tabla N° 5)

2.2 Grado de Reducción del Control

En base a la tabla N° 06 se elige el grado de reducción (bueno, medio, pobre y nulo) por cada tipo de control, teniendo en cuenta si afecta a la Frecuencia o Impacto.

$RF_i, RI_i = \{0\%, 30\%, 60\%, 90\%\}$

Donde:

RFi: Reducción del control i sobre la Frecuencia

RCi: Reducción del control i sobre el Impacto

2.3 Cobertura del Control

2.3.1 Control reduce la frecuencia

$$CF = \frac{\sum Ec_i \times RFi}{n}$$

Donde:

CF: Cobertura del Control sobre la frecuencia

RFi: Grado de Reducción del Control i sobre la frecuencia

Eci: Efectividad del control i

n: Número de controles que afectan a la frecuencia

2.3.2 Control reduce el impacto

$$CI = \frac{\sum Ec_i \times RI_i}{n}$$

Donde:

CI: Cobertura del Control i sobre el Impacto

RIi: Grado de Reducción del control i sobre el Impacto

Eci: Efectividad del control i

n: Número de controles que afectan al Impacto

Una vez hallada la cobertura del control sobre la frecuencia y/o sobre el impacto, se hallarán los niveles de frecuencia e impacto residuales, es decir considerando los controles.

2.3.3 Frecuencia residual del riesgo

$$F_r = F_a \times (1 - CF)$$

Donde:

Fr: Frecuencia residual del riesgo

Fa: Frecuencia absoluta

CF: Cobertura del Control sobre la frecuencia

2.3.4 Impacto del riesgo con controles

$$I_r = I_a \times (1 - CI)$$

Donde:

Ir: Impacto residual del riesgo

Ia: Impacto absoluto

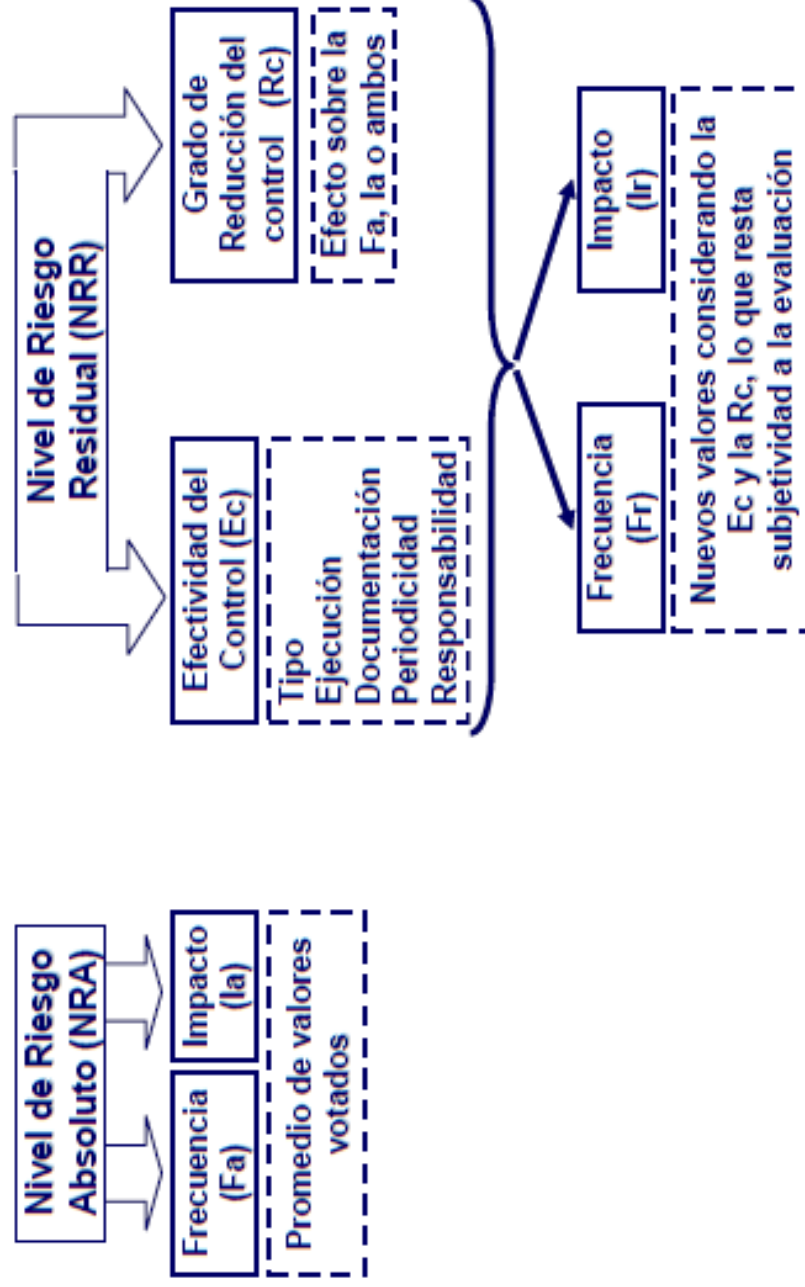
CI: Cobertura del control sobre el impacto

Finalmente, el nivel del riesgo residual se halla como el producto de la frecuencia e impacto residuales.

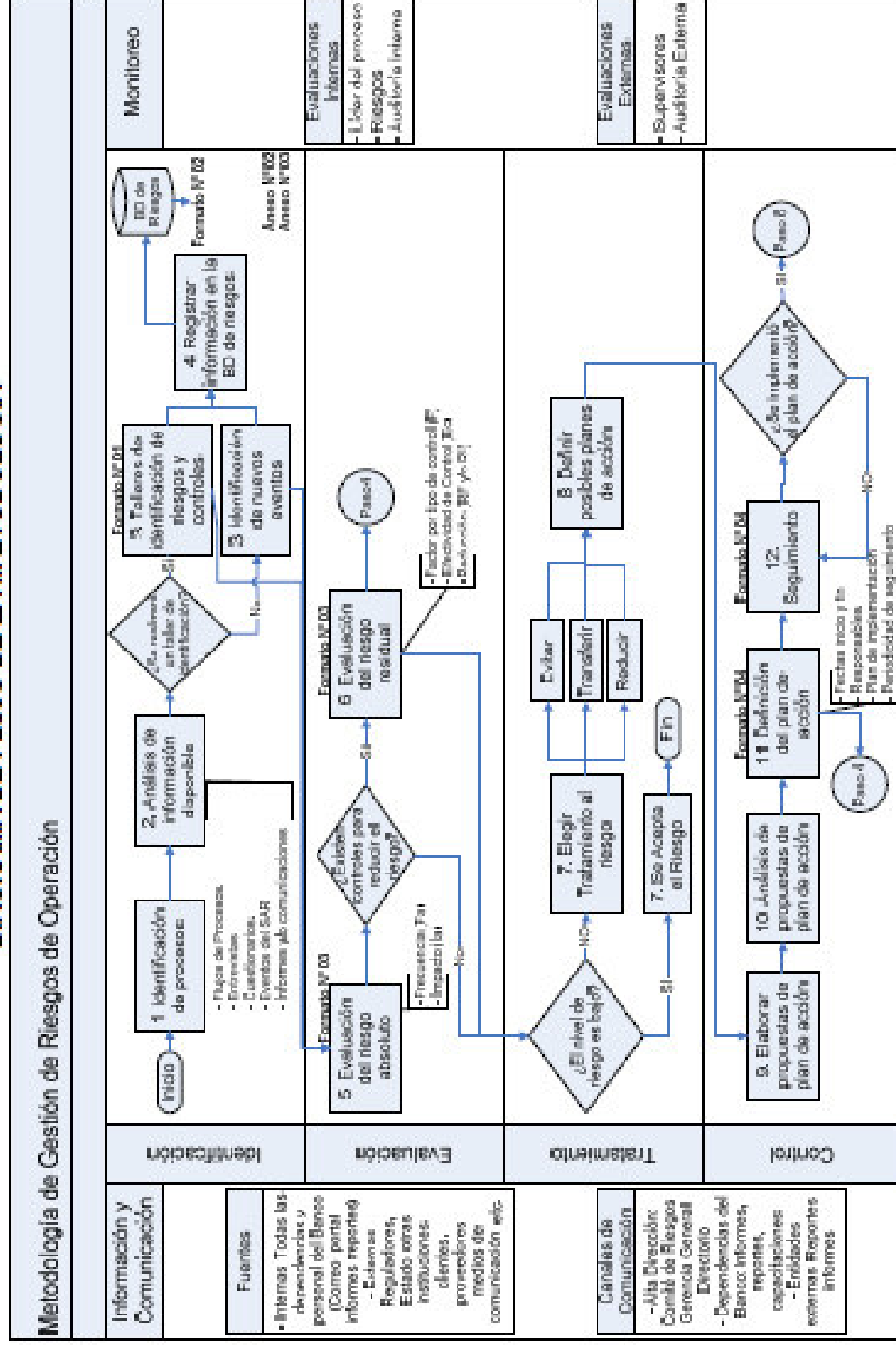
$$NRR = F_r \times I_r$$

Una vez implementado el plan de acción, el Nivel de Riesgo Residual debe ser reevaluado.

ANEXO N° 05
ESQUEMA DE EVALUACIÓN DE NIVELES DE RIESGO



ANEXO Nº 06 DIAGRAMA DE FLUJO DE LA METODOLOGÍA



ANEXO 07

Lima, 10 de enero de 2008

Resolución S.B.S.

N° 37 - 2008

*El Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones:*

CONSIDERANDO:

Que, el numeral 2 del artículo 134° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702 y sus modificatorias, en adelante Ley General, dispone como un medio de protección al ahorrista, supervisar que las empresas del sistema financiero se encuentren debidamente organizadas, así como administradas por personal idóneo;

Que, la Asociación Internacional de Supervisores de Seguros –IAIS – dispone en el Principio Básico de Seguros 18 “Evaluación y administración de riesgos” que la autoridad supervisora requiere que las aseguradoras reconozcan el rango de riesgos que ellos enfrentan y que los evalúen y administren con efectividad;

Que, conforme al inciso e) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF, es atribución y obligación de la Superintendencia fiscalizar a las AFP en el cumplimiento de las disposiciones legales y directivas administrativas que les rigen, razón por la cual resulta conveniente incluirlas dentro del ámbito de aplicación de la Gestión Integral de Riesgos;

Que, de conformidad con el artículo 290° de la Ley General, constituye un requisito para la ampliación de las operaciones de las empresas del sistema financiero, contar con controles internos adecuados para las nuevas operaciones;

Que, es objetivo de esta Superintendencia propender a que las empresas supervisadas cuenten con una Gestión Integral de Riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios;

Que, dicha Gestión Integral de Riesgos debe estar diseñada para contar con un entorno interno apropiado, desarrollar una adecuada determinación de objetivos, implementar una oportuna identificación, evaluación,

tratamiento y control de riesgos, así como elaborar los reportes pertinentes y efectuar un adecuado monitoreo;

Que, es necesario revisar los criterios previstos en el Reglamento del Sistema de Control interno a fin de hacerlo compatible con las mejores prácticas internacionales para el desarrollo de una Gestión Integral de Riesgos, tomando como referencia, entre otros documentos, al Marco Integrado para la Gestión de Riesgos Corporativos, publicado por el Committee of Sponsoring Organizations of the Treadway Commission (COSO); y hacerlo extensivo al conjunto de las empresas supervisadas bajo un único marco de referencia;

Estando a lo opinado por las Superintendencias Adjuntas de Banca y Microfinanzas, Seguros, Administradoras Privadas de Fondos de Pensiones, Riesgos, Asesoría Jurídica, así como por la Gerencia de Estudios Económicos; y,

En uso de las atribuciones conferidas por el numeral 7 del artículo 349° de la Ley General;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento de la Gestión Integral de Riesgos, que forma parte de la presente Resolución.

Artículo Segundo.- La presente Resolución entra en vigencia a partir del día siguiente a su publicación en el Diario Oficial El Peruano, otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de diciembre de 2008, fecha a partir de la cual quedarán sin efecto la Resolución SBS N° 1040-99, así como todas aquellas disposiciones que se le opongan de manera total o parcial.

Artículo Tercero.- Incorpórese el procedimiento N° 110 “Autorizaciones especiales sobre la Gestión Integral de Riesgos” del Texto Único de Procedimientos Administrativos – TUPA de la Superintendencia de Banca, Seguros y AFP aprobado mediante Resolución SBS N° 131-2002, conforme el texto que se adjunta a la presente Resolución.

Regístrese, comuníquese y publíquese,

FELIPE TAM FOX

Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

REGLAMENTO DE LA GESTIÓN INTEGRAL DE RIESGOS

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1°.- Alcance

El presente Reglamento será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Artículo 2°.- Definiciones

Para la aplicación de la presente Norma deberán considerarse las siguientes definiciones:

- a) **Apetito por el riesgo.-** El nivel de riesgo que la empresa está dispuesta a asumir en su búsqueda de rentabilidad y valor.
- b) **Casa Matriz.-** Se refiere a la sociedad principal o a la que ejerza el control en un conglomerado financiero o mixto.
- c) **Control interno.-** Un proceso, realizado por el Directorio, la Gerencia y el personal, diseñado para proveer un aseguramiento razonable en el logro de objetivos referidos a la eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, y cumplimiento de las leyes aplicables y regulaciones.
- d) **Directorio.-** Toda referencia al Directorio, entiéndase realizada también a cualquier órgano equivalente.
- e) **Director Independiente.-** Un director que es seleccionado por su prestigio profesional y que no se encuentra vinculado con la administración de la empresa ni con el grupo económico de la misma.
- f) **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.
- g) **Impacto.-** La consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos. Usualmente se expresará en términos monetarios, como pérdidas financieras. También es llamado severidad.
- h) **Manuales de gestión de riesgos.-** Documentos que contienen las funciones, responsabilidades, políticas, metodologías y procedimientos dispuestos para la identificación, evaluación, tratamiento, control, reporte y monitoreo de los riesgos de la empresa.
- i) **Manuales de organización y funciones.-** Documentos que detallan la estructura orgánica de la empresa, los objetivos y funciones de sus unidades, así como las obligaciones y responsabilidades de su personal.

- j) Manuales de políticas y procedimientos.- Documentos que contienen funciones, responsabilidades, las políticas, metodologías y procedimientos establecidos por la empresa para la realización de las actividades de cada una de las unidades con las que cuenta, incluyendo las que corresponden a la gestión de riesgos.
- k) Probabilidad.- La posibilidad de la ocurrencia de un evento que usualmente es aproximada mediante una distribución estadística. En ausencia de información suficiente, o donde no resulta posible obtenerla, se puede aproximar mediante métodos cualitativos.
- l) Proceso.- Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- m) Riesgo.- La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.
- n) Seguridad razonable.- Se refiere al nivel de seguridad que una empresa puede tener en alcanzar sus objetivos, considerando que siempre es posible que se produzcan desviaciones o impactos financieros importantes que no sean prevenidos o detectados, dada la incertidumbre inherente al futuro.
- o) Subcontratación.- Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizada por la empresa contratante.
- p) Superintendencia.- Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.
- q) Tolerancia al riesgo.- El nivel de variación que la empresa está dispuesta a asumir en caso de desviación a los objetivos empresariales trazados.

CAPÍTULO II

GESTIÓN INTEGRAL DE RIESGOS

Artículo 3º.- Gestión Integral de Riesgos

La Gestión Integral de Riesgos es un proceso, efectuado por el Directorio, la Gerencia y el personal aplicado en toda la empresa y en la definición de su estrategia, diseñado para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos.

La Gestión Integral de Riesgos considera las siguientes categorías de objetivos:

- a) Estrategia.- Son objetivos de alto nivel, vinculados a la visión y misión empresarial.
- b) Operaciones.- Son objetivos vinculados al uso eficaz y eficiente de los recursos.
- c) Información.- Son objetivos vinculados a la confiabilidad de la información suministrada.
- d) Cumplimiento.- Son objetivos vinculados al cumplimiento de las leyes y regulaciones aplicables.

Las empresas deben efectuar una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

Artículo 4º.- Componentes

La Gestión Integral de Riesgos puede descomponerse en componentes, que se encuentran presentes en diverso grado, según se analice la totalidad de la empresa, una línea de negocio, un proceso o una unidad organizativa. La empresa podrá contar con una

descomposición propia, que se adapte a su organización, pero ella debe considerar los principales elementos descritos a continuación:

- a) **Ambiente interno.-** Que comprende, entre otros, los valores éticos, la idoneidad técnica y moral de sus funcionarios; la estructura organizacional; y las condiciones para la asignación de autoridad y responsabilidades.
- b) **Establecimiento de objetivos.-** Proceso por el que se determinan los objetivos empresariales, los cuales deben encontrarse alineados a la visión y misión de la empresa, y ser compatibles con la tolerancia al riesgo y el grado de exposición al riesgo aceptado.
- c) **Identificación de riesgos.-** Proceso por el que se identifican los riesgos internos y externos que pueden tener un impacto negativo sobre los objetivos de la empresa. Entre otros aspectos, considera la posible interdependencia entre eventos, así como los factores influyentes que los determinan.
- d) **Evaluación de riesgos.-** Proceso por el que se evalúa el riesgo de una empresa, actividad, conjunto de actividades, área, portafolio, producto o servicio; mediante técnicas cualitativas, cuantitativas o una combinación de ambas.
- e) **Tratamiento.-** Proceso por el que se opta por aceptar el riesgo, disminuir la probabilidad de ocurrencia, disminuir el impacto, transferirlo total o parcialmente, evitarlo, o una combinación de las medidas anteriores, de acuerdo al nivel de tolerancia al riesgo definido.
- f) **Actividades de control.-** Proceso que busca asegurar que las políticas, estándares, límites y procedimientos para el tratamiento de riesgos son apropiadamente tomados y/o ejecutados. Las actividades de control están preferentemente incorporadas en los procesos de negocio y las actividades de apoyo. Incluye los controles generales así como los de aplicación a los sistemas de información, además de la tecnología de información relacionada. Buscan la eficacia y efectividad de las operaciones de la empresa, la confiabilidad de la información financiera u operativa, interna y externa, así como el cumplimiento de las disposiciones legales que le sean aplicables.
- g) **Información y comunicación.-** Proceso por el que se genera y transmite información apropiada y oportuna a la dirección, la gerencia, el personal, así como a interesados externos tales como clientes, proveedores, accionistas y reguladores, entre ellos esta Superintendencia. Esta información es interna y externa, y puede incluir información de gestión, financiera y operativa.
- h) **Monitoreo.-** Proceso que consiste en la evaluación del adecuado funcionamiento de la Gestión Integral de Riesgos y la implementación de las modificaciones que sean requeridas. El monitoreo debe realizarse en el curso normal de las actividades de la empresa, y complementarse por evaluaciones independientes o una combinación de ambas. Incluye el reporte de las deficiencias encontradas y su corrección.

Artículo 5º.- Tipos de riesgos

Los riesgos pueden surgir por diversas fuentes, internas o externas, y pueden agruparse en diversas categorías o tipos. Algunos riesgos pueden encontrarse asociados a una actividad en particular, como en el proceso de inversión, que se encuentra expuesto a riesgos de crédito, de mercado, de operación, entre otros. A continuación se enumera una lista no limitativa de los diversos tipos de riesgos a que está expuesta una empresa:

- a) **Riesgo de crédito**

La posibilidad de pérdidas por la imposibilidad o falta de voluntad de los deudores o contrapartes, o terceros obligados para cumplir completamente sus obligaciones contractuales registradas dentro o fuera del balance general.

b) Riesgo estratégico

La posibilidad de pérdidas por decisiones de alto nivel asociadas a la creación de ventajas competitivas sostenibles. Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias claves de la empresa y en el proceso de generación e innovación de valor.

c) Riesgo de liquidez

La posibilidad de pérdidas por incumplir con los requerimientos de financiamiento y de aplicación de fondos que surgen de los descargos de flujos de efectivo, así como por no poder cerrar rápidamente posiciones abiertas, en la cantidad suficiente y a un precio razonable.

d) Riesgo de mercado

La posibilidad de pérdidas en posiciones dentro y fuera de balance derivadas de fluctuaciones en los precios de mercado.

e) Riesgo operacional

La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

f) Riesgo de seguro

La posibilidad de pérdidas por las bases técnicas o actuariales empleadas en el cálculo de las primas y de las reservas técnicas de los seguros, insuficiencia de la cobertura de reaseguros, así como el aumento inesperado de los gastos y de la distribución en el tiempo de los siniestros. Se le conoce también como riesgo técnico.

g) Riesgo de reputación

La posibilidad de pérdidas por la disminución en la confianza en la integridad de la institución que surge cuando el buen nombre de la empresa es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una organización.

Artículo 6°.- Prácticas cuestionables

La empresa deberá establecer los sistemas internos apropiados que faciliten la oportuna denuncia e investigación de las actividades ilícitas, fraudulentas, identificadas por cualquier trabajador de la empresa o por alguna persona que interactúa con ésta. Dichas actividades deberán ser reportadas a la unidad de auditoría interna, para lo cual la empresa implementará procedimientos que permitan mantener la confidencialidad del denunciante. En el caso de que los hechos sean significativos, la unidad de auditoría interna deberá informar al Comité de Auditoría y a la Superintendencia.

Artículo 7°.- Relación de la Gestión Integral de Riesgos y el Control Interno

La Gestión Integral de Riesgos incluye al control interno del que es parte integral. La Gestión Integral de Riesgos expande y desarrolla los conceptos de control interno en una forma más amplia y sólida, con un mayor énfasis en el riesgo.

El objetivo de confiabilidad en la información financiera del control interno se encuentra principalmente referido a la confiabilidad de los estados financieros. En la Gestión Integral de Riesgos, este objetivo es expandido para incluir todos los reportes e informes generados por las empresas, tanto internos como externos. Entre ellos los usados por la Dirección y la Gerencia, aquellos enviados a terceros, información entregada a los reguladores, así como a accionistas y otros grupos de interés. El alcance también incorpora la información no financiera.

De acuerdo a lo indicado en el artículo 3°, una nueva categoría de objetivos referidos a la estrategia, y las categorías de objetivos referidos a las operaciones, información y cumplimiento deben encontrarse alineados a la estrategia. La Gestión Integral de Riesgos es aplicada también en la selección de objetivos.

CAPÍTULO III

EL DIRECTORIO Y LA GERENCIA

Artículo 8°.- Responsabilidad del Directorio

El Directorio es responsable de establecer una gestión integral de riesgos y de propiciar un ambiente interno que facilite su desarrollo adecuado. Entre sus responsabilidades específicas están:

- a) Aprobar las políticas generales que guíen las actividades de la empresa en la gestión de los diversos riesgos que enfrenta.
- b) Seleccionar una plana gerencial con idoneidad técnica y moral, que actúe de forma prudente y apropiada en el desarrollo de sus negocios y operaciones, así como en el cumplimiento de sus responsabilidades.
- c) Aprobar los recursos necesarios para el adecuado desarrollo de la Gestión Integral de Riesgos, a fin de contar con la infraestructura, metodología y personal apropiado.
- d) Establecer un sistema de incentivos que fomente el adecuado funcionamiento de una gestión integral de riesgos y que no favorezca la toma inapropiada de riesgos.
- e) Aprobar los manuales de organización y funciones, de políticas y procedimientos y demás manuales de la empresa.
- f) Aprobar políticas generales para las responsabilidades a cargo de la empresa, incluyendo:
 - f.1 La administración prudente y según los acuerdos establecidos o la regulación aplicable, de los activos en depósito y en custodia, administrados o invertidos por cuenta de clientes y terceros, evitando conflictos de interés.
 - f.2 Asegurar razonablemente que los consejos de inversión o similares realizados en su ámbito, son presentados con la información apropiada, al tener en cuenta la tolerancia al riesgo y expectativa de rendimiento del cliente.
- g) Establecer los objetivos empresariales, evaluar y aprobar sus planes de negocios con debida consideración a los riesgos asociados.
- h) Conocer los principales riesgos afrontados por la entidad estableciendo, cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.
- i) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.

- j) Asegurar razonablemente que el patrimonio contable de la empresa sea suficiente para enfrentar los riesgos a los que está expuesto, para lo cual debe conocer las necesidades de capital y establecer políticas de gestión que apoye las necesidades de la empresa, cumpliendo con los requerimientos regulatorios de manera apropiada.
- k) Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión de los riesgos a que está expuesta, y que los principales riesgos se encuentran bajo control dentro de los límites que han establecido.

Artículo 9º.- Declaración de cumplimiento del Directorio

El Directorio es responsable de evaluar el adecuado funcionamiento de los criterios definidos en la presente normativa. Anualmente, el Directorio suscribirá una Declaración de cumplimiento, que contendrá cuando menos lo indicado a continuación, pudiendo la Superintendencia definir criterios mínimos adicionales mediante oficio múltiple de aplicación general:

- a) Que el Directorio conoce los estándares previstos en la presente norma, así como sus responsabilidades.
- b) Que la empresa cuenta con una gestión apropiada de sus riesgos para la complejidad y tamaño de la empresa, así como de los criterios indicados en la presente norma, con la excepción de posibles deficiencias identificadas y comunicadas en la declaración.
- c) Que el Directorio ha tomado conocimiento de la información de la Gerencia, de los informes del Comité de Auditoría, del Comité de Riesgos, de Auditoría Externa, y de otra información que el Directorio considere relevante, y que las medidas correctivas dispuestas consten en las actas correspondientes.

Esta declaración será suscrita en un plazo que no excederá de ciento veinte (120) días calendario posterior al ejercicio anual, debiendo estar a disposición de esta Superintendencia.

Artículo 10º.- Responsabilidad de la Gerencia

La gerencia general tiene la responsabilidad de implementar la Gestión Integral de Riesgos conforme a las disposiciones del Directorio, además de las responsabilidades dadas por otras normas.

La gerencia podrá constituir comités para el cumplimiento de sus responsabilidades.

Los gerentes de las unidades organizativas de negocios o de apoyo, en su ámbito de acción, tienen la responsabilidad de administrar los riesgos relacionados al logro de los objetivos de sus unidades. Entre sus responsabilidades específicas están:

- a) Asegurar la consistencia entre las operaciones y los niveles de tolerancia al riesgo definidos aplicables a su ámbito de acción.
- b) Asumir, ante el gerente de nivel inmediato superior, los resultados de la gestión de riesgos correspondiente a su unidad; y así hasta llegar al gerente general que tiene esta responsabilidad ante el Directorio.

CAPÍTULO IV LOS COMITÉS DEL DIRECTORIO

Artículo 11°.- Comités

El Directorio podrá constituir los comités que considere necesarios con la finalidad de dar cumplimiento a las disposiciones contenidas en el presente reglamento y a las responsabilidades señaladas por el artículo 8° anteriormente citado.

Para el caso de las empresas de operaciones múltiples y las empresas de seguros a las que se refiere el artículo 16° de la Ley General, así como para las AFP, será obligatoria la constitución de un comité de auditoría y un comité de riesgos. En el caso de aquellas empresas que no se encuentren obligadas a constituir los comités y que, además, decidan no hacerlo, todas las funciones atribuidas a el(los) comité(s) no constituido(s) serán asumidas por el Directorio.

Artículo 12°.- Reglamento de los Comités

Los Comités constituidos por el Directorio deberán contar con un Reglamento que contendrá las políticas y procedimientos necesarios para el cumplimiento de sus funciones. Dicho reglamento establecerá, entre otros aspectos, los criterios para evitar conflictos de intereses, incompatibilidad de funciones, la periodicidad de sus reuniones, sus actividades programadas, la información que debe ser remitida, así como la forma como reportará al Directorio. Los acuerdos adoptados en las reuniones deberán constar en un Libro de Actas.

SUB-CAPÍTULO I COMITÉ DE RIESGOS

Artículo 13°.- Conformación del comité de riesgos

El comité de riesgos deberá estar conformado por al menos un miembro del Directorio, y se organizará como un comité integral, que deberán abarcar las decisiones que atañen a los riesgos significativos a los que esté expuesta la empresa. Los integrantes del Comité de Riesgos deben tener los conocimientos y la experiencia necesaria para cumplir adecuadamente sus funciones.

El Directorio podrá crear los comités de riesgos especializados que considere necesarios, en razón del tamaño y complejidad de las operaciones y servicios de la empresa.

Artículo 14°.- Funciones del comité de riesgos

El comité de riesgos, por delegación del Directorio y dentro de los límites que éste fije, podrá asumir las siguientes funciones:

- a) Aprobar las políticas y la organización para la Gestión Integral de Riesgos, así como las modificaciones que se realicen a los mismos.
- b) Definir el nivel de tolerancia y el grado de exposición al riesgo que la empresa está dispuesta a asumir en el desarrollo del negocio.
- c) Decidir las acciones necesarias para la implementación de las acciones correctivas requeridas, en caso existan desviaciones con respecto a los niveles de tolerancia al riesgo y a los grados de exposición asumidos.

- d) Aprobar la toma de exposiciones que involucren variaciones significativas en el perfil de riesgo de la empresa o de los patrimonios administrados bajo responsabilidad de la empresa.
- e) Evaluar la suficiencia de capital de la empresa para enfrentar sus riesgos y alertar de las posibles insuficiencias.
- f) Proponer mejoras en la Gestión Integral de Riesgos.

SUB-CAPÍTULO II COMITÉ DE AUDITORÍA

Artículo 15°.- Conformación del comité de auditoría

El comité de auditoría deberá estar conformado por miembros del Directorio que no realicen actividades de gestión en la empresa. Dicho comité tendrá como mínimo tres (3) miembros, debiendo renovarse cada tres (3) años, al menos, uno de ellos. Los integrantes del comité de auditoría deben tener los conocimientos y la experiencia necesarios para cumplir adecuadamente sus funciones.

Para el caso de las empresas de operaciones múltiples y las empresas de seguros a las que se refiere el artículo 16° de la Ley General; así como para las AFP; el comité de auditoría deberá estar conformado por al menos un director independiente.

Artículo 16°.- Funciones del comité de auditoría

El comité de auditoría tiene como propósito principal vigilar que los procesos contables y de reporte financiero sean apropiados, así como evaluar las actividades realizadas por los auditores internos y externos.

Entre sus principales funciones están:

- a) Vigilar el adecuado funcionamiento del sistema de control interno;
- b) Informar al Directorio sobre la existencia de limitaciones en la confiabilidad de los procesos contables y financieros;
- c) Vigilar y mantener informado al Directorio sobre el cumplimiento de las políticas y procedimientos internos y sobre la detección de problemas de control y administración interna, así como de las medidas correctivas implementadas en función de las evaluaciones realizadas por la unidad de auditoría interna, los auditores externos y esta Superintendencia;
- d) Definir los criterios para la selección y contratación de los auditores externos, evaluar su desempeño así como determinar los informes complementarios que requieran para el mejor desempeño de sus funciones o el cumplimiento de requisitos legales, salvo en aquellos casos en los que el comité de auditoría de la casa matriz asuma las funciones de definir los criterios para la selección y contratación de los auditores externos, así como la evaluación de sus desempeño; y,
- e) Definir los criterios para la selección y contratación del auditor interno y sus principales colaboradores, fijar su remuneración y evaluar su desempeño, así como su

régimen de incentivos monetarios, salvo que dichas funciones sean asumidas por el comité de auditoría de la casa matriz.

CAPÍTULO V

UNIDAD DE RIESGOS

Artículo 17º.- Unidad de Riesgos

La Gestión Integral de Riesgos requiere que las empresas se organicen de acuerdo a su complejidad y líneas de negocio en que operan. En este sentido, las empresas podrán contar con una unidad centralizada o con unidades especializadas en la gestión de riesgos específicos, de acuerdo a la naturaleza de las operaciones y la estructura de la empresa, siempre que cuando sean éstas tomadas en su conjunto, permitan la implementación de los criterios previstos en la presente norma.

La Superintendencia podrá requerir la creación de una unidad de riesgos integral en empresas que a su criterio resulten complejas, y cuando se observe en el ejercicio de las acciones de supervisión que no se cumple con los criterios previstos en la normativa vigente.

Siempre que no sea requerido por la normativa vigente, cuando no exista una unidad de riesgos especializada, y en ausencia de delegación del Directorio, se entenderá que estas funciones han sido asignadas a la gerencia general.

Los integrantes de la Unidad de Riesgos deberán poseer la experiencia y conocimientos que les permitan el apropiado cumplimiento de sus funciones, para lo cual deberá establecerse un plan de capacitación que será presentado al directorio anualmente.

Artículo 18º.- Funciones de la Unidad de Riesgos

La Unidad de Riesgos deberá participar en el diseño y permanente adecuación de los manuales de gestión de riesgos y demás normas internas que tengan por objeto definir las responsabilidades de las unidades de negocios y sus funcionarios en el control de riesgos de la empresa.

La Unidad de Riesgos es la encargada de apoyar y asistir a las demás unidades de la empresa para la realización de una buena gestión de riesgos en sus áreas de responsabilidad, y para ello debe ser independiente de las unidades de negocios.

Las principales responsabilidades de la unidad de riesgos son las siguientes:

- a) Proponer las políticas, procedimientos y metodologías apropiadas para la Gestión Integral de Riesgos en la empresa, incluyendo los roles y responsabilidades;

- b) Velar por una Gestión Integral de Riesgos competente, promoviendo el alineamiento de las medidas de tratamiento de los riesgos de la empresa con los niveles de tolerancia al riesgo y el desarrollo de controles apropiados;
- c) Guiar la integración entre la gestión de riesgos, los planes de negocio y las actividades de gestión empresarial;
- d) Establecer un lenguaje común de gestión de riesgos basado en las definiciones de esta norma y de los demás reglamentos aplicables;
- e) Estimar los requerimientos patrimoniales que permitan cubrir los riesgos que enfrenta la empresa, así como los requerimientos regulatorios, de ser el caso. Además, alertar sobre las posibles insuficiencias de patrimonio efectivo para cubrir los riesgos identificados; y,
- f) Informar a la gerencia general y al comité de riesgos los aspectos relevantes de la gestión de riesgos para una oportuna toma de decisiones.

Artículo 19°.- Jefe de la Unidad de Riesgos

El jefe de la Unidad de Riesgos deberá tener apropiada formación académica y experiencia relevante, quién debe coordinar permanentemente con la gerencia, el comité de riesgos, el comité de auditoría, los comités especializados, las unidades de negocio y de apoyo, así como con esta Superintendencia, en cuanto a la Gestión Integral de Riesgos realizada por la empresa.

Además, es responsable de informar al Directorio, comités respectivos y a las áreas de decisión correspondientes, sobre los riesgos, el grado de exposición al riesgo aceptado y la gestión de éstos, de acuerdo a las políticas y procedimientos establecidos por la empresa.

Los criterios mencionados son de aplicación a los jefes de las unidades de riesgos especializadas, en caso que no exista una unidad centralizada.

El jefe de la Unidad de Riesgos, en caso que la Unidad de Riesgos sea centralizada, deberá tener nivel gerencial.

Artículo 20°.- Informe Anual de Riesgos

La Unidad de Riesgos deberá elaborar al cierre de cada ejercicio, un informe anual de riesgos, que incluya el plan de actividades para el ejercicio siguiente.

Posteriormente, mediante Oficio Múltiple, la Superintendencia podrá definir la estructura mínima del informe anual de riesgos, informes parciales por riesgos, informes periódicos de situación, así como su presentación por medios electrónicos.

CAPÍTULO VI SUBCONTRATACIÓN

Artículo 21°.- Subcontratación

Las empresas y las personas cuyas responsabilidades se hayan determinado en el presente reglamento y demás normas, asumen plena responsabilidad sobre los resultados de los procesos subcontratados con terceros, pudiendo ser sancionados por su incumplimiento. Asimismo deben asegurarse que se mantenga reserva y confidencialidad sobre la información que pudiera serles proporcionada.

En toda subcontratación significativa, un análisis formal de los riesgos asociados deberá ser realizado y puesto en conocimiento del Directorio para su aprobación. Se entenderá por 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.

La subcontratación de una o más funciones de la gestión de riesgos será considerada como significativa para fines de este reglamento.

Las empresas deberán asegurarse de que en los casos de subcontratación significativa, los contratos suscritos con los proveedores correspondientes incluyan cláusulas que faciliten una adecuada revisión de la respectiva prestación por parte de las empresas, de la Unidad de Auditoría Interna, de la Sociedad de Auditoría Externa, así como por parte de la Superintendencia o la persona que ésta designe.

En el caso de subcontratación significativa del servicio de auditoría interna, se sujetará a lo establecido en el Reglamento de Auditoría Interna.

CAPÍTULO VII ROL DE LA AUDITORÍA INTERNA Y EXTERNA

Artículo 22°.- Unidad de Auditoría Interna

La Auditoría Interna, desempeña un rol independiente a la gestión, que vigila la adecuación de la Gestión Integral de Riesgos, debiendo sujetarse a las disposiciones específicas que regulan su actividad en el Reglamento de Auditoría Interna.

Artículo 23°.- Auditores Externos

La Auditoría Externa es independiente a la empresa y tiene como función principal la evaluación de la confiabilidad de la información financiera, debiendo sujetarse a las disposiciones específicas que regulan su actividad en el Reglamento de Auditoría Externa.

DISPOSICIONES FINALES Y TRANSITORIAS

Primera.- Autorizaciones especiales

En caso justificado, la empresa podrá solicitar a la Superintendencia, exoneración específica de alguno de los requerimientos normativos indicados en este Reglamento, adjuntando la documentación de sustento correspondiente respecto a alguno de los siguientes requisitos en lo que sea apropiado para la debida evaluación de esta Superintendencia:

- a) La empresa cuenta con un sistema de gestión que, tomado en su conjunto, cumple sustancialmente con los criterios mínimos indicados en la presente normativa.
- b) Cuando la organización recibe diversos servicios de su casa matriz, de la empresa que ejerce el control directo o indirecto, o de la que tenga responsabilidad directa de la operación, siempre que tomados en su conjunto igualen o excedan los criterios previstos en el Reglamento.
- c) Cuando por limitación legal, le resulta imposible cumplir con parte de la normativa.
- d) Cuando se requiera por fines de estandarización y lenguaje común con su casa matriz, o con la empresa que ejerza el control directo o indirecto o la que tenga responsabilidad directa de la operación, a fin de aprovechar ventajas metodológicas, como por ejemplo conocimiento y experiencia demostrada en diseño e implementación de gestión de riesgos acorde con buenas prácticas, infraestructura, y métodos y procedimientos que demuestren un claro conocimiento y gestión de los riesgos a los que están expuestos.

Las funciones del comité de auditoría podrán ser asumidas por la Casa Matriz, sólo si las actividades del conglomerado al que pertenezca una empresa supervisada no se desarrollen principalmente en el Perú y bajo autorización expresa de esta Superintendencia. Para ello las empresas deberán solicitar autorización indicando la forma en que se cumplirán las disposiciones establecidas en el presente Reglamento, obligación que permanece mientras se encuentre vigente la autorización.

Las Resoluciones de autorización correspondientes, serán publicadas en el Diario Oficial El Peruano.

Esta Superintendencia podrá suspender en cualquier momento las autorizaciones especiales concedidas a que hace referencia esta norma, cuando en el ejercicio de su función supervisora observe que las circunstancias lo ameritan, que la empresa ha incumplido con las obligaciones previstas, o que la autorización concedida no ha contribuido a una mejora de su práctica de gestión de riesgos, lo que comunicará a la empresa mediante oficio.

Segunda.- Transparencia

La empresa deberá revelar en su Memoria Anual, cuando menos una descripción general de las principales características de la Gestión Integral de Riesgos.

Tercera.- Plazo y Plan de Adecuación

En un plazo que no excederá de noventa (90) días calendario de haberse publicado el presente Reglamento, las empresas deberán remitir a esta Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico preliminar de la situación existente en la empresa, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Cuarta.- Declaración del Directorio

La primera declaración a que hace referencia el artículo 9° será exigible, por el ejercicio correspondiente al 2008, lo cual se encontrará a disposición de esta Superintendencia dentro de los 120 días calendario del 2009.

*Resolución S.B.S.
N° 2116 -2009*

*El Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones*

CONSIDERANDO:

Que, mediante la Resolución SBS N° 37-2008 del 10 de enero de 2008, se aprobó el Reglamento de la Gestión Integral de Riesgos, que establece que las empresas supervisadas deben contar con una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios;

Que, entre los riesgos que enfrentan las empresas supervisadas en el desarrollo de sus actividades se encuentra el riesgo operacional, el cual puede generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos;

Que, mediante la Resolución SBS N° 006-2002 del 4 de enero de 2002 y sus modificatorias, se aprobó el Reglamento para la Administración de los Riesgos de Operación;

Que, en consecuencia, resulta necesario realizar modificaciones al Reglamento para la administración de los riesgos de operación, a fin que dicha norma sea consistente con las disposiciones del Reglamento de la Gestión Integral de Riesgos, así como con los desarrollos recientes sobre la materia;

Que, asimismo, resulta conveniente ampliar el alcance de la regulación referida a la gestión del riesgo operacional a las Administradoras Privadas de Fondos de Pensiones;

Estando a lo opinado por las Superintendencias Adjuntas de Banca y Microfinanzas, Seguros, Administradoras Privadas de Fondos de Pensiones, Riesgos y Asesoría Jurídica; y,

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702 y sus modificatorias, y el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para la Gestión del Riesgo Operacional, que forma parte integrante de la presente Resolución.

Los anexos que forman parte del Reglamento aprobado por la presente Resolución se publican en el Portal institucional (<http://www.sbs.gob.pe>), conforme a lo dispuesto en el Decreto Supremo N° 001-2009-JUS.

Artículo Segundo.- Sustituir el artículo 117° del Título VI del Compendio de Normas de Superintendencia Reglamentarias del Sistema Privado de Administración de Fondos de Pensiones (SPP), por el texto siguiente:

“Artículo 117°.- Riesgo Operacional. Para administrar los riesgos operacionales asociados con el proceso de inversiones, las AFP se sujetarán a las disposiciones establecidas en el Reglamento para la Gestión del Riesgo Operacional.

Asimismo, como parte de las medidas para el tratamiento de este riesgo, las empresas deberán realizar lo siguiente:

- a. Implementar procedimientos para que las operaciones de inversión cuenten con confirmaciones, ya sean escritas o por medios auditivos o electrónicos, suscritas por los intermediarios;
- b. Implementar procedimientos para que las operaciones de inversión cumplan con las normas internas y externas aplicables y que las mismas se hayan realizado bajo condiciones de mercado, contando con los poderes y las firmas autorizadas;
- c. Implementar planes de contingencia ante fallas técnicas en los sistemas de información o ante la ocurrencia de eventos de fuerza mayor que puedan afectar la gestión de las inversiones;
- d. Establecer los procedimientos para el funcionamiento de sistemas de grabaciones de audio adecuados para la concertación de las operaciones de inversión, y el mantenimiento de dichas grabaciones por un mínimo de dos (2) años;
- e. Establecer procedimientos relacionados a la concertación, registro, liquidación, guarda física y custodia de las operaciones de inversión y al mantenimiento y control de expedientes;
- f. Establecer políticas y procedimientos que permitan una adecuada instrumentalización de convenios y contratos a fin de delimitar derechos y obligaciones contractuales tanto de las Carteras Administradas como de la AFP en aspectos vinculados con el proceso de inversión;
- g. Establecer adecuados canales de difusión entre sus funcionarios de las disposiciones legales y administrativas aplicables a sus operaciones de inversión;
- h. Evaluar y monitorear los efectos que habrán de producirse sobre los actos en materia de inversiones que realice la AFP, de conformidad con el régimen legal nacional o extranjero aplicable;
- i. Evaluar y monitorear las implicancias jurídicas en caso de incumplimiento en el pago de una inversión realizada por parte de un emisor o contraparte y la factibilidad de ejecución de las garantías;

- j. Establecer condiciones y requerimientos para el accionar diligente de los funcionarios en el proceso de inversión en resguardo de los recursos de las Carteras Administradas; y,
- k. Asegurar un adecuado cumplimiento de las políticas sobre la conducta ética y las políticas orientadas a evitar conflictos de interés u otras irregularidades en la gestión de las inversiones de los recursos de las Carteras Administradas.”

Artículo Tercero.- Incorpórese el procedimiento N° 122 “Autorizaciones especiales para la Gestión del Riesgo Operacional” y el procedimiento N° 123 “Autorización del Procesamiento Principal en el Exterior” en el Texto Único de Procedimientos Administrativos – TUPA de la Superintendencia de Banca, Seguros y AFP aprobado mediante Resolución SBS N° 131-2002, cuyos textos se anexan a la presente Resolución y se publican conforme lo dispuesto en el Decreto Supremo N° 004-2008-PCM, reglamento de la Ley N° 29091. (Portal institucional: www.sbs.gob.pe).

Artículo Cuarto.- La presente Resolución entra en vigencia a partir del día siguiente a su publicación en el Diario Oficial El Peruano, otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010, fecha a partir de la cual quedarán sin efecto la Resolución SBS N° 006-2002 y sus normas modificatorias, la Circular G-130-2007, así como todas aquellas disposiciones que se le opongan de manera total o parcial.

Las Administradoras Privadas de Fondos de Pensiones tendrán un plazo de adecuación al Reglamento aprobado por la presente Resolución hasta el 30 de junio de 2010.

Regístrese, comuníquese y publíquese,

FELIPE TAM FOX
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

REGLAMENTO PARA LA GESTIÓN DEL RIESGO OPERACIONAL

CAPITULO I DISPOSICIONES GENERALES

Artículo 1°.- Alcance

El presente Reglamento será de aplicación a las empresas señaladas en el artículo 16° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Las empresas de servicios complementarios y conexos señaladas en el artículo 17° de la Ley General se sujetarán, para la gestión de su riesgo operacional, a lo establecido en sus normas específicas. Asimismo, podrán tomar en consideración las disposiciones señaladas en el presente Reglamento en función a su tamaño y complejidad.

Artículo 2°.- Definiciones

Para los efectos de la presente norma deben considerarse los siguientes términos:

- a. **Apetito por el riesgo:** El nivel de riesgo que la empresa está dispuesta a asumir en su búsqueda de rentabilidad y valor.
- b. **Directorio:** Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente.
- c. **Evento:** Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
- d. **Evento de pérdida por riesgo operacional:** El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.
- e. **Información:** Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.
- f. **Proceso:** Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- g. **Reglamento de la Gestión Integral de Riesgos:** Reglamento de la Gestión Integral de Riesgos aprobado mediante la Resolución SBS N° 37-2008 del 10 de enero de 2008.
- h. **Riesgo legal:** Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros.
- i. **Subcontratación:** Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.
- j. **Superintendencia:** Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

- k. Tolerancia al riesgo: El nivel de variación que la empresa está dispuesta a asumir en caso de desviación de los objetivos empresariales trazados.

Artículo 3°.- Riesgo operacional

Entiéndase por riesgo operacional a la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

Las empresas deben realizar una gestión adecuada del riesgo operacional que enfrentan, para lo cual observarán los criterios mínimos indicados en el presente Reglamento.

Artículo 4° Factores que originan el riesgo operacional

i) Procesos internos

Las empresas deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

ii) Personal

Las empresas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros.

iii) Tecnología de información

Las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

iv) Eventos externos

Las empresas deberán gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

Artículo 5°.- Eventos de pérdida por riesgo operacional

Los eventos de pérdida por riesgo operacional pueden ser agrupados de la manera descrita a continuación:

- a. Fraude interno.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.

- b. Fraude externo.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.
- c. Relaciones laborales y seguridad en el puesto de trabajo.- Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.
- d. Clientes, productos y prácticas empresariales.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.
- e. Daños a activos materiales.- Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.
- f. Interrupción del negocio y fallos en los sistemas.- Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.
- g. Ejecución, entrega y gestión de procesos.- Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

En el Anexo N° 1, se incluye una categorización de los tipos de eventos de pérdida aplicable según el sector al que pertenece la empresa.

CAPITULO II ROLES Y RESPONSABILIDADES

Artículo 6°.- Responsabilidades del Directorio

El Directorio tiene las siguientes responsabilidades específicas respecto a la gestión del riesgo operacional:

- l) Definir la política general para la gestión del riesgo operacional.
- m) Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiados.
- n) Establecer un sistema de incentivos que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.
- o) Aprobar el manual de gestión del riesgo operacional.
- p) Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.
- q) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.

- r) Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión del riesgo operacional, y que los principales riesgos identificados se encuentran bajo control dentro de los límites que han establecido.

Artículo 7º.- Responsabilidades de la Gerencia

La gerencia general tiene la responsabilidad de implementar la gestión del riesgo operacional conforme a las disposiciones del Directorio.

Los gerentes de las unidades organizativas de negocios o de apoyo tienen la responsabilidad de gestionar el riesgo operacional en su ámbito de acción, dentro de las políticas, límites y procedimientos establecidos.

Artículo 8º.- Comité de riesgos

Las funciones del Comité de Riesgos señaladas en el Reglamento de la Gestión Integral de Riesgos, son de aplicación a la gestión del riesgo operacional en lo que corresponda.

Artículo 9º.- Unidad de riesgos

De conformidad con el Reglamento de la Gestión Integral de Riesgos, las empresas podrán contar con una Unidad de Riesgos centralizada o con unidades especializadas en la gestión de riesgos específicos.

En ese sentido, la Unidad de Riesgos de la empresa o, de ser el caso, la unidad especializada de gestión del riesgo operacional deberá cumplir con las siguientes funciones:

- a. Proponer políticas para la gestión del riesgo operacional.
- b. Participar en el diseño y permanente actualización del Manual de gestión del riesgo operacional.
- c. Desarrollar la metodología para la gestión del riesgo operacional.
- d. Apoyar y asistir a las demás unidades de la empresa para la aplicación de la metodología de gestión del riesgo operacional.
- e. Evaluación del riesgo operacional, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.
- f. Consolidación y desarrollo de reportes e informes sobre la gestión del riesgo operacional por proceso, o unidades de negocio y apoyo.
- g. Identificación de las necesidades de capacitación y difusión para una adecuada gestión del riesgo operacional.
- h. Otras necesarias para el desarrollo de la función.

Las empresas deberán asignar recursos suficientes para la gestión del riesgo operacional, que les permita un adecuado cumplimiento de las funciones señaladas en el presente artículo y asegurar una adecuada independencia entre el área que asuma las funciones de gestión del riesgo operacional señaladas en el presente artículo y aquellas otras unidades de negocio o de apoyo.

Los bancos, las financieras, las empresas de seguros y las AFP deberán contar con una función especializada en riesgo operacional. De acuerdo al tamaño y complejidad de las operaciones que realice la empresa, la Superintendencia podrá requerir la creación de una unidad especializada.

CAPITULO III

LA GESTIÓN DEL RIESGO OPERACIONAL

Artículo 10°.- Manual de gestión del riesgo operacional

Las empresas deberán contar con un manual de gestión del riesgo operacional, el cual deberá contemplar por lo menos los siguientes aspectos:

- a. Políticas para la gestión del riesgo operacional.
- b. Funciones y responsabilidades asociadas con la gestión del riesgo operacional del Directorio, la Gerencia General, el Comité de Riesgos, la Unidad de Riesgos (o la unidad especializada, si corresponde) y las unidades de negocio y de apoyo.
- c. Descripción de la metodología aplicada para la gestión del riesgo operacional.
- d. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición al riesgo operacional de la empresa y de cada unidad de negocio.
- e. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

Artículo 11°.- Metodología para la gestión del riesgo operacional

La metodología definida por la empresa para la gestión del riesgo operacional, cuando sea tomada en su conjunto, deberá considerar los componentes señalados en el artículo 4° del Reglamento de la Gestión Integral de Riesgos.

Asimismo, deberán cumplirse los siguientes criterios:

- a. La metodología debe ser implementada en toda la empresa en forma consistente.
- b. La empresa debe asignar recursos suficientes para aplicar su metodología en las principales líneas de negocio, y en los procesos de control y de apoyo.
- c. La aplicación de la metodología debe estar integrada a los procesos de gestión de riesgos de la empresa.
- d. Deben establecerse incentivos que permitan una mejora continua de la gestión del riesgo operacional.
- e. La aplicación de la metodología de gestión del riesgo operacional debe estar adecuadamente documentada.
- f. Deben establecerse procedimientos que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operacional.

Artículo 12°.- Base de datos de eventos de pérdida

Las empresas deberán contar con una base de datos de los eventos de pérdida por riesgo operacional.

Debe tenerse en cuenta que un evento puede tener como efecto una o más pérdidas, por lo cual las empresas deberán estar en capacidad de agrupar las pérdidas ocurridas por evento.

La base de datos deberá cumplir con los siguientes criterios:

- a. Deben registrarse los eventos de pérdida originados en toda la empresa, para lo cual se diseñarán políticas, procedimientos de captura, y entrenamiento al personal que interviene en el proceso.
- b. Debe registrarse, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas:
- Código de identificación del evento.
 - Tipo de evento de pérdida (según tipos de eventos señalados en el Anexo 1 del presente Reglamento).
 - Línea de negocio asociada, según líneas señaladas en el Anexo 2 del presente Reglamento para las empresas del sistema financiero, Anexo 3 para las empresas de seguros y Anexo 4 para las AFP. Deberán considerarse los niveles 1 y 2 de los cuadros señalados en los anexos. Estos cuadros podrán ser actualizados por la Superintendencia mediante Circular.
 - Descripción corta del evento.
 - Descripción larga del evento.
 - Fecha de ocurrencia o de inicio del evento.
 - Fecha de descubrimiento del evento.
 - Fecha de registro contable del evento.
 - Monto(s) bruto(s) de la(s) pérdida(s), moneda y tipo de cambio.
 - Monto(s) recuperado(s) mediante coberturas existentes de forma previa al evento, moneda, tipo de cambio y tipo de cobertura aplicada.
 - Monto total recuperado, moneda y tipo de cambio.
 - Cuenta(s) contable(s) asociadas.
 - Identificación si el evento está asociado con el riesgo de crédito (para empresas del sistema financiero) o con el riesgo de seguros (para empresas del sistema de seguros).

En el caso de eventos con pérdidas múltiples, las empresas podrán registrar la información mínima requerida por cada pérdida, y establecer una forma de agrupar dicha información por el evento que las originó.

De otro lado, podrá registrarse información parcial de un evento, en tanto se obtengan los demás datos requeridos. Por ejemplo, podrá registrarse primero el monto de la pérdida, para posteriormente añadir las recuperaciones asociadas.

- c. Deben definirse y documentarse criterios objetivos para asignar los eventos de pérdida a los tipos de evento señalados en el Anexo 1 del presente Reglamento, así como a las líneas de negocio señaladas en los Anexos 2, 3 y 4. Asimismo, deben definirse criterios específicos para aquellos casos en que un evento esté asociado a más de una línea de negocio.
- d. Debe definirse un monto mínimo de pérdida a partir del cual se registrará un evento en la base de datos. Al respecto, se fija un monto mínimo de 3 000 nuevos soles para los bancos, las financieras, las compañías de seguros y las AFP, y de 1 000 nuevos soles para el resto de empresas. Las empresas podrán establecer un monto mínimo inferior al

indicado, teniendo en cuenta su volumen de operaciones y complejidad asociada. La Superintendencia podrá actualizar el monto mínimo definido por medio de Circular.

- e. Debe definirse un monto mínimo de pérdida a partir del cual deberá contarse con un expediente físico o electrónico que contenga información adicional a la solicitada en el literal b. y que permita conocer el modo en que se produjo el evento, características especiales y otra información relevante, así como las acciones que hubiera tomado la empresa, incluyendo entre otras las mejoras o cambios requeridos en sus políticas o procedimientos. Dicho monto mínimo deberá ser aprobado por el Comité de Riesgos. La Superintendencia podrá establecer posteriormente un monto mínimo de carácter general.

Artículo 13°.- Gestión de la continuidad del negocio y de la seguridad de la información

Como parte de una adecuada gestión del riesgo operacional, las empresas deben implementar un sistema de gestión de la continuidad del negocio que tendrá como objetivo implementar respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Asimismo, las empresas deben contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

Para ello, las empresas deberán aplicar las disposiciones que se establezcan en las normas específicas sobre estos temas.

Artículo 14°.- Subcontratación

Con el fin de gestionar los riesgos operacionales asociados a la subcontratación, las empresas deberán establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados. Dichas políticas y procedimientos deberán considerar:

- a. El proceso de selección del proveedor del servicio
- b. La elaboración del acuerdo de subcontratación
- c. La gestión y monitoreo de los riesgos asociados con el acuerdo de subcontratación
- d. La implementación de un entorno de control efectivo
- e. Establecimiento de planes de continuidad

Los acuerdos de subcontratación deberán formalizarse mediante contratos firmados, los cuales deben incluir acuerdos de niveles de servicio, y definir claramente las responsabilidades del proveedor y de la empresa.

CAPITULO IV REQUERIMIENTOS DE INFORMACION

Artículo 15°.- Informe a la Superintendencia

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

El contenido mínimo del referido informe, así como los aspectos operativos del IG-ROp, relacionados con las instrucciones, responsables y demás aspectos necesarios para su adecuado funcionamiento, se establecen en el “Manual del IG-ROp”, el cual estará publicado en el “Portal del Supervisado” de la SBS. Asimismo, en el Portal, se publicarán instrucciones adicionales para el adecuado uso del sistema.

Las empresas supervisadas deberán designar un funcionario responsable por la información a ser reportada a través del IG-ROp, y tomarán las medidas necesarias para asegurar la veracidad de dicha información. El funcionario responsable deberá corresponder a cualquiera de las siguientes clasificaciones: Director, Gerente o Funcionario Principal, según las disposiciones de la Circular G-119-2004, referida a las normas para el registro de Directores, Gerentes y Principales Funcionarios – REDIR.

Artículo 16°.- Información adicional

La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión del riesgo operacional de la empresa.

Asimismo, la empresa deberá tener a disposición de la Superintendencia todos los documentos mencionados por el presente Reglamento, así como los informes de auditoría o revisiones realizadas por la casa matriz en caso de ser aplicable.

CAPITULO V COLABORADORES EXTERNOS

Artículo 17°.- Auditoría Interna

La Unidad de Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional, así como de lo dispuesto en el presente Reglamento, de conformidad con lo establecido en el Reglamento de Auditoría Interna.

Artículo 18°.- Auditoría Externa

Las sociedades de auditoría externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la gestión del riesgo operacional, considerando el cumplimiento de lo dispuesto en el presente Reglamento.

Artículo 19°.- Empresas Clasificadoras de Riesgo

Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la gestión del riesgo operacional en el proceso de clasificación de las empresas supervisadas.

DISPOSICIONES FINALES Y TRANSITORIAS

Primera.- Autorizaciones especiales

Las empresas podrán solicitar a la Superintendencia exoneración específica de alguno de los requerimientos normativos indicados en este Reglamento, adjuntando la documentación de sustento correspondiente, para lo cual serán de aplicación los requisitos señalados en la Primera Disposición Final y Transitoria del Reglamento de la Gestión Integral de Riesgos, en lo que sea aplicable a la gestión del riesgo operacional.

Segunda.- Régimen simplificado para las Edpymes

Las Edpymes no están obligadas a implementar la base de datos de eventos de pérdida requerida en el artículo 12° del presente Reglamento. No obstante, la Superintendencia podrá exigir la aplicación de dicho artículo a aquellas Edpymes que considere apropiadas, teniendo en consideración su tamaño, complejidad y volumen de operaciones.

Tercera.- Sanciones

En caso de incumplimiento de las disposiciones contenidas en el presente Reglamento la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Cuarta.- Transparencia

Como parte de la información que debe ser revelada en la Memoria Anual de las empresas, conforme a lo señalado en el Reglamento de la Gestión Integral de Riesgos, deben incluirse las características principales de la gestión del riesgo operacional implementada por la empresa.

Quinta.- Adecuación de las Administradoras Privadas de Fondos de Pensiones

En un plazo que no excederá de noventa (90) días calendario de haberse publicado el presente Reglamento, las AFP deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico de la situación existente en la AFP respecto al cumplimiento de cada uno de los artículos del presente Reglamento, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

ANEXO N° 1

TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Tipo de evento (Nivel 1)	Definición	Tipo de evento (Nivel 2)	Ejemplos
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicado, al menos, un miembro de la empresa.	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones (intencional).
		Robo y fraude	Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional).
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	Robo y fraude	Robo, falsificación.
		Seguridad de los sistemas	Daños por ataques informáticos, robo de información.
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad o discriminación.	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
		Higiene y seguridad en el trabajo	Casos relacionados con las normas de higiene y seguridad en el trabajo; indemnización a los trabajadores.
		Diversidad y discriminación	Todo tipo de discriminación.
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información (conocimiento del cliente, etc.), quebrantamiento de la privacidad de información sobre clientes minoristas, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial.
		Prácticas empresariales o de mercado improcedentes	Prácticas restrictivas de la competencia, prácticas comerciales / de mercado improcedentes, manipulación del mercado, abuso de información privilegiada (en favor de la empresa), lavado de dinero.
		Productos defectuosos	Defectos del producto (no autorizado, etc.), error de los modelos.
		Selección, patrocinio y riesgos	Ausencia de investigación a clientes conforme a las directrices, exceso de los límites de riesgo frente a clientes.

		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento.
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Desastres y otros acontecimientos	Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo).
Interrupción del negocio y fallos en los sistemas	Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas	Sistemas	Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo (p.ej. en el Delivery vs. Payment).
		Seguimiento y presentación de informes	Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas).
		Aceptación de clientes y documentación	Inexistencia de autorizaciones / rechazos de clientes, documentos jurídicos inexistentes / incompletos.
		Gestión de cuentas de clientes	Acceso no autorizado a cuentas, registros incorrectos de clientes (con generación de pérdidas), pérdida o daño de activos de clientes por negligencia.
		Contrapartes comerciales	Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes.
		Distribuidores y proveedores	Subcontratación, litigios con proveedores.

ANEXO N° 2

LINEAS DE NEGOCIO GENÉRICAS PARA EMPRESAS DEL SISTEMA FINANCIERO

Nivel 1	Nivel 2	Definición
Finanzas corporativas	Finanzas corporativas	Realización de operaciones de financiamiento estructurado y participación en procesos de titulización; underwriting; asesoramiento financiero a empresas corporativas, grandes y medianas empresas, así como al gobierno central y entidades del sector público; entre otras actividades de naturaleza similar.
	Finanzas de administraciones públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Operaciones de tesorería; compra y venta de títulos, monedas y commodities por cuenta propia; entre otras actividades de naturaleza similar.
	Creación de mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Financiamiento a clientes minoristas incluyendo tarjetas de crédito, préstamo automotriz, entre otros.
Banca comercial	Banca comercial	Financiamiento a clientes no minoristas, incluyendo: factoring, descuento, arrendamiento financiero, entre otros.
Liquidación y pagos	Clientes externos	Actividades relacionadas con pagos y cobranzas, transferencia interbancaria de fondos, compensación y liquidación, entre otras actividades de naturaleza similar.
Otros servicios	Custodia	Servicios de custodia, fideicomisos, comisiones de confianza y otros servicios.
	Encargos de confianza	
	Fideicomisos	
	Otros servicios	

ANEXO N° 3

LINEAS DE NEGOCIO GENÉRICAS PARA EMPRESAS DE SEGUROS

NIVEL 1	NIVEL 2	Definición
Ramos generales	Incendio y Domiciliario	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Incendios - Líneas Aliadas Incendio - Lucro Cesante - Cristales - Terremoto - Domiciliario
	Ramos Técnicos	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Todo riesgo para contratistas - Rotura de maquinaria - Lucro cesante de Rotura de maquinaria - Montaje contra todo riesgo - Todo riesgo equipo electrónico - Todo riesgo equipo para contratistas - Calderas
	Robo, Bancos y 3D	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Robo y asalto - Deshonestidad frente a la empresa - Comprensivo contra deshonestidad - Seguro de Bancos
	Responsabilidad civil	Se refiere a pólizas emitidas por responsabilidad civil
	Cascos, Transportes y Aviación	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Transportes - Marítimo – Cascos - Aviación
	Autos y SOAT	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Vehículos - Líneas aliadas vehículos - SOAT
	Accidentes personales	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Accidentes personales - Escolares
	Asistencia médica	Se refiere a pólizas emitidas por asistencia médica
	Otros	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Cauciones - Crédito Interno - Crédito a la exportación - Multiseguros - Agrícola - Misceláneos - Animales
Ramos de vida	Seguros de Vida en Grupo	Se refiere a las siguientes pólizas: - Seguro de Vida en Grupo Particular - Seguro de Vida para Trabajadores - Seguro de Desgravamen - Seguro de Vida Individual de Corto Plazo

		- Sepelio de Corto Plazo
	Seguros de Vida Individual y Rentas	Se refiere a las siguientes pólizas: - Seguro de Vida Individual de Largo Plazo - Sepelio de Largo Plazo - Seguro de Vida para ex - Trabajadores - Renta Particular - Pensiones del Seguro Complementario de Trabajo de Riesgo - Renta de Jubilación - Pensión de Invalidez - Pensión de Supervivencia - Pensión de Invalidez-Régimen Temporal - Pensión de Supervivencia-Régimen Temporal
	Seguros Previsionales y SCTR	Se refiere a las siguientes pólizas: - Seguro Complementario de Trabajo de Riesgo - Invalidez - Supervivencia - Gastos de Sepelio
Finanzas corporativas	Finanzas corporativas	Deuda subordinada, emitir acciones, ofertas públicas iniciales y colocaciones en mercado secundario, fideicomiso
Negociación y ventas	Negociación y ventas	Renta fija, renta variable, divisas, posiciones propias en valores, operaciones con pacto de recompra.
Créditos	Créditos	Fianzas, créditos hipotecarios para trabajadores.

ANEXO N° 4

LINEAS DE NEGOCIO GENÉRICAS PARA AFP

Nivel 1	Nivel 2	Definición
Administración de fondos	Administración de aportes obligatorios	En la forma establecida en la Ley del SPP
	Administración de aportes voluntarios	En la forma establecida en la Ley del SPP