UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA INFORMÁTICA

"DESARROLLO, IMPLEMENTACIÓN Y MANTENIMIENTO DE UN SISTEMA DE GESTIÓN DEL RIESGO OPERACIONAL EN EMPRESAS DEL SECTOR FINANCIERO"

INFORME TÉCNICO POR EXPERIENCIA PROFESIONAL CALIFICADA PARA OPTAR EL TÍTULO DE: INGENIERO INFORMÁTICO

PRESENTADO POR BACHILLER: CÉSAR EDUARDO HEEREN CRUZ

LIMA – PERU

AÑO 2013

EDICATORIA *A*

mis padres, motor, confianza inquebrantable e inspiración constante, A mi esposa, mi fuerza continua **,** *A mi hermana, ejemplo a seguir.*

AGRADECIMIENTOS

A mis estimados profesores de la facultad, al Profesor Javier Añaños, al Jurado calificador y en especial al Doctor Hugo Vega que hizo posible la organización y apoyo constante para la realización de este informe.

ÍNDICE

INTRODUCCIÓN

Comencemos preguntando sobre algo que está presente en cada actividad de nuestra vida, incluso cuando dormimos o no estamos conscientes de nuestros actos: El Riesgo. ¿Qué es el Riesgo? Lo primero que se nos viene a la mente es la "incertidumbre" de que algo va pasar y nos pueda afectar. En efecto, el riesgo definido a manera general es una acción que tiene la **posibilidad** de **impactarnos,** no dejándonos lograr uno a más objetivos determinados.

Hay muchas clases de riesgo, como los siguientes: riesgo de crédito, riesgo de mercado, riesgo reputacional, riesgo de liquidez, riesgo legal, riesgo estratégico y ***riesgo operacional***. En el sector financiero estos son los riesgos en los que se tiene especial cuidado, priorizando el establecer un sistema de gestión adecuado para controlarlos a un nivel aceptable para la organización, porque ese es el objetivo de un sistema de gestión del riesgo: Controlar el Riesgo. El riesgo es inherente en todas las actividades de cualquier tipo de empresa, el nivel de riesgo nunca es cero, pero si se gestiona, puede llegar a tener un nivel en el cual la organización pueda convivir con él.

Según la Resolución N° 2116-2008 de la Superintendencia de Banca, Seguros y AFP, organismo encargado de la Regulación y Supervisión del Sistema Financiero, de Seguros y del Sistema Privado de Pensiones, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo, el riesgo operacional es la posibilidad de pérdidas que surge por fallas en los procesos, la tecnología o el personal debidos a eventos internos o externos.

Imaginemos que tuviéramos la posibilidad de estar preparados ante eventos de caída de los sistemas de una empresa, poder estimar cuánta pérdida económica podríamos tener ante un evento de fraude interno en un data center, tener la certeza de que un proceso mal diseñado nos está generando pérdida o dejar de ganar dinero en el negocio, tener desarrollado un plan que nos permita seguir ofreciendo nuestros servicios transaccionales ante un desastre natural, todo ello son acciones relacionadas con una adecuada gestión del riesgo operacional. Tener un sistema de gestión adecuado nos dará como resultados principales: perder menos dinero en la empresa y generar mayor rentabilidad. ¿Qué empresa no quiere esos dos grandes resultados?

A continuación, en el informe se describe la experiencia laboral desempeñado en los últimos 3 años desarrollando, implementando y manteniendo el Sistema de Gestión de Riesgo Operacional en la siguiente empresa:

VisaNet Perú S.A.C, la única del país encargada de prestar servicios relacionados con operaciones a través de tarjetas VISA y la más importante en administración de operaciones con tarjetas en el país.

En el informe técnico, se hablará de manera general cómo se ha aplicado una metodología para gestionar el riesgo como solución a una problemática, de ella se tiene lecciones aprendidas y consejos para cada una de las 7 fases de la metodología. Dado que los riesgos específicos son propios y confidenciales de cada empresa no se podrá poner una lista de riesgos de este centro laboral más solo mencionar la metodología para propósitos educativos.

Es importante señalar, que a través de los cursos, proyectos informáticos y experiencias expuestas por nuestros profesores en la Carrera de Ingeniería Informática, puedo dar fe que, cada uno de los cursos relacionados en especial a la gestión de los sistemas de información, metodologías de gestión administrativa, gestión de proyectos, manejo de infraestructura tecnológicas fueron fundamentales para el desarrollo profesional, laboral y personal del autor de este informe.

CAPÍTULO 1 : ALCANCE

En el presente informe se describen las fases principales de la gestión de riesgo operacional en las empresas del sector financiero. Se describe a manera de experiencia personal cómo aplicarlas en cada fase de la metodología. Se detalla la solución a implementar en la empresa descrita siguiendo una metodología que cumpla con los requisitos mínimos esperados para una buena gestión siguiendo las mejores prácticas de la industria.

CAPÍTULO 2 : CONCEPTOS GENERALES

A continuación se describen algunos términos y abreviaturas que se utilizan en el presente informe para una mejor comprensión.

Basilea II

Estándar internacional que sirve de referencia a los reguladores bancarios, con el objetivo de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos. En ella de se describen 3 pilares que deben ser aplicados por todas las empresas peruanas reguladas por la SBS.

Pilar I: el cálculo de los requisitos mínimos de capital. Capital necesario para afrontar posible materialización de riesgos en las entidades.

Pilar II: el proceso de supervisión de la gestión de los fondos propios. Los supervisores deben evaluar el cumplimiento de la suficiencia de capital.

Pilar III: la disciplina de mercado. Establecimiento de normas de transparencia y la publicación periódica de información acerca de su exposición a los diferentes riesgos y la suficiencia de sus fondos propios

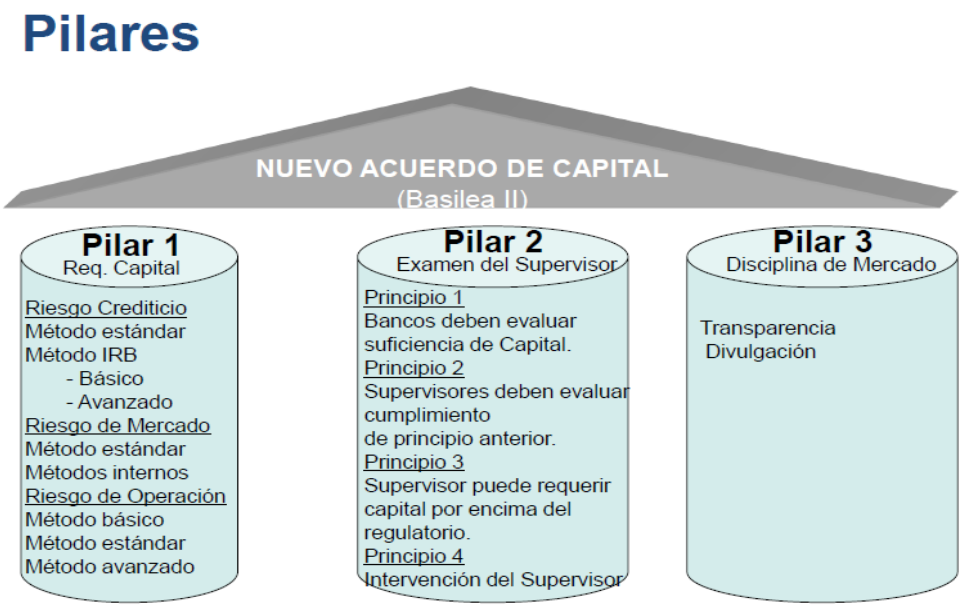


Gráfico 1: Pilares de Basilea II

Gestión del Riesgo

Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular. Existen varias metodologías para gestionar el riesgo sin embargo todas manejan la misma relación a grandes rasgos: percibir, valorar y manejar el riesgo.

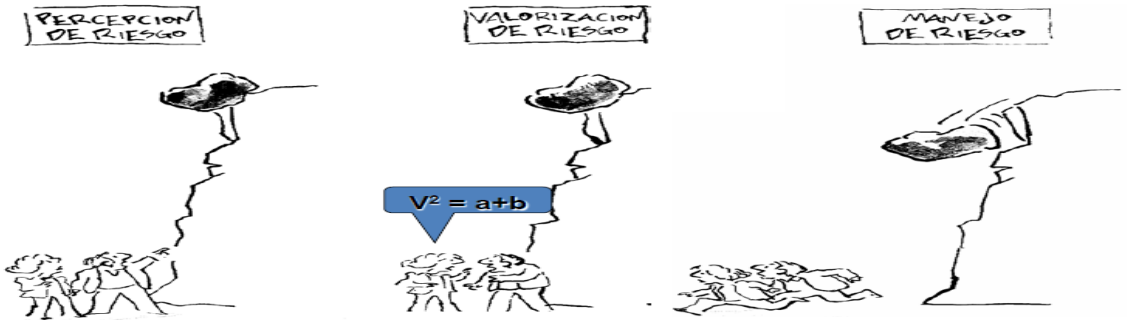


Gráfico 2: Ejemplo de gestión de riesgos

Riesgo Operacional

Según Basilea II, el Riesgo Operacional es la posibilidad de pérdida económica por fallas en los procesos, personas, tecnología de la información y eventos externos. Incluye el riesgo legal pero excluye el riesgo reputacional y estratégico. El riesgo operacional se materializa mediante Eventos de riesgo operacional.

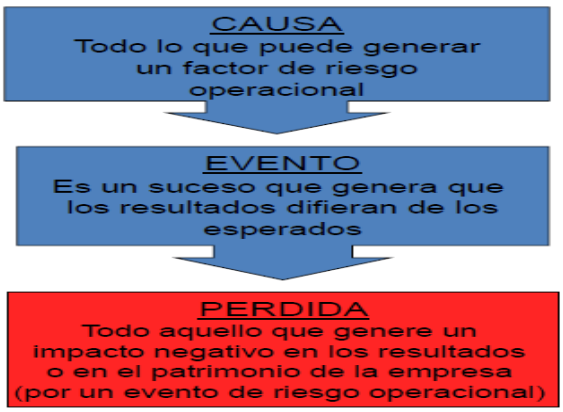


Gráfico3: Evento de Riesgo

Para ello, Basilea II clasifica los eventos de riesgo operacional en 7 tipos:

Fraude Interno: son eventos de 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.

Fraude Externo: son eventos de pérdida 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.

Relaciones laborales y seguridad en el puesto de trabajo: son eventos de pérdidas derivados 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.

Clientes, productos y prácticas empresariales: son eventos de 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.

Daños a los activos materiales: son eventos de pérdida derivados de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

Interrupción del negocio y fallos en los sistemas: Son eventos de pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

Ejecución, entrega y gestión de procesos: Son eventos de pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

Sistema de Gestión del Riesgo Operacional (SGRO)

Es un conjunto de lineamientos que controlan el riesgo a un nivel aceptado por la organización; se plasman en una metodología y esta puede estar basada en las mejores prácticas de la industria financiera, tales como el Estándar Australiano/Neozelandés de Administración de Riesgos – AS/NZS-4360, COSO ERM, el acuerdo de Basilea II o las Resoluciones/Circulares sobre Riesgo Operacional emitidas por la Superintendencia de Banca y Seguros - SBS.

Las fases de la metodología son:

Fase I Establecer el contexto: definición de los diferentes criterios y lineamientos para la gestión del riesgo operacional.

Fase II Identificar Riesgos Operacionales: identificar los Riesgos Operacionales mediante los canales: talleres, encuestas y autoevaluaciones. **Fase III Analizar Riesgos Operacionales:** determinar la frecuencia e impacto de los riesgos ya identificados mediante una escala de criterios cualitativos y cuantitativos.

Fase IV Evaluar Riesgos Operacionales: determinar el nivel de riesgo en una matriz la cual nos dará a conocer si debemos o no aceptar el riesgo. **Fase V Tratar Riesgos Operacionales:** implementar planes de mitigación a los riesgos no tolerables, eligiendo las opciones para tratarlos, así como realizar la evaluación de dichas opciones.

Fase VI Monitorear y Revisar Riesgos: Resumen de las acciones tomadas en forma oportuna con el objetivo de aprovechar adecuadamente la toma de decisiones.

Fase VII Comunicar y Consultar Riesgos Operacionales: implementar indicadores adecuados para alertarnos de la posibilidad de incremento del nivel de riesgo de los procesos.

El gráfico 4 muestra un diagrama de cómo funciona la metodología. El detalle de las fases de la metodología se presenta en el Capitulo 8. Aplicación de la Metodología (Ver pág. 34)

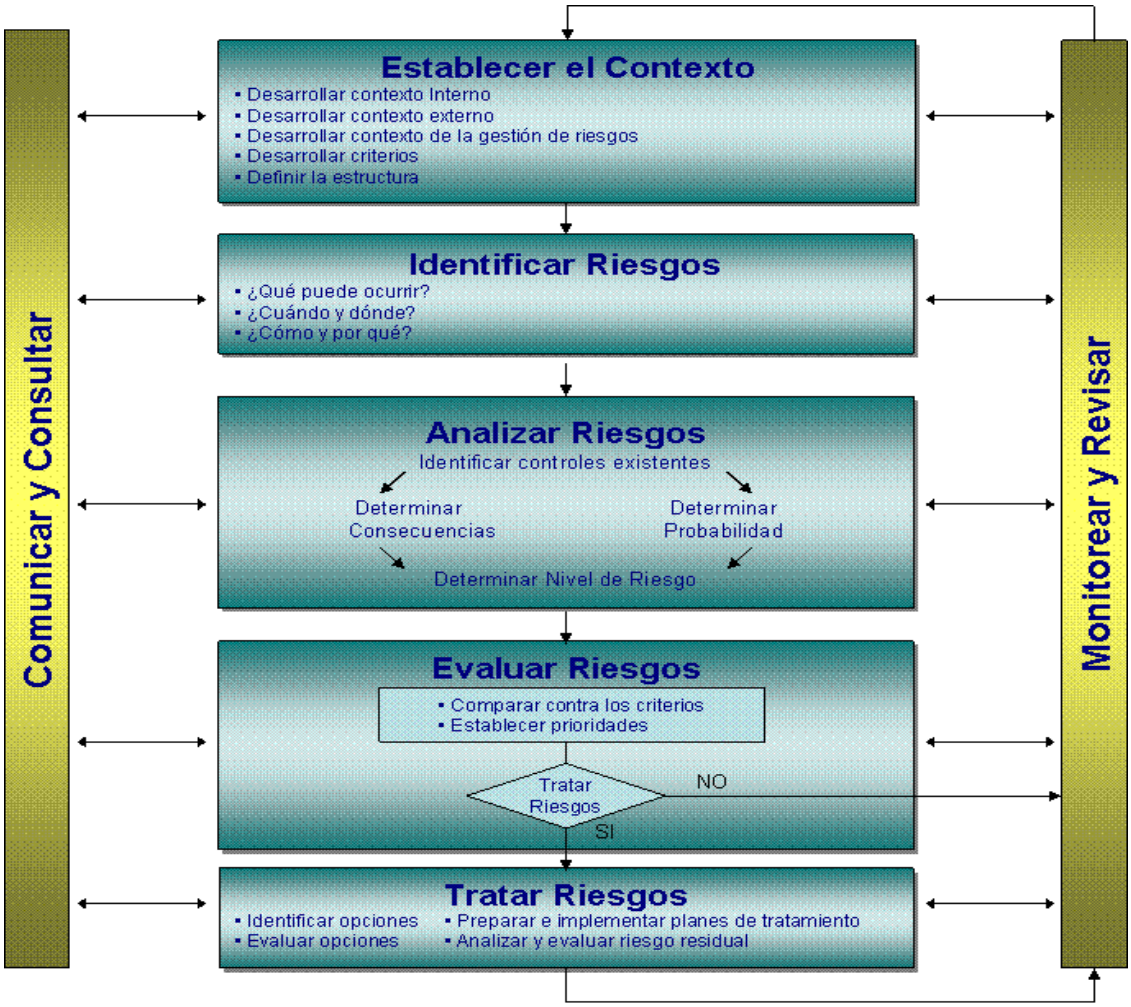


Gráfico 4: Metodología Riesgo Operacional

Dos de los componentes del Riesgo operacional más importantes son: la Continuidad del negocio y la Seguridad de la Información.

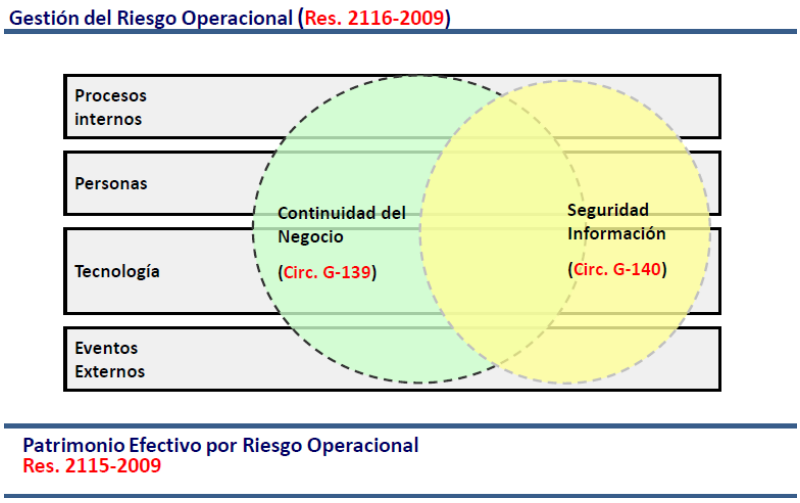


Gráfico 5: Componentes del Riesgo Operacional

Seguridad de la Información

Se entiende por **seguridad de la información** a todas aquellas medidas que permitan resguardar y proteger la información buscando mantener la *confidencialidad*, la *disponibilidad* e *Integridad* de la misma.

Confidencialidad: es la propiedad de prevenir la divulgación de información a personas o sistemas autorizados. Algunas preguntas que se harían para definirlo serian: Cuan confidente se mantiene la data en mis sistemas de información. ¿Está controlado el acceso a la información crucial?, ¿saben mis empleados la importancia de la seguridad y de la información que se maneja? Estas son algunas de las cosas que nos tenemos que preguntar cuando hablamos de la confidencialidad.

Integridad: es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Algunas preguntas que se harían para definirlo serian: ¿Cuán confiable es el medio por donde viaja mi información? , ¿Nadie la esta interceptando?, ¿Está llegando la información íntegra al destino?

Disponibilidad: característica cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Algunas preguntas que se harían para definirlo:

¿La data está data disponible cuando la necesita?, ¿está disponible en todas las partes que se necesita que esté?, ¿la están visualizando las personas adecuadas?

Gráfico 6: Triángulo CID

Sistema de Gestión de Seguridad de la Información (SGSI)

Es un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001(estándar para la seguridad de la información).

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

Al igual que un SGRO (Sistema de gestión de Riesgo Operacional), se implementa mediante una metodología, la cual se basa en el ciclo de Deming (PDCA).

La ISO/IEC 27001 por lo tanto incorpora el típico "Plan-Do-Check-Act" (PDCA) que significa "Planificar-Hacer-Controlar-Actuar" siendo este un enfoque de mejora continua:

Plan (planificar): es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

Do (hacer): es una fase que envuelve la implantación y operación de los controles.

Check (verificar): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

Act (actuar): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento

Gráfico 7: Metodología para Implantación SGSI según ISO/IEC 27001

Para mayor detalle ver el **Anexo 1** que es la resolución emitida por la SBS que da los lineamientos como gestionar la seguridad de la información.

PCI DSS (Payment Card Industry Data Security Standard)

Es un Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago. Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago débito y crédito.

Las compañías que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o arriesgan la pérdida de sus permisos para procesar las tarjetas de crédito y débito (Pérdida de franquicias), enfrentar auditorías rigurosas o pagos de multas. Los Comerciantes y proveedores de servicios de tarjetas de crédito y débito, deben validar su cumplimiento al estándar en forma periódica.

Esta validación es realizada por auditores autorizados Qualified Security Assessor (QSAs). Sólo a las compañías que procesan menos de 80,000 transacciones por año se les permite realizar un auto evaluación utilizando un cuestionario provisto por el Consorcio del PCI (PCI SSC).

La versión actual de la norma (2.0) especifica 12 requisitos para el cumplimiento, organizados en 6 secciones relacionadas lógicamente, que son llamadas "objetivos de control."

Los objetivos de control y sus requisitos son los siguientes:

Desarrollar y Mantener una Red Segura

Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.

Requisito 2: No usar contraseñas del sistema y otros parámetros de seguridad predeterminados provistos por los proveedores.

Proteger los Datos de los propietarios de tarjetas.

Requisito 3: Proteger los datos almacenados de los propietarios de tarjetas.

Requisito 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.

Mantener un Programa de Manejo de Vulnerabilidad

Requisito 5: Usar y actualizar regularmente un software antivirus.

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar Medidas sólidas de control de acceso

Requisito 7: Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.

Requisito 8: Asignar una Identificación única a cada persona que tenga acceso a un computador.

Requisito 9: Restringir el acceso físico a los datos de los propietarios de tarjetas.

Monitorear y Probar regularmente las redes

Requisito 10: Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.

Requisito 11: Probar regularmente los sistemas y procesos de seguridad.

Mantener una Política de Seguridad de la Información

Requisito 12: Mantener una política que contemple la seguridad de la información

Estos requisitos dan como un total de 492 controles, 19 no son aplicados para VisaNet.

Gestión de la Continuidad del Negocio (BCM = Business Continuity Management)

Es la capacidad estratégica y táctica de una organización que le permite responder ante incidentes e interrupciones de negocio a fin de continuar con el desarrollo de sus operaciones bajo niveles aceptables de funcionamiento previamente establecidos. Una adecuada gestión de la continuidad del negocio se convierte en una herramienta clave para minimizar los efectos adversos producidos por la materialización de riesgos operacionales que pueden conllevar a la interrupción de los procesos del negocio.

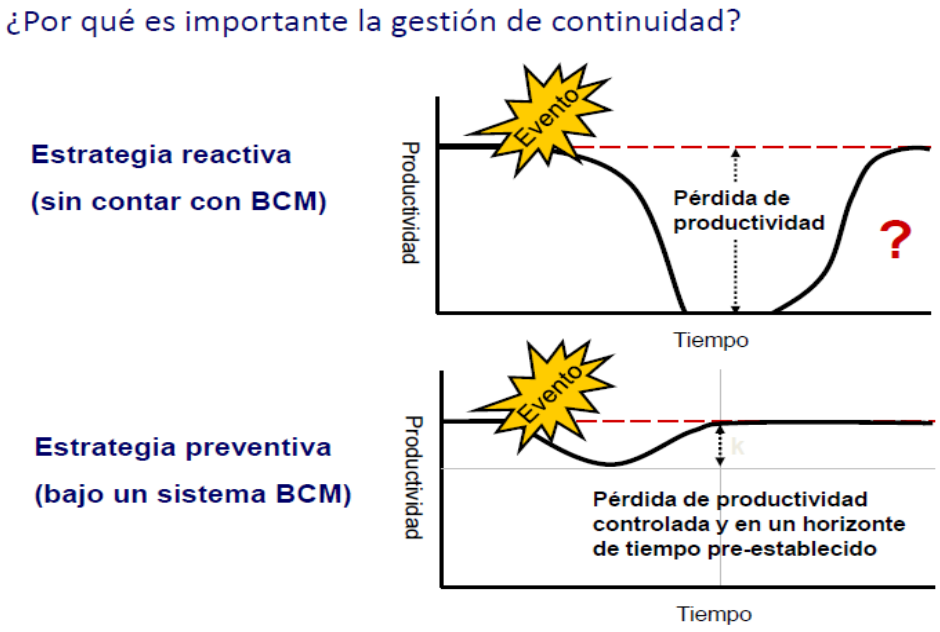


Gráfico 8: Importancia del BCM

Sistema de Gestión de Continuidad del Negocio

Conjunto de lineamientos que ayudan a mantener a un negocio dentro de los niveles aceptables durante y después de un evento que puede parar parcial o totalmente sus operaciones. Este sistema contiene varios documentos específicos que deben ser actualizados permanentemente ante cambios significativos. El estándar usado para gestionar adecuadamente un Sistema de Gestión de Continuidad del negocio es el BS-25999. Este consta de cinco etapas:

Entendimiento de la Organización: Esta etapa consiste en conocer los objetivos y metas de la empresa; identificar los principales procesos, productos, servicios y proveedores, así como las actividades y recursos requeridos; evaluar los riesgos que podrían causar una interrupción de dichas actividades, y el impacto que podría tener dicha interrupción.

Las actividades mínimas a desarrollar durante esta fase son las siguientes:

Análisis de impacto: Consiste en determinar el impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios de la empresa. Para ello, deben considerarse aspectos como: daños a la viabilidad financiera de la empresa, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. Según ello, debe establecerse el período máximo tolerable de interrupción por cada uno de estos procesos. El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados. Se identifican 2 valores importantes en esta etapa como el RTO y RPO. El RTO (Recovery Time Objetive) es el tiempo en que se espera recuperar la infraestructura después de un desastre y el RPO (Recovery Point Objetive).

Evaluación de riesgos: Consiste en identificar y evaluar los riesgos que podrían causar una interrupción del negocio. Para ello, deberá seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos que enfrenta la empresa.

La empresa debe definir qué procesos requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos.

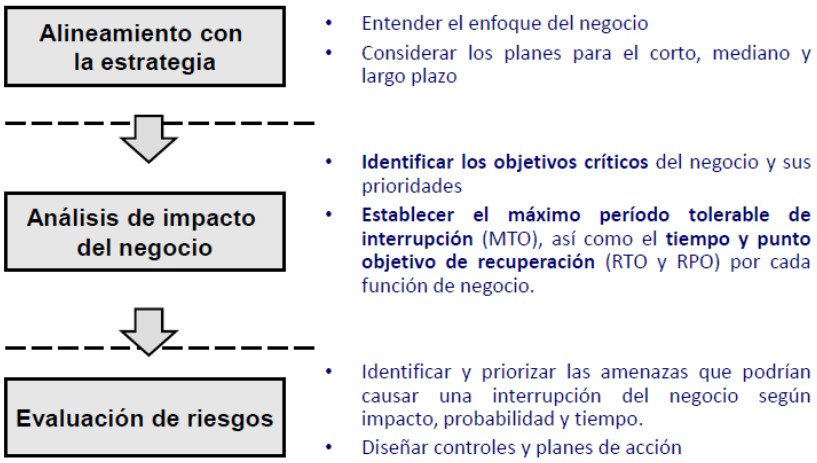


Grafico 9: Entendimiento de la Organización

Gráfico 10: RPO vs RTO

Selección de la estrategia de continuidad: determinar las estrategias de continuidad que permitan mantener las actividades y procesos de negocio luego de ocurrida una contingencia. En ella se selecciona los métodos alternos de operación a ser utilizados luego de una interrupción, según las prioridades establecidas en el análisis de impacto de negocios. Se debe asegurar como mínimo mantener la continuidad de los procesos que soportan los principales productos y servicios de la empresa, dentro del tiempo objetivo de recuperación, definido para cada proceso. Las estrategias de continuidad deben tomar en cuenta los siguientes aspectos, según sea aplicable para cada proceso:

Seguridad del personal.

Habilidades y conocimientos asociados al proceso.

Instalaciones alternas de trabajo.

Infraestructura alterna de tecnología de información que soporte el proceso.

Seguridad de la Información.

Equipamiento necesario para el proceso.

Desarrollo e implementación de la capacidad de la respuesta: En esta etapa, se deben desarrollar los planes de respuesta ante los eventos analizados en las fases previas, e implementar un modelo de respuesta flexible y escalable que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con la estrategia seleccionada, para enfrentar con éxito un evento de interrupción de operaciones. Se deben desarrollar los siguientes planes como mínimo:

Plan de gestión de crisis: Tiene como objetivo dotar a la empresa de la capacidad de mantener, o de ser el caso recuperar, los principales procesos de negocio dentro de los parámetros previamente establecidos.

Plan de Emergencia: Plan que tiene como objetivo salvaguardar la integridad física del personal

Plan de recuperación de desastres: Plan que busca inicialmente restaurar los servicios de tecnología de información dentro de los parámetros establecidos, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.

Pruebas, mantenimiento y auditoria: Los planes de continuidad del negocio deberán ser probados cuando menos una vez al año. A continuación se detallan las mínimas actividades que debería tener esta fase:

Ejecución de pruebas: El alcance de las pruebas debe ser consistente con el alcance de los planes de continuidad del negocio. Cada prueba debe tener objetivos definidos y un reporte que resuma los resultados alcanzados y recomendaciones

Actualización de planes: Las empresas deben definir políticas y procedimientos para la actualización de los planes de gestión de la continuidad

del negocio, de tal manera que cualquier cambio que impacte a la empresa (ya sea interno o externo) sea revisado en relación con la continuidad del negocio.

Acoplar la gestión de la continuidad del negocio dentro de la cultura organizacional: las actividades mínimas de esta etapa son:

Evaluación de grado de conocimiento sobre la gestión de la continuidad.

Desarrollo y mejora de la cultura de continuidad.

Monitoreo permanente.

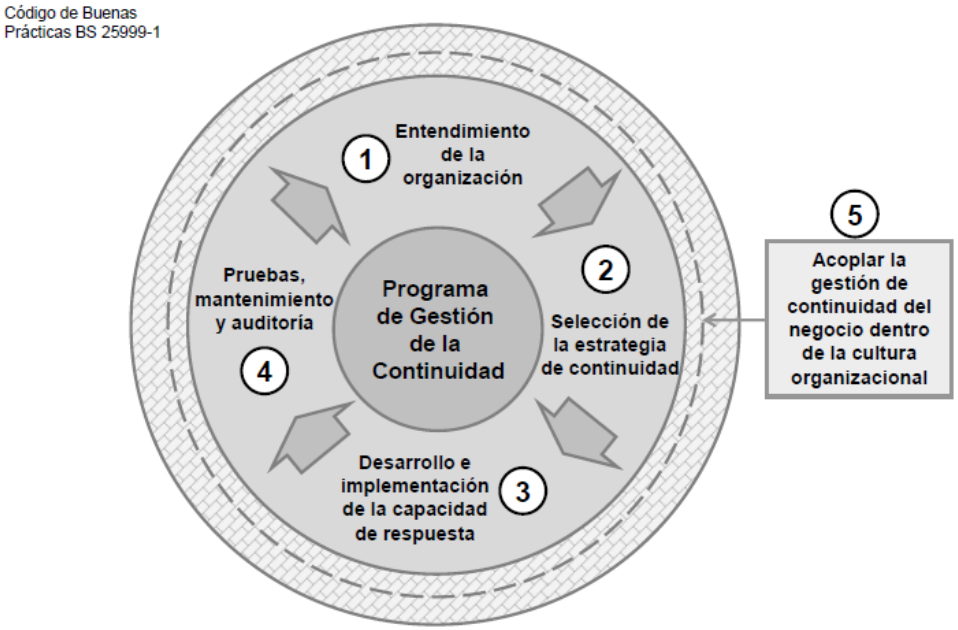


Gráfico 11: Sistema de Gestión de Continuidad del Negocio

Para mayor detalle ver el **Anexo 2** que es la resolución emitida por la SBS que da los lineamientos como gestionar la continuidad del negocio.

CAPÍTULO 3 : POLITICAS DE RIESGO OPERACIONAL

Las políticas de Riesgo Operacional son los lineamientos generales que se esperan en toda gestión. Para cada política se espera uno o más planes de acción para implementar en la empresa, desde la creación de nuevos puestos de trabajo, hasta la compra de herramientas informáticas para automatizar toda la gestión. A continuación se recomendará algunas políticas que se debe tener una empresa como mínimo para realizar adecuadamente su gestión:

Se deberá establecer una instancia directiva de rango gerencial para dirigir el programa de riesgos Operacional. El compromiso de la alta dirección es fundamental para que el programa de gestión de riesgos operacionales funcione. Sin el apoyo del Directorio y de la Gerencia General de la empresa, el programa no tendría el sponsor necesario para calar en todos los procesos de la empresa. Adicionalmente del apoyo en aprobación de documentación y el económico.

Establecer dentro del organigrama un área independiente para la gestión del riesgo operacional. Se deberá crear un área independiente para la gestión del riesgo dado que depender de un área tales como planeamiento, finanzas o sistemas podría generar conflicto de intereses. Es por ello que se recomienda establecer el área de riesgo operacional en una Gerencia de Riesgos que depende de un Comité de Riesgos o de la Gerencia General.

Capacitación y concientización a todo el personal. Se debe capacitar a todo el personal desde que ingresa a la empresa y durante la ejecución de sus funciones periódicamente. Esto es necesario debido a que es el personal de todas las áreas quienes se comportan como socios de la gestión al reportar eventos, implementar planes de acción, ejecutar controles preventivos y correctivos.

Basarse en mejores prácticas de la industria. No se debe inventar la rueda, en el mercado abundan las resoluciones y circulares de la SBS, metodologías

de distintos países para gestionar el riesgo hasta certificaciones. Se recomienda basarse en lo que la banca está obligado a realizar por sus entes reguladores.

Definir una metodología. Sin mapa no hay X, sin X no hay tesoro. Una de las partes más importantes de la gestión es definir una metodología Cualitativa / Semicuantitativa / Cuantitativa que permita dar a conocer a todo el personal cómo se debe gestionar el riesgo operacional. Se debería actualizar como mínimo una vez al año.

El alcance es TODO. La gestión del riesgo operacional solo tiene un alcance y es toda la empresa. No debería abarcar unos cuantos procesos que se entienden como críticos si no todos los procesos debido a que el riesgo está en toda actividad inherente de la empresa. Una materialización de un riesgo podría afectar a toda la organización es por ello que se recomienda no poner filtros si no ver todos los procesos.

Todo cambio denota riesgo. El temor al cambio está relacionado a la incertidumbre de qué podría ocasionar un posible cambio, generalmente como naturaleza humana es el hecho de pensar que lo negativo está a la vuelta de la esquina. Es por ello, que se recomienda que para cambios en procesos, tecnologías, procedimientos, servicios de terceros relevantes se debería realizar una evaluación de riesgos para conocer qué planes se podría implementar para estar preparados ante un posible impacto negativo en la operativa del negocio.

7 x 24 x 365 - Seguros. Una adecuada gestión de la continuidad del negocio y la seguridad de la información son socios estratégicos para la adecuada gestión del riesgo operacional. Asegurar una continuidad de operaciones luego de algún desastre es necesario para minimizar perdidas en la empresa. Adicionalmente asegurar la información mediante la confidencialidad, integridad y disponibilidad permite llevar las operaciones críticas del negocio de una manera óptima.

Todo se reporta, nada se calla. El reporte de eventos de riesgos por parte del personal es pilar fundamental de la gestión. Sin el reporte oportuno del personal no se podría identificar planes de acción futuros que permitan reducir la materialización de eventos, así que todos mea culpa de errores para poder generar mejoras en la empresa, todos somos humanos, todo sistema falla, todo proceso no es perfecto.

CAPÍTULO 4 : ROLES Y RESPONSABILIDADES DE RIESGO OPERACIONAL

La empresa deberá detallar e implementar una estructura adecuada para la adecuada gestión del riesgo operacional. Es por ello que toda la empresa deberá tener un rol. A continuación detallaré los roles y responsabilidades que se debe tener como mínimo en una empresa:

Directorio

Responsabilidad general:

Definir los objetivos estratégicos base para la definición de los objetivos operacionales

Responsabilidades específicas:

Brindar lineamientos generales y prioridades para la Gestión del Riesgo Operacional.

Revisar periódicamente el status de la Gestión del Riesgo Operacional.

Aprobar las políticas, normas, procedimientos y otros documentos relacionados con la Gestión del Riesgo Operacional, según le corresponda de acuerdo a los niveles de aprobación establecidos en la Compañía.

Asegurar que los gerentes integrantes gestionan los riesgos operacionales dentro de su ámbito de acción.

Evaluar y aprobar la designación de los Dueños de Procesos.

Evaluar y aprobar la definición de los objetivos operacionales realizada por los Dueños de Procesos.

Evaluar y aprobar las escalas de medición del riesgo propuestas por el Área de Riesgo Operacional.

Evaluar y aprobar los límites de aceptación y rechazo de los riesgos operacionales.

Evaluar y aprobar el marco metodológico de la Gestión del Riesgo Operacional.

Tratar casos especiales de la Gestión del Riesgo Operacional, que no puedan resolverse en el Comité de Riesgo.

Aprobar los casos o circunstancias especiales que aceptan ciertos riesgos, siempre que la relación costo-beneficio sea favorable a la Compañía.

Comité de Riesgo

Responsabilidad general:

Ejercer la máxima instancia de coordinación y aprobación de estrategias, metodologías, lineamientos, herramientas, recursos, roles y responsabilidades, relacionados con la Gestión del Riesgo Operacional.

Responsabilidades específicas:

Brindar lineamientos generales y prioridades para la Gestión del Riesgo Operacional.

Garantizar que la Compañía tenga políticas, normas y procedimientos documentados para la Gestión del Riesgo Operacional.

Garantizar la asignación de los recursos necesarios para la eficiente Gestión del Riesgo Operacional.

Revisar periódicamente las políticas, normas y procedimientos relacionados con la Gestión del Riesgo Operacional, promoviendo sus modificaciones y/o actualizaciones, según corresponda.

Revisar y aprobar técnicamente las metodologías y lineamientos relacionados con la Gestión del Riesgo Operacional.

Revisar, aprobar y efectuar el seguimiento de los planes de trabajo.

Tratar casos especiales de la Gestión del Riesgo Operacional, que no puedan resolverse entre los participantes que implementan los lineamientos establecidos para dicha gestión.

Analizar los reportes de riesgo emitidos por el Área de Riesgo Operacional, y proponer acciones al respecto.

Revisar y aprobar los Planes de Mitigación.

Solicitar el análisis y evaluación del riesgo operacional de procesos específicos, considerando determinados productos o proyectos nuevos para la Compañía.

Área de Riesgo Operacional

Responsabilidad general:

Gestionar los riesgos operacionales de acuerdo con los lineamientos establecidos por la Compañía.

Facilitar o asesorar a los Dueños de Controles, Dueños de Procesos, Comité de Riesgo y Comité de Gestión para gestionar de manera apropiada los riesgos operacionales de la Compañía.

Responsabilidades específicas:

Desarrollar las políticas, normas y procedimientos relacionados con la Gestión del Riesgo Operacional

Desarrollar el marco metodológico que regirá la Gestión del Riesgo Operacional en la Compañía.

Proponer escalas de medición de los riesgos y los niveles de riesgo aceptable por la Compañía.

Proponer roles y responsabilidades relacionados con la Gestión del Riesgo Operacional.

Proponer la utilización de herramientas y las mejores prácticas de la industria, para la Gestión del Riesgo Operacional.

Apoyar a las demás unidades de la empresa en el proceso de implementación de los lineamientos relacionados con la Gestión del Riesgo Operacional.

Elaborar conjuntamente con los Dueños de Procesos el plan de mitigación sobre los riesgos identificados, considerando aspectos de costo-beneficio y temas de factibilidad técnica-operativa.

Monitorear el proceso de la Gestión del Riesgo Operacional e informar de sus resultados al Comité de Riesgo.

Reportar al Comité de Riesgo, Dueños de Procesos o Directorio, según corresponda, las exposiciones, avances, niveles de riesgo de los procesos y resultados relacionados con las distintas fases de la Gestión del Riesgo Operacional.

Mantener y administrar la Base de Datos de Eventos de Pérdida y asegurar su permanente actualización.

Coordinar las necesidades de capacitación y difusión para una eficiente Gestión del Riesgo Operacional.

Dueños de Procesos

Responsabilidad general:

Asegurar que sus procesos se encuentran en un nivel de riesgo aceptable por la compañía.

Responsabilidades específicas:

Definir los objetivos operacionales de sus respectivos procesos.

Asegurar que se mantiene actualizada la documentación que describen los procesos, promoviendo y participando activamente en su elaboración y actualización.

Participar conjuntamente con el Área de Riesgo Operacional en la implementación de los lineamientos relacionados con la Gestión del Riesgo Operacional.

Aprobar e implementar los planes de mitigación de los riesgos operacionales de sus respectivos procesos, gestionando los recursos necesarios para dicha implementación.

Reportar al Área de Riesgo Operativo las incidencias, nuevos eventos o cualquier situación que afecte la evaluación de los riesgos operacionales.

Definir indicadores KRI (Indicadores Claves de Riesgo) de los procesos asignados.

Elaborar los reportes de KRI definidos para los procesos asignados, e informar periódicamente al Área de Riesgo Operacional.

Establecer un procedimiento adecuado de delegación de facultades y de segregación de funciones dentro del ámbito de sus procesos.

Evaluación del riesgo operacional, de forma previa al lanzamiento de nuevos productos, subcontrataciones significativas y ante cambios importantes en el ambiente operativo o informático.

Dueños de Controles

Responsabilidades específicas:

Participar en la definición de los controles relacionados con sus funciones.

Ejecutar y/o administrar los controles definidos en los planes de mitigación y aquellos relacionados con sus funciones.

Mantener registros o evidencia que sustenten la aplicación de sus actividades de control.

Reportar al Área de Riesgo Operacional las incidencias y/o eventos acordes con sus actividades de control.

Auditoría

Responsabilidades específicas:

Auditar el cumplimiento de las políticas, normas, procedimientos y responsabilidades relacionadas con la Gestión del Riesgo Operacional en la Compañía.

Auditar el cumplimiento de los planes de mitigación aprobados por la Compañía.

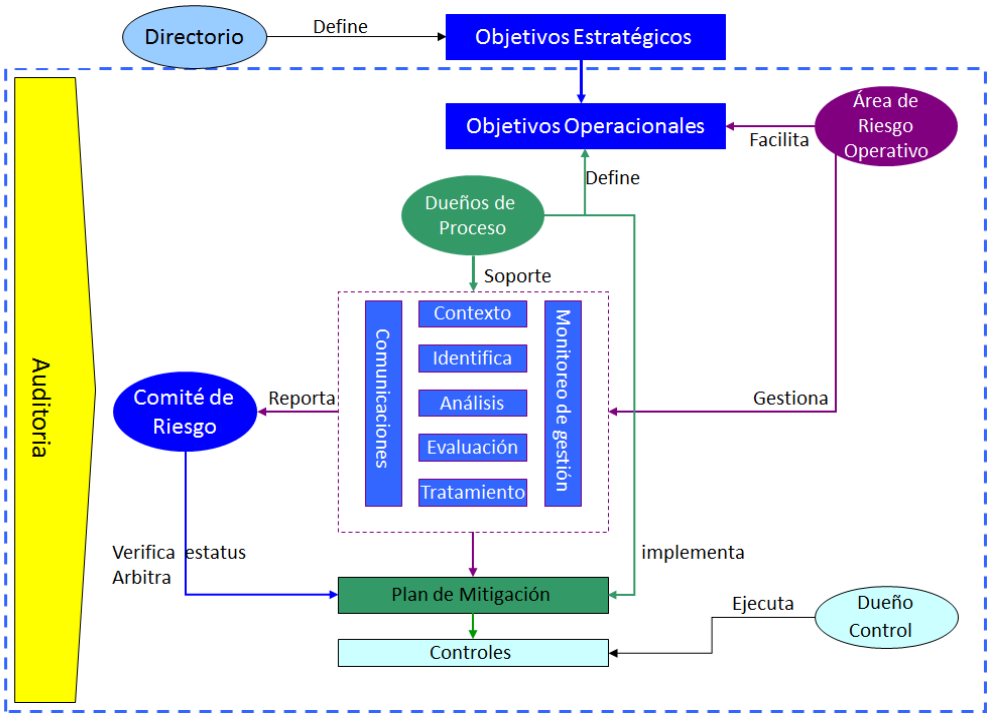


Gráfico 12: Esquema de Roles y Responsabilidades

CAPÍTULO 5 : ORGANIZACION

5.1 Breve reseña de la organización

En 1997, la Compañía Peruana de Medios de Pago S.A.C (VisaNet Perú) se crea con el objetivo de ser una empresa orientada a prestar servicios relacionados con operaciones a través de tarjetas Visa. Estos servicios permiten a los establecimientos comerciales el cobro de productos y servicios a través de medios de pago de la marca Visa.

Para ello VisaNet Perú ofrece la instalación y mantenimiento de terminales electrónicos, el procesamiento de datos y transacciones, que se refieran al servicio de afiliación de establecimientos comerciales, y el servicio de comercio electrónico.

5.2 Clientes

Sus clientes son más de 60, 000 comercios desde grandes empresas en sector retail (Saga, Ripley entre otros) hasta los comercios más pequeños de todas las provincias del país.

5.3 Organización

Gráfico 13: Puestos clave en organigrama

5.4 Procesos

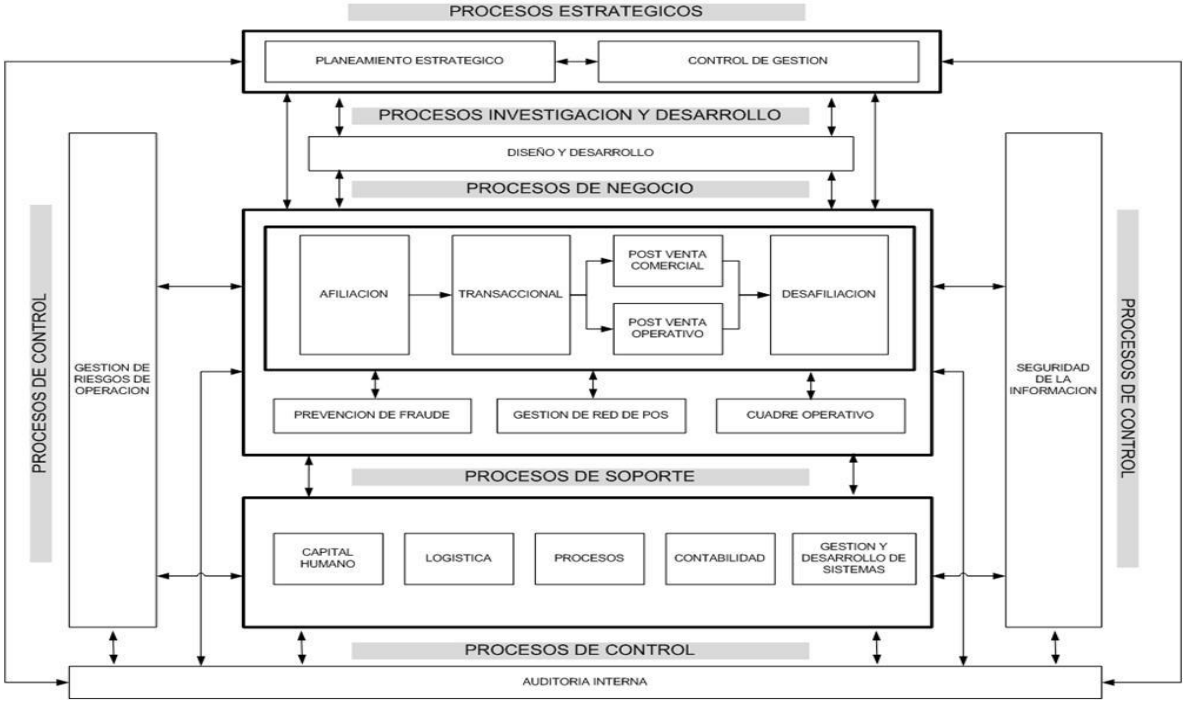


Gráfico 14: Macro procesos de la empresa

5.5 Misión y Visión

Misión

La misión de VisaNet del Perú es ofrecer los mejores canales de atención para sus clientes (tarjetahabientes), a través de una adecuada red de Comercios y Empresas afiliadas logrando que ambos, clientes y establecimientos prefieran utilizar las tarjetas o medios de pago de la marca VISA en vez del dinero en efectivo. La compañía desarrollará sus negocios en el Perú, pero apoyará a los empresarios peruanos que quieran ofrecer sus productos y servicios al exterior con canales adecuados para hacerlo.

El compromiso de la compañía se extiende para con sus empleados, proveedores y comunidad, buscando que estas relaciones les permitan crear valor.

Además la compañía ofrecerá servicios de procesamiento y respaldo operativo a terceros, para conservar servicios de gran calidad con menores costos para los accionistas.

La compañía estará a la búsqueda de la más alta tecnología disponible, para seleccionar la más adecuada y mantenerse a la vanguardia en el país y en la misma línea tecnológica que Visa Internacional.

Visión

La Compañía será la mejor y más grande empresa de servicios relacionados con tarjetas de crédito y otros medios de pago, contando con una infraestructura moderna y eficiente, incentivando la utilización de los medios de pago de la marca VISA con una activa gestión Comercial. La Compañía también ofrecerá servicios técnicos y operativos a otras marcas de medios de pago, reduciendo así los costos de mantenerse con los más altos niveles de tecnología y eficiencia.

Desde su papel de miembro de Grupo Adquiriente en el Perú, la compañía se identificará con el nombre comercial de "Visanet del Perú" y orientará sus esfuerzos para que el consumo privado de los peruanos se canalice con el uso de tarjetas u otro medios de pago electrónicos, desplazando al dinero en efectivo; asimismo apoyará a sus accionistas en la creación de nuevos usuarios, desarrollando productos seguros y accesibles para disminuir el flujo de efectivo y evitar la informalidad en la economía.

5.6 Productos

Servicio básico: Servicio con POS regular con distintas tecnologías como la IP, Telefónica.

Pos Delivery: Pos con tecnología inalámbrica celular.

MOTO: Sistema de autorización de pagos mediante teléfono o correo.

Cargos recurrentes: Afiliación de comercios con cargos con periodicidad frecuente automática.

Comercio Electrónico: Autorización de transacciones por plataforma web.

5.7 Mundo VISA

Grafico 15: Mundo Visa y sus participantes

CAPÍTULO 6 : DIAGNOSTICO

6.1 Problemática

La empresa como cualquier otra, manejaba sus riesgos e incidentes aisladamente, sin que se tenga un responsable de hacer seguimiento y validar que riesgos eran los más críticos en la empresa. Se tenía la política de planificar mejoras pero si había errores se recurría al “apaga incendios” como una empresa proactiva en minimizar el impacto de lo que ocurría. Los errores en cualquier empresa se materializan en pérdidas monetarias directas que son reflejadas en la contabilidad de la misma así como el lucro cesante por dejar de operar cierta cantidad de tiempo, hacía denotar un dejar de ganar dinero que se podía estimar perdiendo rentabilidad y valor por riesgos no identificados en su momento. Esto es un problema de las mayorías de empresas que no manejan sus riesgos.

A medida del crecimiento exponencial de sus clientes así como de sus transacciones se decidió realizar una consultoría del estado actual del control interno de la misma. En esta consultoría se identificó algunas brechas que se podrían mejorar en cuestión a organigrama y procesos recurrentes para el control oportuno de la materialización del riesgo. En las recomendaciones realizadas en el informe se especificó la creación de un área de riesgo operacional que se encargue principalmente de:

Identificar los riesgos críticos del negocio.

Evaluar su frecuencia y posible impacto en la empresa.

Definir e identificar controles para mantener el riesgo a un nivel aceptable para la organización.

Ser Project manager de todos los planes de acción de la empresa que son creados para mitigar riesgos críticos del negocio.

Administrar una base de datos con todos los eventos que han generado pérdidas al negocio para definir mediante estadísticas posibles planes de acción futuro.

Definir un tablero de control de indicadores para alertas tempranas de riesgos de nivel moderado.

Velar por la adecuada implementación de la gestión de seguridad de la información y continuidad del negocio de la empresa.

CAPÍTULO 7 : IMPLEMENTACION DE LA SOLUCION

7.1 Equipo

Dado las circunstancias del momento, la empresa decidió en contratar al autor de este informe para la implementación del Sistema de Gestión del Riesgo Operacional en coordinación directa con toda la empresa, desde practicantes hasta directores. El reporte directo era al Jefe de Procesos y Riesgo Operacional.

Gráfico 16: Participación de la empresa en la implementación

La solución se implementó mediante la definición de lineamientos generales así como la implementación de una metodología robusta que fomente la participación de toda la empresa con roles debidamente definidos.

CAPÍTULO 8 : APLICACIÓN DE LA METODOLOGIA

A continuación, detallaremos la metodología de 7 fases, presentada en el capítulo 2.1 y grafico 4 (páginas 13 y 14).

La aplicación de la misma se ha realizado en forma cíclica, una vez iniciada la aplicación de cada fase y terminado las 7, se vuelve a realizar el ciclo con una periodicidad mínima de 1 vez al año. A continuación se detallará las actividades principales de cada fase:

8.1 Establecer el contexto

En esta fase se deberá dejar por sentado toda la base e información necesaria para implementar la metodología como objetivo principal. Para ello se deberá tener los siguientes puntos:

Lineamientos generales

Misión: Brindar los lineamientos y procedimientos necesarios para gestionar la administración del riesgo operacional a través de la asistencia a todas las áreas de la organización asegurando la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de dichos riesgos, con la finalidad de mantener los riesgos operacionales en un nivel aceptable por la organización para que no afecten el logro de los objetivos

Identificación de objetivos operacionales y estratégicos: Son los objetivos de mayor nivel en la empresa fin de establecer una correcta relación entre el Establecimiento del Contexto con el resto de las etapas del modelo, se deben identificar los objetivos operacionales a nivel de procesos.

Sin embargo, cabe precisar la diferencia conceptual entre un objetivo estratégico y un objetivo operacional, tal como se indica en el siguiente recuadro:

Tipo de Objetivos	Definición
Estratégicos	Corresponde a los objetivos definidos y/o aprobados por el Directorio de la compañía y que guardan relación con los planes de mediano y largo plazo de la organización, y se expresan, por ejemplo, en metas de participación de mercado, volúmenes de venta, posicionamiento de marca, cobertura geográfica, etc.
Operacionales	Corresponde a los objetivos de los procesos, que se realizan en las distintas áreas de la empresa. Estos objetivos deben ser medibles, estar definidos por su dueño respectivo y estar aprobados. Asimismo, no lograr dichos objetivos representa un riesgo importante para el proceso.

Cuadro 1: Objetivos estratégicos y operacionales

Para identificar los objetivos operacionales se deben tener en cuenta por lo menos algunos de estos criterios:

Mediante los Objetivos Estratégicos: cada objetivo estratégico deberá relacionarse con uno o más objetivos operacionales de uno o más procesos de la empresa. En este caso, es conveniente identificar los objetivos operacionales mediante talleres o relevamientos específicos.

Mediante los Dueños de los Procesos y/o participantes del proceso: debido a su experiencia y conocimiento del proceso, definirán los objetivos operacionales pudiendo requerir el apoyo del área de riesgos operacionales.

Mediante los Riesgos Corporativos: En este caso, los objetivos operacionales se deberían identificar desde la perspectiva del riesgo corporativo, es decir, con

la finalidad de evitar o minimizar aquellos eventos de riesgo propios del negocio de la empresa.

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos operacionales, para cada proceso, y son establecidos por el Comité de Riesgos. La tolerancia debe ser expresada en alguna unidad de medición.

Definición de las categorías de riesgos/tipos de eventos: Los eventos/riesgos se pueden agrupar de acuerdo con su naturaleza en las siguientes categorías:

Fraude Interno

Fraude Externo

Prácticas laborales y seguridad del ambiente de trabajo.

Prácticas relacionadas con clientes, los productos y el negocio.

Daños a los activos físicos.

Interrupción del negocio por fallas en la tecnología de información.

Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores externos.

Niveles de Riesgo Operacional: Los niveles de riesgo operacional son los criterios los cuales se mide el riesgo. Se tiene 2 aspectos para obtener los niveles de riesgo:

Impacto: Es el aspecto en el cual se detalla los posibles impactos que podría generar la materialización del riesgo. En el mundo del riesgo operacional el impacto económico es el necesario sin embargo se pueden agregar otros tipos de impacto que ayuden a entender mejor las consecuencia de un riesgo. A continuación doy un ejemplo de cómo se podría estructurar una matriz de impacto de cinco niveles:

N°	Criterios	IMPACTO
5	Muy Alto	- Causarán daño económico>= S/.80,001 - Casos severos de incumplimiento reglamentario, que podría ocasionar la pérdida de la licencia. - Pérdida de información crítica de la Compañía o de terceros que no se pueda recuperar; lo cual conlleve a la interrupción de la continuidad del negocio.
4	Alto	- Causarán daño económico >= S/.60,001 y < S/.80,000 - Casos de incumplimiento de exigencias reglamentarias que decantan en el pago de penalidades graves. - No disponibilidad oportuna de la información crítica, lo cual conlleve a la interrupción de procesos clave.
3	Moderado	- Causarán daño económico >= S/.40,001 y < S/.60,000 - Casos de incumplimiento de exigencias reglamentarias que decantan en el pago de penalidades leves. - No disponibilidad oportuna de la información crítica, pero que no conlleva a la interrupción de procesos clave.
2	Bajo	- Causarán daño económico >= S/.20,001 y < S/.40,000 - Se presentan casos no severos, o aislados, de incumplimiento del reglamento operativo causando sólo amonestaciones - No disponibilidad oportuna de información que no afecta la continuidad del negocio.
1	Muy bajo	- Causarán daño económico < S/ 20, 000 - No se presentan incumplimientos de exigencias legales o reglamentarias. - Casos aislados de no disponibilidad oportuna de información.

Cuadro 2: Matriz de Impacto

Cabe resaltar que todos los datos de la matriz son ficticios y generales, cada empresa deberá identificar cuáles son sus niveles.

Frecuencia: Es el aspecto orientado a definir la probabilidad de ocurrencia de un riesgo con valores cualitativos o cuantitativos. Para ello es necesario definir el alcance de la frecuencia. Generalmente se utiliza como alcance un año y dentro de ese año se hace las divisiones respectiva de tres a cinco niveles como mínimo. A continuación doy un ejemplo de cómo se podría distribuir la frecuencia:

N°	Criterios	FRECUENCIA
5	**Muy Alto**	Recurrente. Evento relacionado a una transacción que sucede una, varias veces al día o que ocurra en el siguiente rango: (>52 al año)
4	**Alto**	Frecuente. Evento relacionado a una transacción con frecuencia semanal o que ocurra en el siguiente rango: (>24 y <=52 al año)
3	**Moderado**	Probable. Evento relacionado a una transacción u operación por lo menos mensual, quincenal o que ocurra en el siguiente rango: (>4 y <=24 al año)
2	**Bajo**	Ocasional. Evento relacionado a una transacción u operación por lo menos semestral, trimestral o que ocurra en el siguiente rango: (>1 y <=4 al año)
1	**Muy bajo**	Posible. Evento excepcional que se presenta cada uno o dos años.

Cuadro 3: Matriz de Frecuencia

Matriz de Riesgo: Es el resultado de la multiplicación entre el impacto y la frecuencia. Es la matriz más importante de la gestión en la cual se podrá visualizar cuales son los riesgos más críticos de la empresa y en los cuales se deberá tener mayor prioridad la implementación de planes. Se puede gestionar a nivel empresa o a nivel proceso.

Impacto						
	Muy Alto	Moderado	Alto	Muy Alto	Muy Alto	Muy Alto
	Alto	Bajo	Moderado	Alto	Muy Alto	Muy Alto
	Moderado	Bajo	Moderado	Alto	Alto	Muy Alto
	Bajo	Muy Bajo	Bajo	Moderado	Moderado	Alto
	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo	Moderado
		Muy Bajo	Bajo	Moderado	Alto	Muy Alto
		Frecuencia				

Cuadro 4: Matriz de Riesgo

8.2 Identificar el riesgo operacional

En esta fase se deberá explicar cuáles son las técnicas, preguntas o alcance de que debemos tener en cuenta en esta fase, una de las más importantes debido

a que en ella deberemos tratar de identificar todos los riesgos que podrían impactar en el negocio:

Lineamientos generales

Criterios: Se tendrá como criterio básico de identificación de eventos de riesgo operacional, el aporte de los colaboradores especialmente de los que participan en la supervisión, diseño y/o ejecución de los respectivos procesos; a través de la ejecución de cualquiera de las siguientes técnicas:

Talleres,

Reuniones,

Autoevaluaciones,

Encuestas,

Checklists,

Lluvia de ideas,

Recorrido de los procesos validando sus respectivos documentos, entre otros.

Se deben identificar riesgos para cada proceso, en los cuales los facilitadores (área de riesgo operacional) podrán realizar las siguientes preguntas secuencialmente, con el objetivo de relevar posibles eventos de riesgo:

¿qué puede fallar?,

¿en qué parte del proceso?,

¿en qué momento del periodo de ejecución del proceso?,

¿cómo sucedería? y

¿cuáles serían las causas principales para que suceda?

La identificación de riesgos operacionales se realizará a través del uso de las técnicas mencionadas con anterioridad, que serán elegidas dependiendo del criterio y juicio experto del facilitador (área de Riesgo Operacional) con el soporte de los dueños de los procesos. Es recomendable que las personas que participen de los talleres tengan el soporte documental con información confiable (Ej. informes gerenciales y de auditoría, hallazgos de las empresas de seguridad y control, planes, matriz FODA, regulaciones y normatividad, encuestas, listas de chequeo, datos estadísticos, registros de incidentes, etc.) y deberán tener conocimiento apropiado del proceso o parte del mismo.

Para realizar una adecuada identificación de riesgos operacionales el área de Riesgo Operacional deberá ejecutar, por lo menos las siguientes actividades principales:

Entendimiento de los procesos y sus principales componentes.-

Se tiene que lograr un conocimiento del proceso a evaluar, identificando como mínimo los siguientes aspectos:

Objetivos del proceso.

Diagrama de Bloque.

Entradas y Salidas.

Comienzo y fin del proceso (alcance).

Sistemas de Información que soportan el proceso.

Recursos Humanos involucrados en el proceso.

Documentación relacionada.

Controles actuales del proceso.

Con el objetivo de tener un marco de referencia general para entender el proceso en análisis, y realizar una adecuada identificación de los riesgos, se recomienda buscar las faltas o fallas en los aspectos listados en la parte superior, que den como resultado que el proceso no se desarrolle como fue definido.

Entendimiento de los objetivos y sus métricas.-

Es necesario conocer también los factores críticos de éxito y sus Indicadores de desempeño (KPI) con el objetivo de saber cómo estas fallas pueden afectar al proceso.

Reunir Información necesaria.-

Con la participación de los dueños de procesos, o las personas designadas por éstos, se podrán aplicar diversas técnicas para identificar y documentar todos los riesgos de cada proceso como:

Entrevistas con los dueños del proceso al momento del levantamiento y documentación. Obtención de otras opiniones (Jefes, Sub-Gerentes y Gerentes), si se estima conveniente, para validar y complementar las entrevistas anteriores. Obtención de documentación adicional y complementaria (trabajos de las áreas y departamentos relacionados con la identificación de Riesgos e Informes de Auditoría Interna o Externa). Dentro de las fuentes de información disponibles en La compañía, se podrá utilizar:

Datos Contables sobre pérdidas.

Informes de desempeño de sistemas.

Estadísticas de interrupciones, eventos de pérdida entre otros.

Datos del área de Help Desk.

Información de seguridad

Campos mínimos para la identificación:

Código: correlativo de un riesgo identificado.

Evento de Riesgo: suceso el cual tiene la posibilidad que ocurra e impacte negativamente el logro de objetivos operacionales.

Causa del riesgo: circunstancia que desencadena el origen del riesgo. Esta circunstancia es ocasionada por los factores de riesgo operacional.

Tipificación Basilea II / Tipo de eventos de Pérdida de Riesgo Operacional (Nivel 1): Clasificación referente al tipo de riesgo que genera pérdidas por riesgo operacional según las buenas prácticas de Basilea II.

Tipificación Basilea II / Tipo de eventos de Pérdida de Riesgo Operacional (Nivel 2): Sub Clasificación referente al tipo de riesgo que genera pérdidas por riesgo operacional según las buenas prácticas de Basilea II.

Factor que origina el Riesgo Operacional: son acciones que originan el riesgo operacional como: personas, procesos, tecnologías de la información y eventos externos.

Control actual: Es la actividad que se realiza actualmente con el objetivo de minimizar el riesgo.

Aplicación de riesgos informáticos/tecnológicos;

Debido a que el nivel de riesgos tecnológicos demanda la necesidad de tener conocimientos específicos de arquitecturas, tecnologías, topologías de TI se necesita aplicar un enfoque distinto para identificarlos. Se recomienda realizar los siguientes pasos:

Identificar un inventario de activos de información que comprendan una lista de hardware y software de toda la empresa.

Se deberá calificar y clasificar cada activo de información identificado. La calificación está relacionada a una pérdida o falla en un determinado activo de la información que afecte la confidencialidad, integridad o disponibilidad de la información así como los propietarios de la misma. La clasificación del activo generalmente se estipula como: confidencial, pública y privada.

Se identifican las vulnerabilidades y las amenazas que explotan esas vulnerabilidades. Se pone un peso para cada amenaza así como la probabilidad de ocurrencia, esta multiplicación da como resultado el cálculo del riesgo.

Se pondera el mayor valor de la multiplicación, en ella se dará prioridad a los valores mayores para implementar planes de acción relacionados con el activo.

Se ha descrito los pasos de manera muy general debido a que la gestión de la seguridad de la información es todo un mundo dentro de la gestión de riesgo operacional. Siempre se recomienda manejar los talleres de riesgos y seguridad en distintas reuniones porque puede llegar a confundir al dueño del proceso. Sin embargo, es algo obligatorio tener las evidencias respectivas que se sigue en las metodologías para cada aplicación.

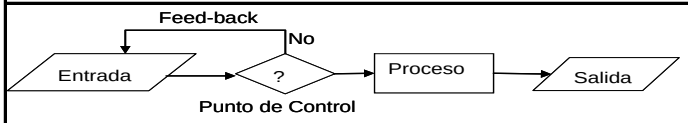
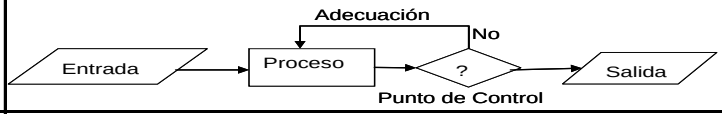
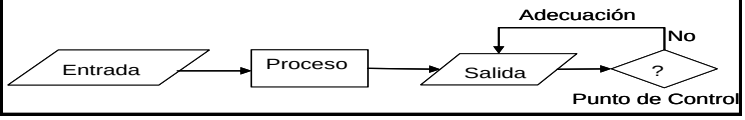
8.3 Análisis del Riesgo Operacional

En esta Fase se deberá explicar cuáles son las actividades necesarias para calificar el riesgo de acuerdo a su impacto y frecuencia con ayuda de la matriz de impacto y frecuencia definidas en la fase Establecer el Contexto.

Lineamientos generales

Determinación del riesgo inherente: Riesgo natural de los procesos que enfrenta una entidad, sin considerar controles para modificar su impacto y frecuencia. Existen controles que se consideran como naturales y forman parte del elemento bajo análisis, por ejemplo, las puertas de oficinas y el mobiliario normal deben considerarse como parte de las protecciones de un documento ubicado al interior de la oficina al establecer su nivel de riesgo inherente. Por el contrario, si el documento se ubica dentro de una caja fuerte, la caja en sí es claramente un control especial que no ha de considerarse para definir el riesgo inherente. Con esta analogía Se deberá elegir del cuadro 2 que tipo de impacto podría generar la materialización del riesgo, he propuesto 5 niveles desde muy bajo hasta muy alto, va depender mucho que siempre nos pongamos en la situación de preguntarnos: Qué pasaría en el peor de los casos? Es por ello que el primer valor a elegir es el impacto. El siguiente valor es la frecuencia que tiene de alcance un año, pensemos así como en el impacto, si no tuviéramos controles cuantas veces al año podría materializarse el riesgo, porque de eso se trata del riesgo inherente, pensar que no tenemos controles y poder así estimar cuánto daño nos podría hacer que se materialice el riesgo analizado. Una vez obtenido cada valor podremos localizar el resultado dentro de la matriz de riesgo del cuadro 4 con una simple multiplicación del impacto con la frecuencia.

Evaluación de Controles: Se debe calificar, cualitativamente, la efectividad de los controles (si se han identificado en la etapa anterior) asociados a los riesgos evaluados. En la evaluación cualitativa de los controles se utilizará una escala predefinida para calificar su efectividad con el objetivo de considerar su grado de mitigación en forma separada para el impacto y la frecuencia. Al evaluar los controles, es conveniente determinar también la clasificación del control (manual, automático, preventivo, detectivo y correctivo), la periodicidad del mismo y considerar a los responsables de su ejecución. También ha de considerarse el historial de eventos producidos en el proceso, lo que permitirá conocer los riesgos que puedan haberse materializado, la calificación otorgada por auditoria así como los planes implementados en el año que ayudan a reducir el riesgo. A continuación hago un resumen de algunas características de los controles:

TIPO DE CONTROL	
Preventivo	Son controles orientados a **prevenir** las causas del riesgo en una etapa muy temprana, ayudan a prevenir una pérdida.
	
Detectivo	Orientados a detectar actos indeseables. El punto de control se ubica dentro del proceso y las adecuaciones se enfocan a **detectar** y compensar los errores o desviaciones antes de que se elabore el resultado.
	
Correctivo	Son controles orientados a corregir las causas que originan el riesgo. El punto de control se ubica al final del flujo del proceso y las adecuaciones se enfocan a **corregir** los errores sobre el resultado obtenido.
	

Cuadro 5: Tipos de controles

Como resultado final de la etapa debería obtener una calificación final de cada control para poder obtener el riesgo residual.

Determinación del riesgo residual: Una vez realizada la evaluación de los controles, se podrá determinar el Riesgo residual, es decir el nivel de riesgo considerando la eficacia del control obteniendo los nuevos valores para el impacto y la frecuencia. Esta etapa debe tener la suficiente prueba metodológica para comprobar y evidencia que realmente un control o conjunto de ellos está mitigando adecuadamente los riesgos inherentes ya sea en su impacto, en su frecuencia o en ambos.

8.4 Evaluación del Riesgo Operacional

Lineamientos generales

El propósito de la evaluación de riesgos es tomar decisiones basadas en los resultados del análisis de riesgos de la etapa anterior, acerca de los riesgos que necesitan ser tratados y las prioridades de tratamiento con el objetivo de tenerlos en un nivel aceptable para. La evaluación de riesgo incluye comparar el nivel de riesgo residual encontrado durante el proceso de análisis con los criterios de tolerancia o aceptación del riesgo definido en la Etapa I- Establecimiento del Contexto. Con los niveles de tolerancia al riesgo establecido en la etapa 1: se debe distinguir aquellos riesgos que deben ser considerados para un tratamiento; en consecuencia, en esta actividad se obtienen los eventos de riesgo que tengan un riesgo residual superior a lo tolerable.

8.5 Tratar el Riesgo Operacional

Lineamientos generales

En esta etapa se identifican las opciones para tratar los riesgos, realizar la evaluación de dichas opciones, preparar los planes de mitigación de riesgos y su implementación. Sin embargo, la empresa puede decidir aceptar el riesgo sin tomar acciones adicionales.

Esta etapa involucra las siguientes actividades:

Identificar las opciones para la mitigación de riesgos. Las opciones, que no son necesariamente excluyentes y apropiadas en todas las circunstancias, incluyen lo siguiente:

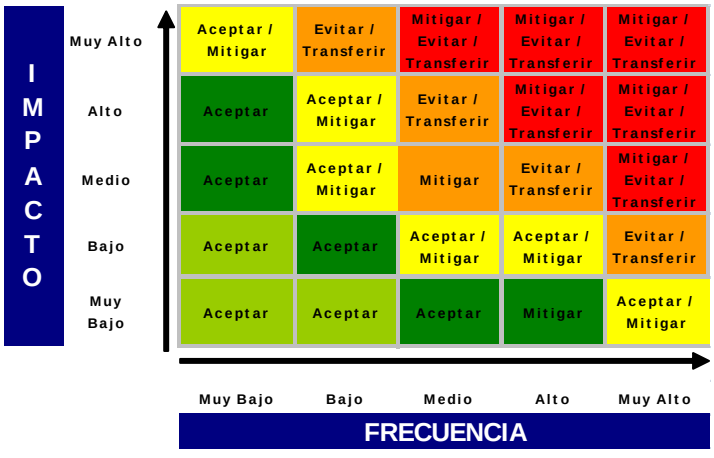
Aceptar el Riesgo.- Cuando se encuentra en un nivel que puede ser aceptado por la empresa, sin necesidad de tomar otras medidas de control diferentes a las que poseen.

Evitar el Riesgo.- Se evita el riesgo si se decide no proceder con la actividad que probablemente generaría el riesgo (cuando esto es practicable).

Reducir el Riesgo.- Reducir o controlar la probabilidad de la ocurrencia, Reducir o controlar las consecuencias

Transferir los riesgos.- Esto involucra que otra parte soporte o comparta parte del riesgo. Los mecanismos incluyen el uso de contratos arreglos de seguros y estructuras organizacionales tales como sociedades. La transferencia de un riesgo a otras partes, o la transferencia física a otros lugares, reducirá el riesgo para la Institución original, pero puede no disminuir el nivel general del riesgo para la sociedad.

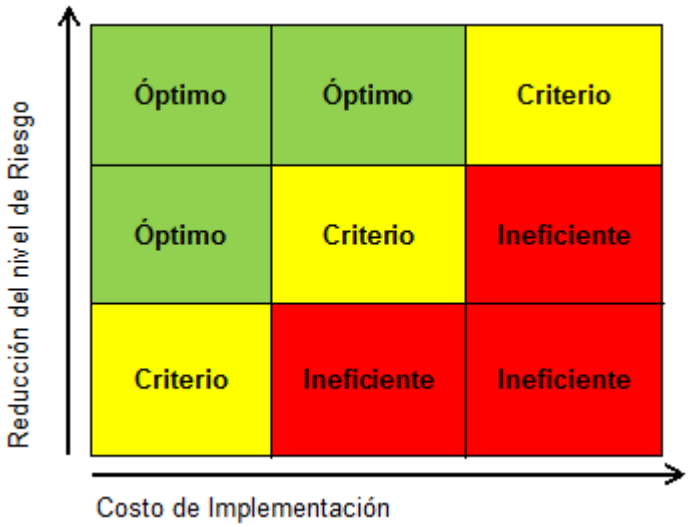
A continuación, se muestra una propuesta para tomar opciones para la mitigación de riesgos, de acuerdo al nivel de exposición.



Cuadro 6: Opciones de tratamiento al riesgo según su nivel

Evaluar las opciones de mitigación de riesgos.- Las opciones son evaluadas sobre la base del alcance de la reducción del riesgo, y el alcance de cualquier beneficio u oportunidad adicional creadas. Se consideran y aplican una cantidad de opciones ya sea individualmente o combinadas.

La selección de la opción más apropiada involucra balancear el costo de implementar cada opción contra los beneficios derivados de la misma. En general, el costo de administrar los riesgos es conmensurado con los beneficios obtenidos, como se muestra en el cuadro Nº 7:



Cuadro 7: Evaluación del Nivel de Riesgo vs. Costo de reducir el riesgo

Evaluar la efectividad de los planes de tratamiento, luego de implementados los diferentes planes de tratamiento para la mitigación de los riesgos identificados, según sea el caso, se deberá evaluar tomando en cuenta primero si el control existe y si esta implementado formalmente, si es apropiado y si existen debilidades en los procedimientos para su aplicación.

Se deben establecer planes de acción con el objetivo de reducir el nivel de riesgo residual obtenido de los riesgos identificados en las etapas anteriores y que no son tolerables o aceptables para la empresa. En dichos planes se describirán las acciones necesarias para el diseño e implementación de los mismos en un tiempo determinado.

El costo de la implementación de planes de acción no deberían exceder los beneficios esperados. Se debe dar prioridad de implementación a los planes que reducen riesgos de nivel Alto y Muy alto dependiendo de la tolerancia de la empresa. Los planes de acción deberán implementarse en el menor plazo

posible considerando el nivel de riesgo, la complejidad del plan, recursos y otros factores determinados por el responsable.

La designación del responsable la realizará el dueño del proceso Esta persona debe tener conocimientos, responsabilidad y cargo necesario para llevarlo a cabo.

El responsable del plan debe considerar que los costos de implementación sean menores a la pérdida que se podría producir por la materialización del evento de riesgo operacional.

8.6 Monitorear el Riesgo Operacional

Lineamientos generales

Esta etapa consiste en asegurar que la estrategia de gestión de riesgos operacionales está siendo cumplida y mantenida para la empresa. El procedimiento asociado al monitoreo de los riesgos requiere una revisión continua de los riesgos identificados, su nivel de riesgo determinado así como de las acciones planteadas como parte de los Planes de acción de los mismos.

Es importante poder determinar cómo se van comportando los riesgos en el tiempo, que acciones se vienen implementando por las áreas responsables así como poder identificar y registrar nuevos riesgos que hayan ocurrido.

Objetivos de la etapa

Monitorear el cumplimiento de las políticas, procedimientos y metodología de gestión del riesgo operacional.

Efectuar el seguimiento de los planes de mitigación, controles y KRI (Indicadores clave de Riesgo).

Identificar necesidades de capacitación y sensibilización para mejorar el proceso de implementación de la gestión de riesgo operacional.

Informar a instancias superiores los resultados de la función de monitoreo.

Identificar riesgos referentes a nuevos productos o servicios que la Compañía decida lanzar al mercado.

Actualización de la matriz de riesgos, incluyendo aquellos riesgos ya evaluados previamente.

Actividades a realizar

La etapa de Monitoreo y Revisión es un proceso continuo a través de todas las etapas de la metodología con el objetivo de medir constantemente la correcta ejecución de los mismos. Las actividades a realizar en esta etapa son:

Se debe tener un mecanismo para registrar eventos de riesgo operacional. Dicho registro debe contar con los datos necesarios que permitan analizar las causas y las consecuencias, para poder actualizar apropiadamente la matriz de riesgo y sus calificaciones de impacto y frecuencia cuando corresponda.

Evaluar los cambios en los procesos

Hacer seguimiento a los planes de acción relacionados a riesgos identificados de nivel alto y muy alto.

Actualización de matrices de riesgo por ocurrencia de eventos e informes de auditoría.

Base de eventos de pérdida

La base de datos de eventos de pérdida es un repositorio de información referente a eventos que se han materializado y han generado pérdida, dejar de ganar y dejar de cobrar. A continuación se explica el detalle de cada uno de estos eventos:

Pérdida de dinero: Impacto negativo en el Estado de Resultados o en patrimonio de la Entidad y que se registra contablemente.

Dejar de ganar: Ingreso susceptible de estimación que la entidad deja de percibir por la ocurrencia de un evento de riesgo operacional (lucro cesante).

Dejar de cobrar: Ingreso real que la entidad deja de percibir por la ocurrencia de un evento de riesgo operacional.

El área de Riesgo Operacional analizará el evento recabando de las áreas respectivas la documentación e información que sea necesaria para determinar el impacto y su registro en la base. De acuerdo a los resultados de la investigación, se emitirán los reportes respectivos conforme a lo establecido en la Etapa VII de la metodología.

La finalidad de tener una base de datos de eventos de pérdida es:

Mantener un registro histórico de eventos de pérdida, asociando los riesgos involucrados y priorizar acciones a tomar según su impacto

Permitir hacer proyecciones acerca de los eventos y las pérdidas que se puedan presentar en los procesos.

Determinar responsables de los eventos y tener criterios de escalamiento para los mismos.

Actualizar los niveles de riesgos de los procesos.

Sensibilizar e informar sobre la experiencia de los incidentes y eventos de pérdida registrados.

Determinar métricas de incidentes y eventos de pérdidas de los distintos Procesos.

La responsabilidad de actualizar y mantener la Base de Eventos de pérdida recaerá en el área de Riesgos Operacionales. Los campos mínimos de la base de datos de eventos de pérdida son (Ver **Anexo 3**):

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 Reglamento para la gestión del Riesgo Operacional de la SBS (R 2116 – 2009).

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).

Registro de eventos de pérdida

Una vez detectado un evento de pérdida, el colaborador que conoce del evento debe reportarlo al área de riesgo operacional quien procederá al análisis del mismo y en caso que determine que si es un evento de pérdida procederá a registrarlo en la base de eventos.

En la base de datos se registran los eventos que han generado pérdida, dejar de ganar, dejar de cobrar así como los eventos que no hayan generado un impacto y que podrían representar una oportunidad de mejora para reducir la probabilidad de ocurrencia.

En todo evento se registrará, en la medida que se obtenga la información, tanto las pérdidas directas de la empresa.

Identificación y análisis de riesgos en nuevos productos/servicios y cambios significativos en sistemas

Se debe realizar una identificación y análisis de nuevos productos/servicios después de haberse generado la idea, haberse verificado la viabilidad presupuestal para el proyecto y antes de tomarse la decisión de implementar el proyecto. Para realizar la identificación y análisis de riesgos el área de riesgos operacionales conjuntamente con el funcionario designado para el proyecto deberán realizar un análisis completo de riesgos sobre la base de la información recogida hasta ese momento, con el objetivo de identificar y analizar los riesgos que podrían materializarse si se implementa el nuevo producto/servicio para así tomar acciones que mitiguen, eviten, transfieran o acepten estos riesgos. El resultado de esta actividad se entregará al colaborador responsable del nuevo/producto y servicio quien determinará las acciones para reducir los riesgos que tengan un nivel no aceptable por la organización. Se adjunta un modelo de matriz de identificación de riesgos para nuevos productos/servicios y cambios significativos en sistemas.

Area de Riesgos Operacionales						*PRODUCTOS / SERVICIOS NUEVOS* *IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS OPERACIONALES*							FICHA N° :
Area Responsable del producto					Funcionario del Proyecto				Jefe/Analista R.O.				Fecha de Evaluación:
1.-	Denominación nuevo producto o servicio												
2.-	Descripción general de la nueva operación												
3.-	Diagrama de Bloques												
4.-	Procesos	Riesgos identificados	Impacto	Frecuencia	Nivel de Riesgo	Tipos de eventos de riesgo operacional							
						Fraude Interno	Fraude Externo	Daños a los activos materiales	Interrupción del negocio y fallos en los sistemas	Ejecución, entrega y gestión de procesos	Relaciones laborales y seguridad en el puesto de trabajo	Clientes, productos y prácticas empresariales	Plan de Acción
5.-	Acciones a tomar												
6.-	Conclusiones												

Cuadro N°8: Matriz de riesgos para nuevos productos/servicios y cambios significativos en sistemas

Implementación de indicadores de riesgo

Los KRI (Key Risk Indicators – indicadores claves de riesgo) permiten tener un marco de referencia de los riesgos operacionales siendo parte fundamental, ya que proveen una fuente de información para la Gestión de Riesgos Operacionales. Su implementación dependerá del análisis del riesgo que se realice, ya que en esta etapa, es donde se identifican los riesgos de nivel medio los cuales necesitaran un respectivo monitoreo a través de estas métricas.

Los KRI´s tienen como objetivo monitorear eventos de riesgo materializados para emitir alertas oportunas que permitan a la organización tomar acciones antes que los riesgos superen la tolerancia definida por la empresa. La materialización de los riesgos se identifica gracias al establecimiento de métricas de alerta que permiten advertir la ocurrencia de dichos eventos.

Los parámetros de las alertas deben ser definidos por medio de estos indicadores para asegurar que las respectivas acciones se ejecuten para así efectuar un monitoreo en forma periódica.

8.7 Comunicar el Riesgo Operacional

Lineamientos generales

La finalidad de esta etapa es proporcionar retroalimentación sobre las actividades de gestión de riesgo operacional Esta etapa debe desarrollarse a lo largo de todo la metodología.

Tipos de Informes

Los informes permiten a la compañía contar con un lenguaje común para administrar los resultados de la implementación y seguimiento de la gestión de Riesgos Operacionales y con ello entregar información que soporte la toma de decisiones en forma oportuna y efectiva.

Los informes serán entendidos como un conjunto de reportes utilizados para proveer a las Gerencias, Áreas y a cualquier otro involucrado de una clara visión del estado y la efectividad de la Gestión del Riesgo Operacional.

Los tipos de informes recomendados son:

Tipo de Informe	Dirigido a	Periodicidad
Informe Mensual de Riesgo Operacional	Jefe de Riesgo Operacional	Mensual
Informe de Pérdida por Riesgo Operacional	Jefe de Riesgo Operacional / Área de Finanzas	De acuerdo a criterio
Evaluación de riesgos operacionales en nuevos productos	Responsable del producto / proyecto	Cada vez que se presente
Informe de gestión de Riesgo Operacional (IGROP)	Gerente General / Comité de Riesgos	Semestral

Cuadro 9: Tipos de Informes

Objetivos principales de los reportes

Contribuir al proceso de sensibilización dentro de la empresa.

Agregar valor en el análisis de causa efecto.

Apoyar la toma de decisiones.

Compartir información.

Establecer procedimiento de escalamiento.

Identificar, informar riesgos y las acciones de mitigación a implementar.

Consideraciones para los reportes

Las siguientes preguntas facilitan dirigir el contenido de los reportes de Gestión de Riesgos Operacionales.

¿Qué es reportado?

¿Con qué frecuencia es reportada?

¿Cuáles son las expectativas de retroalimentación esperada de los reportes?

Los reportes pueden contener información como:

Resumen de reportes de incidentes de riesgos operacionales del último período.

Resumen de análisis y evaluación por procesos y/o subprocesos.

Detalles de Procesos o áreas identificadas como riesgosas.

Identificación y elaboración de Indicadores.

Audiencia

Gerente General

Gerentes y Jefes

Dueños de Procesos

Área de Riesgos Operacionales

Dependiendo de la audiencia receptora, los reportes entregarán información detallada o resúmenes ejecutivos, así los receptores recibirán informes como:

Gerencia General:

Resumen ejecutivo de eventos de pérdida materializados.

Evaluación de riesgos y resultado de indicadores, otros.

Gerencias y/o Jefaturas:

Resumen ejecutivo de sus eventos de pérdida materializados.

Reportes detallados de análisis y evaluación de riesgos de sus áreas.

Resultados del monitoreo de sus Indicadores, otros.

Dueños de Procesos:

Información específica de eventos de pérdida, otros.

Matriz de Riesgos

Una vez aplicada la metodología es necesario presentar mensualmente ya sea por área o de manera general la siguiente Matriz de Riesgos (Los valores son de ejemplo para que se valide que es lo que debe ser completado)

Proceso		Riesgo			Riesgo Inherente		Controles					Riesgo Residual		Plan de Accion			
Codigo Proceso	Nombre Proceso	Causas	Riesgo	Consecuencia	Impacto Inherente	Frecuencia Inherente	Descripcion del control	Documentación	Naturaleza	Oportunidad	Efectividad	Impacto Residual	Frecuencia Residual	Descripcion	Hito	Fecha Inicio	Fecha Fin
TI	Soporte Tecnología de la Información	Que no cuente con respaldo eléctrico	Indisponibilidad del Sistema Transaccional	Perdida de Dinero	Muy Alto	Muy Alto	Anualmente se mantiene los UPS y generador eléctrico	Si	Preventivo	Anual	Inefectivo	Alto	Moderado	Comprar un UPS adicional	Buscar proveedor	01/01/2013	10/01/2013
															Firmar contrato	11/01/2013	21/01/2013
		Que no se realice mantenimiento a los equipos		Multas por incumplimiento de contrato			El jefe de TI tiene un contrato de mantenimiento de servidores	Si	Preventivo	Anual	Efectivo				Realizar seguimiento a la instalación y configuración	22/01/2013	30/01/2013

Cuadro N°10: Matriz de Riesgo Operacional

CAPÍTULO 9 : CONCLUSIONES, LECCIONES APRENDIDAS Y RECOMENDACIONES.

9.1 Conclusiones

La aplicación de la Gestión del Riesgo Operacional es una pieza clave en el desarrollo adecuado de un Banco debido no solo a su obligación de tenerla en los Bancos si no por sus beneficios siendo el principal: Perder menos dinero.

Todos los procesos tienen objetivos, es por ello que es muy importante identificar los objetivos operacionales de los procesos y alinearlos con los objetivos estratégicos de la empresa que responde al Plan Estratégico de la empresa, debido a que los riesgos atacan directamente a los objetivos.

La parte más importante de la Fase I: Establecimiento del Contexto, es la definición de los niveles de riesgo, es con ello como se medirán todos los riesgos más adelante.

La Fase II de la metodología debe ser coordinada y aprobada por el dueño del proceso el cual se le está identificando los riesgos operacionales.

Una de las fases más complicadas es la Fase III: Análisis del riesgo, debido a que se debe tener mucho entendimiento de realmente como un riesgo puede impactar al negocio operacionalmente.

El riesgo residual debería obtenerse automáticamente si es que se definió bien el riesgo inherente así como la calificación de controles.

La Fase IV: Evaluación del Riesgo es una etapa estratégica para definir que riesgos tienen prioridad y que riesgos no. Para ello de la lista de riesgos residuales que se encuentran dentro de la matriz de riesgo y no están dentro de la tolerancia de la empresa (por ejemplo nivel muy alto y alto) se deberá definir estrategias de tratamiento para cada riesgo dentro del umbral no tolerable.

El seguimiento continuo del avance de los planes de acción es clave para que se terminen en el tiempo estimado. Lamentablemente se actúa ante presión, y es por ello que el área de riesgo operacional debe ser responsable de verificar el avance de los principales planes de acción de la empresa.

El resultado crítico de la fase VI es la base de datos de eventos de pérdida. Esta base es un gran repositorio de información rica en amenazas y vulnerabilidades explotadas para que se haya materializado el riesgo. Esta base no debería ser solo un repositorio si no una fuente de información especial que nos permita actualizar los niveles de riesgo debido a que con esta base podremos validar cómo la frecuencia se ha materializado en el tiempo, generalmente en un horizonte de un año.

Los KRI'S como cualquier indicador, es una herramienta que nos genera una alerta temprana para tomar acción de algo.

Los nuevos productos y los cambios significativos en sistemas deberían tener un análisis de riesgos, así como se tiene análisis de viabilidad económica, estudios de mercado entre otros estudios que se estilan para realizar cambios o sacar productos, el análisis de riesgos es fundamental para saber que podría afectarnos y no dejarnos llegar a nuestro objetivo.

La Fase VII es una de las dos fases (también monitoreo) que se realizan en toda la metodología en forma consistentemente, dado que es importante que todos los stakeholders conozcan el avance de la gestión del riesgo operacional.

La Gestión de la Seguridad de la Información y la Continuidad del Negocio son claves en la adecuada implementación de un Sistema de Gestión de Riesgo Operacional. Dependiendo de la empresa estas gestiones pueden llevarse juntas o separadas sin embargo es importante que la Gerencia se asegure que las 3 áreas se complementan y coordinan constantemente.

9.2 Lecciones aprendidas

La Gestión del Riesgo Operacional tiene una gran oportunidad de automatización en su aplicación. Toda la metodología puede ser soportada por un sistema informático dando muchos beneficios al sector financiero que aún no

tenga un sistema para gestionarla. Lo que se ha podido observar es que es mejor comenzar sin un sistema para establecer adecuadamente las bases en toda la organización.

Por experiencia, se ha podido comprobar que los planes de acción generalmente duran más de lo que uno estima. Es por ello que sin proponer hitos y tener un constante seguimiento de su cumplimiento, puede llevar a que los planes de acción se completen con demoras o lleguen a desestimarse.

Desde un inicio, se debe acompañar al usuario para el reporte de eventos de riesgo operacional. Tratar de completar en promedio 21 campos cada vez que se reporta en evento puede llevar a que simplemente los eventos de riesgo operacional no sean reportados no pudiendo agregarlos a la base de datos de eventos de pérdida.

9.3 Recomendaciones

En la Fase I, se recomienda siempre comenzar de una manera cualitativa, usar valores cercanos a la realidad de la empresa, las perdidas y la utilidad antes del impuesto para hallar el impacto económico que puede interrumpir el negocio es uno de las reglas más usadas. No olvidar que también se puede usar el impacto de imagen ante los stakeholders, en cumplimiento de los entes reguladores u otro tipo de impacto que la empresa deba tener en cuenta y que debería ser medido.

En la Fase II: Identificación de riesgos, requiere mucho del entendimiento del proceso, se recomienda que se realice siempre con un diagrama de flujo para identificar por cada actividad que riesgo puede haber, si no se tiene, se hace mucho más rica la reunión si en ese momento se define con el apoyo del dueño del proceso. Sí, es una tarea ardua pero gratificante dado que tanto el área de riesgos operacionales así como el dueño entienden la importancia de identificar riesgos que no le dejen cumplir sus objetivos.

Es recomendable no solo invitar al dueño del proceso sino también a posibles participantes transversales del mismo, en otras palabras si hay otras áreas que participan del proceso es recomendable que también asistan para que comuniquen una perspectiva distinta de los riesgos del proceso. Ha pasado

muchas veces que identificaba más riesgos con un participante externo que con el mismo dueño, dado que no todos los dueños de los procesos quieren comentar sus riesgos, es natural que no todos quieran decir que errores pueden tener en su área.

Se recomienda que en la Fase IV, la tabla de impactos siempre debe realizarse con valores reales del negocio, si no es con la utilidad antes del impuesto, utilizar valores de pérdidas históricas de la compañía debido a que es necesario que el dueño del proceso se sienta identificado con los números que él está eligiendo para medir el impacto. Adicionalmente se pueden utilizar otros tipos de impacto que no están relacionados directamente a la perdida de dinero como el tema de lucro cesante pero no debería ser una elección en primera opción. El riesgo operacional está orientado en tratar de estimar una pérdida de dinero que se pueda reflejar en el estado de ganancias y pérdidas de la empresa en otras palabras está orientado a relacionarse con una cuenta contable de pérdida.

Se recomienda que para calificación de controles siempre debe intervenir Auditoría dado que es el área que realmente valida in situ si un control es efectivo o no, el área de riesgo operacional podrá medir el diseño de un control mas no comprobar si realmente es efectivo o no. Esto es labor de Auditoría dado que con una metodología basada en riesgos, ellos se encargan de evidenciar mediante una muestra representativa que tan efectivo es un control, recomendar mejoras del control entre otros. Para la fase III es fundamental la participación de auditoria conjuntamente con el área de Riesgo Operacional. Es un reto debido a que generalmente cada área tiene sus objetivos individuales y tratan de llegar a ellos pero no se dan cuenta que juntos, con colaboración eficaz y continua pueden cumplir sus objetivos más rápido.

Se recomienda de acuerdo a la experiencia de cada gestor, validar y afinar si es necesario los riesgos dentro del umbral de aceptabilidad de la empresa, deberían ser riesgos que realmente de acuerdo a la envergadura de la empresa son los que pueden hacer más daño.

La principal recomendación en esta fase V es saber cómo y quien define un plan de acción. Si bien es cierto, la estrategia de reducir el riesgo es la más usada porque está en nosotros de tratar de hacer algo para que el riesgo no se

materialice, es importante saber que definimos, por el mismo ímpetu de definir algo que nos ayude puede que definamos acciones que al final cuesten y nos hagan perder horas hombres más de lo que nos costaría de que un riesgo se materialice, es por ello que es importante hacer siempre un juicio de costo/beneficio de implementar un plan de acción. Si es posible se recomienda también hacer pilotos del plan de acción y siempre medir su evolución en el tiempo.

Se recomienda siempre definir hitos en los planes de acción para poder tener un mejor seguimiento debido a que un plan de acción puede definirse a tiempo para su implementación en 1 semana así como 1 año, ¿cómo se puede medir el avance de un plan de 1 año si no se tiene hitos mensuales?

Se recomienda que la alta dirección debe ser sponsor principal para que esta etapa funcione, el seguimiento seguido por parte de la Gerencia General de los planes de acción de la empresa es fundamental para que todas las áreas sientan que realmente la ejecución de los mismos es valioso y necesario.

Se recomienda en la Fase VI que la Base de datos de eventos de perdida se relacione con riesgos ya registrados y si no están registrados inmediatamente agregarlos en la matriz de riesgos generales, de esta manera mantener viva toda la metodología.

Se recomienda que todas las áreas participen del reporte de eventos, no solo el área de riesgo operacional, es imposible estar en todas partes es por ello que las áreas y sus reportes son esenciales.

Se recomienda tener un programa de incentivos diseñado adecuadamente para que empuje a toda la empresa a registrar eventos en búsqueda de la eficiencia de la empresa.

Se recomienda definir KRIS en riesgos de nivel medio dado que esos son los riesgos que más cuidado se deben tener porque están en un umbral que podría en el tiempo cambiarse a un nivel alto y muy alto posiblemente no tolerable para la organización.

Se recomienda hacer el análisis de riesgos desde la concepción de la idea de un producto con un simple diagrama de bloques para identificar las relaciones y procesos involucrados.

Se recomienda en la Fase VII que se debe presentar solo la información que es necesaria, suena fácil pero realmente es complicado cuando se presenta un informe para un equipo multidisciplinario y no se ha definido qué información necesita cada uno. Es por ello que mejor es hacer varios informes que solo uno. Es importante validar el alcance de la información así como el público objetivo de la misma.

Se recomienda identificar activos de información conjuntamente con riesgos operacionales en la Fase 1: Identificación de Riesgos dado que en esta fase se levanta información valiosa para el área de Riesgo Operacional y Seguridad de la Información.

En la implementación de la Gestión de Continuidad del Negocio es importante la etapa de pruebas debido a que en esta etapa se valida si realmente la organización está preparada para cumplir los tiempos que se estimaron en la etapa de entendimiento de la organización. Se recomienda medir tiempos estimados con tiempos reales y ver si la desviación es considerable para actualizar los tiempos estimados.

GLOSARIO DE TERMINOS

BCM: Business Continuity Management, administración de la continuidad del negocio.

Evento de pérdida por riesgo operacional: es el evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.

Evento de riesgo operacional: suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por una o varias causas, que ocurren durante un determinado periodo y que afectan la consecución de los objetivos operacionales de la empresa.

Factores que Originan el Riesgo Operacional: Los factores de riesgo, son aquellas fuentes generadoras de eventos, internas o externas, que pueden originar pérdidas en las operaciones o afectar el cumplimiento de los objetivos estratégicos y/o operacionales de la Institución. Estos son: personas, procesos, tecnología de la información y eventos externos.

FODA: matriz encargada de dar a conocer a la empresa sus fortalezas, oportunidades, debilidades y amenazas.

Fraude Externo: acción que comete perjuicio contra otra persona o contra una organización y es realizada por un externo.

Fraude Interno: acción que comete perjuicio contra otra persona o contra una organización y es realizada por alguien que labora dentro de esa misma entidad.

Gestión del Riesgo Operacional: es reconocida como una parte integral de las buenas prácticas gerenciales y consiste en un método práctico y sistemático de establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos asociados a una determinada actividad o proceso; de este modo, se optimiza la posibilidad de minimizar pérdidas y de identificar claramente las causas, los eventos y el impacto de los Riesgos Operacionales.

Help Desk: Mesa de ayuda. Área de informática encargada de resolver problemas e incidencias dentro de una empresa.

Indicador clave de riesgo (KRI'S: Key Risk Indicators): indicador que se utiliza para alertar sobre la evolución de un riesgo detectando a tiempo si un riesgo está por materializarse.

IP: Internet Protocol. Protocolo de internet.

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

Metodología: guía que se sigue a fin de realizar las acciones propias de una actividad continua.

MTO: Maximum tolerable outage. Significa el tiempo máximo que una organización puede sobrevivir sin procesos de negocio.

Pérdida operacional: todo impacto negativo o reducción en la cuenta de resultados o en la situación patrimonial de VisaNet Perú susceptible de tener reflejo contable, cuyo origen sea un evento de pérdida por riesgo operacional.

Plan de acción: también llamando plan de mitigación que es un conjunto de actividades que se implementan para minimizar un riesgo.

Política: lineamiento de carácter general utilizado como referencia principal, aplicado a toda la compañía y alineado con las estrategias y procesos definidos, que resulta necesario para el logro de los objetivos del negocio.

POS: Point of Sale. Punto de venta. Dispositivo electrónico que se encarga de leer y procesar información de tarjetas de crédito.

Procedimiento: es el modo de ejecutar determinadas acciones que suelen realizarse de la misma forma, con una serie común de pasos claramente definidos, que permiten realizar un trabajo.

Proceso: conjunto de actividades, tareas y procedimientos que se realizan sucesivamente, con el objeto de transformar una serie de entradas (insumos)

específicas en salidas (resultados, productos o servicios) predeterminadas que cumplen un objetivo en común.

Proceso crítico: proceso considerado indispensable para la continuidad de las operaciones y servicios de VisaNet Perú cuya falta o ejecución deficiente puede producir no cumplir con los objetivos del proceso, ni con los objetivos estratégicos de la Institución y/o generar pérdidas financieras, o cuando el nivel de criticidad de un proceso sea el de mayor escala de riesgo establecido por la Compañía.

Riesgo: la condición en la que existe la posibilidad de que un evento ocurra e impacte negativamente el logro de los objetivos de VisaNet Perú. A continuación se describen algunos tipos de riesgo específicos:

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

Riesgo legal: posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros.

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.

Riesgo Reputacional: 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.

Riesgo inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo residual: Nivel resultante del riesgo después de aplicar los controles.

RPO: Recovery point objective. Se refiere a qué tanta información necesitamos para poder continuar nuestra operación con normalidad luego de un evento de continuidad del negocio.

RTO: Recovery time objetive. Se refiere a que tanto tiempo podemos estar inoperativas antes de poder a perder significativamente en el negocio tras un evento de continuidad del negocio.

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

Sponsor: es una empresa o entidad que te patrocina en un emprendimiento y aporta dinero para un proyecto.

Tecnología de información: incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.

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

Tratamiento al riesgo: es la acción que la compañía toma para prevenir o mitigar los impactos de eventos que afectaría el logro de objetivos, mediante una apropiada definición e implementación de controles, de manera que los riesgos se sitúen en un nivel tolerable por la institución.

REFERENCIAS BIBLIOGRAFICAS

Project Management Institute. (2008). A guide to the project management body of knowledge (PMBOK guide) (4th ed.), PA: Project Management Institute.

PMI: http://www.pmi.org/.

SBS: http://www.sbs.gob.pe/0/home.aspx

ISO 27001: http://www.27000.org/iso-27001.htm

BASILEA II: http://www.bis.org/publ/bcbs109esp.pdf

COSO ERM: http://www.coso.org/-erm.htm

Estándar Australiano / Neo Zelandés 4360: http://www.mwds.com/AS4me_files/AS-NZS%204360-2004%20Risk%20Management.pdf

Business Process Management: http://www.bpmi.org/

Operational Risk: http://www.theopriskpractice.com/

ANEXOS

ANEXO N° 1

Lima, 02 de abril de 2009

CIRCULAR Nº G- 140 -2009

Ref.: Gestión de la seguridad de la información

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias en adelante Ley General, y por el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones, las cuales toman como referencia estándares internacionales como el ISO 17799 e ISO 27001, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

Alcance

Artículo 1º.- La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

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

Definiciones

Artículo 2º.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

b. Factor de autenticación: Información utilizada para verificar la identidad de una persona. Pueden clasificarse de la siguiente manera:
- *Algo que el usuario conoce (por ejemplo: una clave de identificación)*
- *Algo que el usuario posee (por ejemplo: una tarjeta)*
- *Algo que el usuario es (por ejemplo: características biométricas)*

c. Incidente de seguridad de información: Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

d. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.[1]

e. Ley General: Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias.

f. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:

I. Confidencialidad: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
II. Integridad: La información debe ser completa, exacta y válida.
III. Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

[1] Literal modificado por la Circular N° G-167-2012 del 05/11/2012.

g. *Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.*

h. *Subcontratación significativa: Aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, o continuidad operativa.*

Sistema de gestión de la seguridad de la información

Artículo 3º.- Las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI).

Las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

a. Definición de una política de seguridad de información aprobada por el Directorio.
b. Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
c. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Estructura organizacional

Artículo 4°.- Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información señalado en el artículo anterior.
Asimismo, deben asegurarse que se desarrollen las siguientes funciones, ya sea a través de una unidad especializada o a través de alguna de las áreas de la empresa:

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

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

Controles de seguridad de información

Artículo 5°.- Como parte de su sistema de gestión de la seguridad de información, las empresas deberán considerar, como mínimo, la implementación de los controles generales que se indican en el presente artículo.

5.1 Seguridad lógica

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.
b) Revisiones periódicas sobre los derechos concedidos a los usuarios.
c) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
d) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
e) Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.
f) Controles especiales sobre usuarios remotos y computación móvil.

5.2 Seguridad de personal

a) Definición de roles y responsabilidades establecidos sobre la seguridad de información.
b) Verificación de antecedentes, de conformidad con la legislación laboral vigente.
c) Concientización y entrenamiento.
d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.
e) Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.

5.3 Seguridad física y ambiental

a) Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.
b) Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.

5.4 Inventario de activos y clasificación de la información

a) Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.
b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

5.5. Administración de las operaciones y comunicaciones

a) Procedimientos documentados para la operación de los sistemas.
b) Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
c) Separación de funciones para reducir el riesgo de error o fraude.
d) Separación de los ambientes de desarrollo, pruebas y producción.
e) Monitoreo del servicio dado por terceras partes.
f) Administración de la capacidad de procesamiento.
g) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
h) Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.

i) Seguridad sobre el intercambio de la información, incluido el correo electrónico.
j) Seguridad sobre canales electrónicos.
k) Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.

5.6. Adquisición, desarrollo y mantenimiento de sistemas informáticos

Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
d) Controlar el acceso a las librerías de programas fuente.
e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.
f) Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.

5.7. Procedimientos de respaldo

a) Procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la empresa.

b) Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento.

5.8. Gestión de incidentes de seguridad de información

Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, las empresas deberán considerar los siguientes aspectos:

a) Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.
b) Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

5.9. Cumplimiento normativo

Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

5.10. Privacidad de la información

Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.

Seguridad en operaciones de transferencia de fondos por canales electrónicos

Artículo 6°.- En el caso de las operaciones de transferencia de fondos a terceros ofrecidas por las empresas para su realización a través de canales electrónicos, las empresas deberán implementar un esquema de autenticación de los clientes basado en dos factores como mínimo. Para el caso en que el canal electrónico sea Internet, uno de los factores de autenticación deberá ser de generación o asignación dinámica. Las empresas podrán utilizar otros factores de autenticación, en tanto éstos proporcionen un nivel de seguridad equivalente o superior respecto a los dos factores señalados, en particular cuando se trate de operaciones importantes según los límites que el banco determine de acuerdo a las características del producto o servicio ofrecido.

La empresa deberá tomar en cuenta los riesgos operacionales asociados, en el diseño de los procedimientos, las definiciones de límites y las consideraciones de seguridad e infraestructura requeridas para un funcionamiento seguro y apropiado en las operaciones de transferencia de fondos.

Subcontratación[2]

Artículo 7º.- Las empresas son responsables y deben verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en el artículo 21° del Reglamento de la Gestión Integral de Riesgos. Asimismo, las empresas deben asegurarse que el procesamiento y la información objeto de la subcontratación, se encuentre efectivamente aislada en todo momento.

Subcontratación significativa de procesamiento de datos en el exterior[3]

Artículo 7.Aº.- En caso que las empresas deseen realizar una subcontratación significativa de su procesamiento de datos, de tal manera que éste sea realizado en el exterior, requerirán de la autorización previa y expresa de la Superintendencia. Para ello, la empresa debe asegurar un adecuado cumplimiento de la presente Circular, en lo que sea aplicable al servicio de procesamiento contratado.

La Superintendencia podrá requerir, cuando así lo considere apropiado, que el proveedor del servicio en el exterior se encuentre sujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio.

[2] Artículo modificado por la Circular N° G-167-2012 del 05/11/2012.

[3] Artículo incorporado por la Circular N° G-167-2012 del 05/11/2012.

La autorización concedida por la Superintendencia, de ser el caso, es específica al proveedor del servicio y el país desde el que se recibe, así como a las condiciones generales que fueron objeto de la autorización, por lo que de existir modificaciones en ellas, se requiere de un nuevo procedimiento de autorización ante la Superintendencia.

En el Anexo A que forma parte de la presente norma y se publica en el Portal electrónico institucional (www.sbs.gob.pe), conforme a lo dispuesto en el Decreto Supremo N° 001-2009-JUS, se detalla la información que debe remitir la empresa adjunta a su solicitud de autorización.

Una vez recibida la documentación completa, dentro de un plazo que no excederá de sesenta (60) días útiles, la Superintendencia emitirá la resolución que autoriza o el oficio que deniega la solicitud presentada por la empresa.

Los servicios objeto de subcontratación en el exterior deberán ser sometidos anualmente a un examen de auditoría independiente, por una empresa auditora de prestigio, que guarde conformidad con el ISAE 3402, emitido por la Federación Internacional de Contadores (IFAC), o la SSAE 16, emitida por el Instituto Americano de Contadores Públicos Certificados (AICPA), debiendo cada entidad remitir a esta Superintendencia el reporte tipo 2 previsto por dichos estándares.

Información a la Superintendencia

Artículo 8°.- Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la gestión del riesgo operacional, emitido por la SBS, las empresas deberán incluir información sobre la gestión de la seguridad de la información.

Información adicional

Artículo 9°.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión de la seguridad de la información de la empresa.

Asimismo, la empresa deberá tener a disposición de la Superintendencia todos los documentos a que hace mención la presente Circular, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de ser aplicable.

Sanciones

Artículo 10°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Vigencia

Artículo 11°.- Las disposiciones de la presente Circular entran en vigencia al día siguiente de su publicación en el Diario Oficial "El Peruano", otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010, fecha a partir de la cual quedará sin efecto la Circular SBS Nº G-105-2002.

Adecuación de las AFP

Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las AFP deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

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

Atentamente,

FELIPE TAM FOX

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

ANEXO A

DOCUMENTACIÓN A REMITIR JUNTO CON LA SOLICITUD DE AUTORIZACIÓN PARA REALIZAR PROCESAMIENTO PRINCIPAL EN EL EXTERIOR

Documento	Contenido mínimo requerido
1. Información general del proveedor y del servicio	• Razón social del proveedor. • Giro del negocio y años de experiencia. Indicar a qué empresas brinda servicios actualmente. • Estados Financieros del proveedor correspondientes a los dos últimos años. • Relación de accionistas del proveedor y funcionarios principales. • Relación con la empresa supervisada (indicar si pertenecen al mismo grupo económico). • Servicios que serán provistos por el proveedor y el tipo de información a ser procesada. • Ubicación (país y ciudad) del centro de procesamiento principal. • Razones para seleccionar al proveedor.
2. Borrador del Contrato	Aspectos a considerar: • Acuerdos de niveles de servicio. • Procedimientos de monitoreo. • Procedimientos de contingencia. • Cumplimiento de las normas sobre secreto bancario y confidencialidad de la información. • Prestación del servicio en regímenes especiales (vigilancia, intervención, liquidación). El proveedor debe seguir brindando el servicio como mínimo un año después de que la empresa ha ingresado a un régimen especial. • Compromiso de cumplimiento de la normativa de la Superintendencia. • Aseguramiento del acceso adecuado a la información con fines de supervisión, en tiempos razonables y a solo requerimiento, por parte de la Superintendencia, Auditoría Interna y Externa, en condiciones normales de operación y en regímenes especiales. Este aspecto debe ser aplicable sobre cualquier otra empresa que el proveedor subcontrate para brindar servicios a la entidad supervisada. • Cláusulas que faciliten una adecuada revisión por parte de la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa y la Superintendencia.
3. Informe de la Plataforma Tecnológica	Aspectos a considerar: (Señalar qué equipos y aplicaciones estarán a cargo del proveedor) • Inventario de equipos de cómputo. • Inventario de software base. • Herramientas y/o manejadores de base de datos. • Aplicaciones críticas. • Esquema de comunicaciones a ser implementado entre el proveedor y la empresa supervisada.
4. Informe de Comunicación con la	• Descripción de la forma de envío de información a la Superintendencia luego de que se implemente el servicio de procesamiento en el exterior. Asimismo, indicar

Superintendencia (SUCAVE, RCD, otros)	los cambios que se aplicarán sobre los procedimientos asociados a la generación, consolidación y reporte de dicha información.
5. Informe de Evaluación de Riesgos	• Evaluación de los riesgos de operación asociados con el esquema propuesto por la empresa, realizada por la Unidad de Riesgos.
6. Gestión de la seguridad de información	• Política de seguridad de información de la empresa. • Estructura organizativa para la gestión de la seguridad de información. • Asignación de responsabilidades asociadas con la seguridad de información en la entidad y el proveedor. • Forma en que se aislará el procesamiento y la información objeto de la subcontratación. • Procedimientos y controles a implementar, considerando el procesamiento en el exterior, en los siguientes aspectos: - Seguridad lógica. - Seguridad de personal. - Seguridad física y ambiental. - Administración de las operaciones y comunicaciones. - Desarrollo y mantenimiento de los sistemas informáticos. - Administración de las copias de respaldo.
7. Gestión de continuidad de negocios	• Plan de Contingencia del proveedor, para asegurar la continuidad del servicio de procesamiento informático. • Señalar la prioridad asignada al procesamiento de la información de la empresa supervisada respecto al resto de clientes del proveedor. • Señalar la forma en que se dará aviso a la empresa supervisada, y las acciones que deberá desarrollar la empresa en caso de una contingencia en el proveedor. • Frecuencia y alcance de las pruebas al Plan de Contingencia del proveedor.
8. Plan de Auditoría de Sistemas	• Señalar el alcance, forma y periodicidad de las revisiones de auditoría de sistemas considerando el nuevo esquema de procesamiento principal de la empresa.
9. Gestión del proyecto	• Cronograma de actividades, incluyendo plazos, responsables y principales hitos de control. • Costo estimado de implementación del proyecto.

ANEXO N° 2

Lima, 02 de abril de 2009

CIRCULAR Nº G- 139 -2009

Ref.: Gestión de la continuidad del negocio

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias en adelante Ley General, y por el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones aprobado por el Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para la gestión de la continuidad del negocio, que forma parte de una adecuada gestión del riesgo operacional que enfrentan las empresas supervisadas, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones, las cuales toman como referencia estándares internacionales como el BS-25999, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

Alcance

Artículo 1º.- La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación

Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Definiciones

Artículo 2º.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

i. 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.

j. Grupos de interés: Personas u organizaciones que se ven impactadas por las operaciones de una empresa. Ejemplos: clientes, socios del negocio, empleados, proveedores, accionistas, entidades gubernamentales, entre otros.

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

l. Ley General: Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias.

m. Periodo máximo tolerable de interrupción: Es el periodo de tiempo luego del cual la viabilidad de la empresa sería afectada seriamente, si un producto o servicio en particular no es reanudado.

n. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.

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

p. 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.

q. Tiempo objetivo de recuperación: Es el tiempo establecido por la empresa para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción.

Gestión de la continuidad del negocio

Artículo 3º.- La gestión de la continuidad del negocio es un proceso, efectuado por el Directorio, la Gerencia y el personal, que implementa respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Las empresas deben realizar una gestión de la continuidad del negocio adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

Responsabilidad del Directorio

Artículo 4º.- El Directorio es responsable de establecer una adecuada gestión de la continuidad del negocio. Entre sus responsabilidades específicas están:

a. Aprobar una política general que defina el alcance, principios y guías que orienten la gestión de la continuidad del negocio.
b. Aprobar los recursos necesarios para el adecuado desarrollo de la gestión de la continuidad del negocio, a fin de contar con la infraestructura, metodología y personal apropiados.
c. Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión de la continuidad del negocio.

Responsabilidad de la Gerencia

Artículo 5º.- La gerencia general tiene la responsabilidad de implementar la gestión de la continuidad del negocio conforme a las disposiciones del Directorio. La gerencia podrá constituir comités para el cumplimiento de sus responsabilidades relacionadas con la gestión de la continuidad del negocio.

Responsabilidad de la Unidad de Riesgos

Artículo 6º.- La Unidad de Riesgos deberá asegurarse que la gestión de la continuidad del negocio que realice la empresa sea consistente con las políticas y procedimientos aplicados para la gestión de riesgos.

Función de continuidad del negocio

Artículo 7º.- Las empresas deberán contar con una función de continuidad del negocio, la cual tendrá a su cargo las siguientes responsabilidades:

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

En función a su tamaño y complejidad de operaciones y servicios, esta función será desempeñada por una unidad especializada o asignada a otra unidad de la empresa.

Fases de la gestión de la continuidad del negocio

Artículo 8º.- Las empresas deberán desarrollar como mínimo las siguientes fases como parte de la gestión de la continuidad del negocio:

8.1. Entendimiento de la organización

Esta fase consiste en conocer los objetivos y metas de la empresa; identificar los principales procesos, productos, servicios y proveedores, así como las actividades

y recursos requeridos; evaluar los riesgos que podrían causar una interrupción de dichas actividades, y el impacto que podría tener dicha interrupción.

Las actividades mínimas a desarrollar durante esta fase son las siguientes:

a. **<u>Análisis de impacto</u>: Consiste en determinar el impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios de la empresa. Para ello, deben considerarse aspectos como: daños a la viabilidad financiera de la empresa, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. Según ello, debe establecerse el período máximo tolerable de interrupción por cada uno de estos procesos.**

   El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados.

b. **<u>Evaluación de riesgos</u>: Consiste en identificar y evaluar los riesgos que podrían causar una interrupción del negocio. Para ello, deberá seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos que enfrenta la empresa.**

La empresa debe definir qué procesos requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos.

8.2. Selección de la estrategia de continuidad

En esta fase, se determinan las estrategias de continuidad que permitirán mantener las actividades y procesos de negocio luego de ocurrido un evento de interrupción de operaciones.

Debe desarrollarse, como mínimo, la siguiente actividad:

a. **<u>Evaluación y selección de estrategias de continuidad por proceso</u>: Se refiere a seleccionar las estrategias que permitirán mantener la continuidad de los procesos que soportan los principales productos y servicios de la empresa, dentro del tiempo objetivo de recuperación, definido para cada proceso. Las estrategias de continuidad deben tomar en cuenta los siguientes aspectos, según sea aplicable para cada proceso:**
   - **Seguridad del personal.**
   - **Habilidades y conocimientos asociados al proceso.**
   - **Instalaciones alternas de trabajo.**
   - **Infraestructura alterna de tecnología de información que soporte el proceso.**
   - **Seguridad de la información.**
   - **Equipamiento necesario para el proceso.**

8.3. Desarrollo e implementación de la estrategia de continuidad

En esta fase, se deben desarrollar los planes de respuesta ante los eventos analizados en las fases previas, e implementar un modelo de respuesta flexible y escalable que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con la estrategia seleccionada, para enfrentar con éxito un evento de interrupción de operaciones. Para este fin, las empresas deberán implementar dos tipos de planes:

a. **<u>Plan de Gestión de Crisis</u>: Consiste en preparar a la empresa para enfrentar la fase aguda de un evento de interrupción de operaciones, incluso de aquellos no esperados. Debe incluir los siguientes aspectos:**
   - **Propósito y alcance**
   - **Roles y responsabilidades**
   - **Criterios de invocación y activación**
   - **Responsable de su actualización**
   - **Planes de acción**
   - **Comunicaciones con el personal, familiares y contactos de emergencia**
   - **Interacción con los medios de comunicación**
   - **Comunicación con los grupos de interés**
   - **Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno)**

b. **<u>Plan(es) de Continuidad del Negocio</u>: Tiene(n) como objetivo dotar a la empresa de la capacidad de mantener, o de ser el caso recuperar, los principales procesos de negocio dentro de los parámetros previamente establecidos. Debe(n) considerar, como mínimo, los siguientes aspectos:**
   - **Propósito y alcance**
   - **Roles y responsabilidades**
   - **Criterios de invocación y activación**
   - **Responsable de su actualización**

- **Planes de acción para reanudar los procesos conforme a la estrategia seleccionada.**
- **Requerimiento de recursos**
- **Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, entre otros)**

Se deben desarrollar planes específicos considerando, por lo menos, los siguientes:

Plan de Emergencia: Plan que tiene como objetivo salvaguardar la integridad física del personal.

Plan de Recuperación de los servicios de tecnología de información: Plan que busca inicialmente restaurar los servicios de tecnología de información dentro de los parámetros establecidos, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.

8.4. Pruebas y actualización

Los planes de continuidad del negocio deberán ser probados cuando menos una vez al año. A continuación se detallan las actividades mínimas que deben ser aplicadas en esta fase:

a. **<u>Ejecución de pruebas</u>: El alcance de las pruebas debe ser consistente con el alcance de los planes de continuidad del negocio. Cada prueba debe tener objetivos definidos y un reporte que resuma los resultados alcanzados y recomendaciones. Esta información debería ser usada para mejorar los planes de continuidad del negocio en forma oportuna. Pueden aplicarse diferentes tipos de prueba, desde las pruebas de escritorio hasta las simulaciones completas de escenarios de interrupción de operaciones.**

   Las empresas deberán asegurarse que sus principales proveedores de servicios cuenten con planes de continuidad y que éstos cumplan con lo señalado en el presente numeral.

b. **<u>Actualización de los planes</u>: Las empresas deben definir políticas y procedimientos para la actualización de los planes de gestión de la continuidad del negocio, de tal manera que cualquier cambio que impacte a la empresa (ya sea interno o externo) sea revisado en relación con la continuidad del negocio.**

8.5. Integrar la gestión de la continuidad del negocio a la cultura organizacional

Las actividades mínimas a desarrollar en esta fase son las siguientes:

a. **<u>Evaluación del grado de conocimiento sobre la gestión de continuidad</u>: Tiene como objetivo determinar el nivel de conocimiento actual y esperado sobre la gestión de continuidad del negocio, los procedimientos implementados, las tareas específicas señaladas en los planes de continuidad, entre otros aspectos.**

b. **<u>Desarrollo y mejora de la cultura de continuidad</u>: Diseñar e implementar planes de capacitación y entrenamiento, a fin de cubrir las deficiencias encontradas en la actividad previa.**

c. **<u>Monitoreo permanente</u>: Revisar periódicamente el nivel de entendimiento de la gestión de continuidad del negocio a fin de identificar requerimientos adicionales.**

Documentación Sustentatoria

Artículo 9°.- Las empresas deberán mantener a disposición de la Superintendencia la documentación necesaria que permita sustentar el desarrollo de cada una de las fases y actividades descritas en el artículo anterior.

Los principales aspectos de la gestión de la continuidad del negocio, incluyendo el programa de pruebas de los planes de continuidad, serán reportados a través del aplicativo IG-ROp en el plazo establecido en el Reglamento para la Gestión del Riesgo Operacional.

Cambios significativos

Artículo 10°.- Las empresas analizarán el impacto que tienen los cambios significativos sobre la continuidad del negocio.

Los cambios significativos podrán considerar entre otros: cambio de la infraestructura tecnológica que soporta los principales productos y/o servicios, fusión con otra empresa, implementación de un nuevo producto, cambio de un proveedor principal, cambio de oficina principal, entre otros.

Auditoría Interna

Artículo 11º.- La Unidad de Auditoría Interna evaluará el cumplimiento de lo dispuesto en la presente norma de acuerdo a su plan de trabajo.

Plan de Adecuación

Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las empresas deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

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

Vigencia y Plazo de Adecuación

Artículo 13°.- La presente Circular entra en vigencia a partir del día siguiente a su publicación en el Diario Oficial El Peruano, otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010. A partir de dicha fecha, queda derogado el artículo 83° del Título III del Compendio de Normas de Superintendencia Reglamentarias del Sistema Privado de Administración de Fondos de Pensiones, referido a Gestión Empresarial.

Atentamente,

FELIPE TAM FOX

Superintendente de Banca, Seguros y

Administradoras Privadas de Fondos de Pensiones

ANEXO N° 3

Lima, 02 de abril de 2009

Resolución S.B.S.

N° 2116 -2009

El Superintendente de Banca, Seguros y

Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

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

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

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

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

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

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

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

RESUELVE:

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

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

Artículo Segundo.- Sustituir el artículo 117º 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 Nº 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 Nº 37-2008 del 10 de enero de 2008.
h. Riesgo legal: Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros.

i. Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.
j. Superintendencia: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.
k. Tolerancia al riesgo: El nivel de variación que la empresa está dispuesta a asumir en caso de desviación de los objetivos empresariales trazados.

Artículo 3°.- Riesgo operacional

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

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

Artículo 4° Factores que originan el riesgo operacional

i) Procesos internos

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

ii) Personal

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

iii) Tecnología de información

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

iv) Eventos externos

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

Artículo 5°.- Eventos de pérdida por riesgo operacional

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

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

b. Fraude externo.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c. Relaciones laborales y seguridad en el puesto de trabajo.- Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

d. Clientes, productos y prácticas empresariales.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

e. Daños a activos materiales.- Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

f. Interrupción del negocio y fallos en los sistemas.- Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

g. Ejecución, entrega y gestión de procesos.- Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

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

CAPITULO II

ROLES Y RESPONSABILIDADES

Artículo 6°.- Responsabilidades del Directorio

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

a) Definir la política general para la gestión del riesgo operacional.
b) Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiados.
c) Establecer un sistema de incentivos que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.
d) Aprobar el manual de gestión del riesgo operacional.
e) Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.
f) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.
g) Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión del riesgo operacional, y que los principales riesgos identificados se encuentran bajo control dentro de los límites que han establecido.

Artículo 7°.- Responsabilidades de la Gerencia

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

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

Artículo 8°.- Comité de riesgos
Las funciones del Comité de Riesgos señaladas en el Reglamento de la Gestión Integral de Riesgos, son de aplicación a la gestión del riesgo operacional en lo que corresponda.

Artículo 9°.- Unidad de riesgos
De conformidad con el Reglamento de la Gestión Integral de Riesgos, las empresas podrán contar con una Unidad de Riesgos centralizada o con unidades especializadas en la gestión de riesgos específicos.

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

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

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

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

CAPITULO III

LA GESTIÓN DEL RIESGO OPERACIONAL

Artículo 10°.- Manual de gestión del riesgo operacional
Las empresas deberán contar con un manual de gestión del riesgo operacional, el cual deberá contemplar por lo menos los siguientes aspectos:

a. *Políticas para la gestión del riesgo operacional.*

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

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

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

Asimismo, deberán cumplirse los siguientes criterios:

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

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

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

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

La base de datos deberá cumplir con los siguientes criterios:

a. Deben registrarse los eventos de pérdida originados en toda la empresa, para lo cual se diseñarán políticas, procedimientos de captura, y entrenamiento al personal que interviene en el proceso.

b. Debe registrarse, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas:

- Código de identificación del evento.
- Tipo de evento de pérdida (según tipos de eventos señalados en el Anexo A del presente Reglamento).
- Línea de negocio asociada, según líneas señaladas en el Anexo B del presente Reglamento para las empresas del sistema financiero, Anexo C para las empresas de seguros y Anexo D

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 A del presente Reglamento, así como a las líneas de negocio señaladas en los Anexos 2, 3 y 4. Asimismo, deben definirse criterios específicos para aquellos casos en que un evento esté asociado a más de una línea de negocio.

d. Debe definirse un monto mínimo de pérdida a partir del cual se registrará un evento en la base de datos. Al respecto, se fija un monto mínimo de 3 000 nuevos soles para los bancos, las financieras, las compañías de seguros y las AFP, y de 1 000 nuevos soles para el resto de empresas. Las empresas podrán establecer un monto mínimo inferior al indicado, teniendo en cuenta su volumen de operaciones y complejidad asociada. La Superintendencia podrá actualizar el monto mínimo definido por medio de Circular.

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

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

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

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

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

Artículo 14°.- Subcontratación

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

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

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

CAPITULO IV
REQUERIMIENTOS DE INFORMACION

Artículo 15°.- Informe a la Superintendencia

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

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

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

Artículo 16°.- Información adicional

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

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

CAPITULO V
COLABORADORES EXTERNOS

Artículo 17º.- Auditoría Interna
La Unidad de Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional, así como de lo dispuesto en el presente Reglamento, de conformidad con lo establecido en el Reglamento de Auditoría Interna.

Artículo 18º.- Auditoría Externa
Las sociedades de auditoría externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la gestión del riesgo operacional, considerando el cumplimiento de lo dispuesto en el presente Reglamento.

Artículo 19º.- Empresas Clasificadoras de Riesgo
Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la gestión del riesgo operacional en el proceso de clasificación de las empresas supervisadas.

DISPOSICIONES FINALES Y TRANSITORIAS

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

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

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

Cuarta.- Transparencia

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

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

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

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

ANEXO A

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	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,

	de la naturaleza o diseño de un producto.		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 B

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 C

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

ANEXO D

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

ANEXO N° 4

Lima, 02 de abril de 2009

Resolución S.B.S.

N° 2115 -2009

El Superintendente de Banca, Seguros y

Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, mediante el Decreto Legislativo N° 1028 se modificó la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702, en adelante Ley General, para permitir la implementación en nuestro país a partir del 1 de julio de 2009 de los estándares recomendados por el Comité de Supervisión Bancaria de Basilea referidos a medidas y normas de capital;

Que, la implementación en nuestro país de los estándares recomendados por el Comité de Supervisión Bancaria de Basilea permitirá adecuar los requerimientos de patrimonio efectivo al riesgo efectivamente asumido por las empresas;

Que, en el artículo 186° de la Ley General modificado por el Decreto Legislativo N° 1028 se establece que para el cálculo del requerimiento de patrimonio efectivo por riesgo operacional, las empresas del sistema financiero utilizarán el método del indicador básico, el método estándar alternativo o métodos avanzados;

Que, en el artículo 194° de la Ley General modificado por el Decreto Legislativo N° 1028 se dispone que las empresas del sistema financiero podrán iniciar el cálculo del requerimiento de patrimonio efectivo por riesgo operacional mediante el método del indicador básico o el método estándar alternativo. No obstante, se precisa que para el uso del método estándar alternativo se requiere previa autorización de la Superintendencia según las normas que establezca este Órgano de Control;

Que, asimismo, en el artículo 194° de la Ley General modificado por el Decreto Legislativo N° 1028 se señala que para hacer uso de los métodos avanzados se requiere, también, autorización previa de esta Superintendencia según las normas que establezca este Órgano de Control;

Que, en consecuencia, resulta necesario establecer la metodología que deberá aplicarse, así como los requisitos que deberán cumplirse, para efectuar el cálculo del requerimiento de patrimonio efectivo por riesgo operacional bajo el método del indicador básico, el método estándar alternativo o los métodos avanzados;

Que, mediante Resolución SBS N° 895-98 y sus normas modificatorias y complementarias se aprobó el Manual de Contabilidad para las Empresas del Sistema Financiero;

Que, resulta necesario modificar el Capítulo V “Información Complementaria” del Manual de Contabilidad para incorporar los Reportes correspondientes al cálculo de los requerimientos de patrimonio efectivo por riesgo operacional;

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

En uso de las atribuciones conferidas en los numerales 7, 9 y 13 del artículo 349º de la Ley General.

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operacional que forma parte integrante de la presente Resolución.

Artículo Segundo.- Modifíquese el Manual de Contabilidad para las Empresas del Sistema Financiero en los siguientes términos:

Incorpórese en el Capítulo V "Información Complementaria" los Reportes N° 2-C1 y N° 2-C2 denominados "Requerimiento de Patrimonio Efectivo por Riesgo Operacional – Método del Indicador Básico" y "Requerimiento de Patrimonio Efectivo por Riesgo Operacional – Método Estándar Alternativo", respectivamente, conforme a los formatos señalados en los Anexos 4 y 5 del Reglamento aprobado por la presente Resolución.

La remisión de dichos reportes se efectuará por medio del Submódulo de Captura y Validación Externa (SUCAVE).

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

Artículo Cuarto.- Incorpórese el procedimiento N° 124 "Autorización para utilizar el método estándar alternativo para el cálculo del requerimiento de patrimonio efectivo por riesgo operacional" en el Texto Único de Procedimientos Administrativos – TUPA de la Superintendencia de Banca, Seguros y AFP aprobado mediante Resolución SBS N° 131-2002, cuyo texto se anexa a la presente Resolución y se publica conforme lo dispuesto en el Decreto Supremo N° 004-2008-PCM, reglamento de la Ley N° 29091. (Portal institucional: www.sbs.gob.pe).

Artículo Quinto.- La presente Resolución entrará en vigencia a partir del 1 de julio de 2009.

Regístrese, comuníquese y publíquese,

FELIPE TAM FOX

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

REGLAMENTO PARA EL REQUERIMIENTO DE PATRIMONIO EFECTIVO POR RIESGO OPERACIONAL

CAPITULO I

PRINCIPIOS GENERALES

Artículo 1°.- Alcance

Las disposiciones de la presente norma son aplicables a las empresas comprendidas en los literales A y B del artículo 16° de la Ley General, al Banco de la Nación, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco Agropecuario, al Fondo MIVIVIENDA S.A. y al Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), en adelante las empresas.

Artículo 2°.- Definiciones

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

l. Casa Matriz: Se refiere a la sociedad principal o a la que ejerza el control en un conglomerado financiero o mixto.
m. 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.
n. Evento de pérdida por riesgo operacional: El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.
o. Pérdida: Es un impacto negativo en los ingresos o en el valor patrimonial de la empresa.
p. Pérdida esperada: Expectativa de pérdida que se encuentra asociada a la marcha regular del negocio.
q. Pérdida no esperada: Es la diferencia entre la máxima pérdida que enfrentaría la empresa dado un nivel de confianza estadístico asociado, y la pérdida esperada.
r. Riesgo operacional: Es la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.
s. Superintendencia: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

Artículo 3°.- Requerimiento de patrimonio efectivo por riesgo operacional[4]

Las empresas deberán destinar patrimonio efectivo para cubrir el riesgo operacional que enfrentan. Para el cálculo de dicho requerimiento patrimonial, las empresas deberán aplicar uno de los siguientes métodos:

a. Método del indicador básico
b. Método estándar alternativo

[4] Artículo sustituido mediante Resolución SBS N° 3127-2012 del 31/05/2012.

c. Métodos avanzados

El uso del método estándar alternativo o de los métodos avanzados requiere la autorización expresa de la Superintendencia.

En tanto no cuenten con la autorización señalada en el párrafo anterior, las empresas deberán aplicar el método del indicador básico.

El requerimiento de patrimonio efectivo por riesgo operacional no será mayor al 20% del requerimiento de patrimonio efectivo total (por riesgo de crédito, riesgo de mercado y riesgo operacional). Para calcular el límite de 20%, las empresas usarán la siguiente fórmula:

Requerimiento de patrimonio efectivo por riesgo operacional $\leq$ 0.25 x (Patrimonio Mín. R. Crédito + Patrimonio Mín. R. Mercado)

Donde:

Patrimonio Mín. R. Crédito: Es el requerimiento mínimo de patrimonio efectivo según el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo de Crédito.

Patrimonio Mín. R. Mercado: Es el requerimiento mínimo de patrimonio efectivo según el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo de Mercado.

Las empresas que obtengan un requerimiento de patrimonio efectivo por riesgo operacional superior a este límite al usar cualquiera de los métodos establecidos en el presente artículo, no tendrán que destinar patrimonio por el monto que exceda al mismo.

Para hallar el equivalente a los activos ponderados por riesgo (APR) en el caso de riesgo operacional, se multiplicará el requerimiento patrimonial calculado según los métodos señalados al inicio de este artículo, por la inversa del límite global que establece la Ley General en el artículo 199°.

Adicionalmente, el APR por riesgo operacional deberá ser multiplicado por un factor, cuyo valor corresponderá al indicado en la siguiente tabla:

Periodo	**Factor de ajuste**
Julio de 2009 - Junio de 2010	0,40
Julio de 2010 - Junio de 2011	0,40
Julio de 2011 – Junio de 2012	0,50
Julio de 2012 – Junio de 2013	0,60
Julio de 2013 – Junio de 2014	0,80
Julio de 2014 – En adelante	1,00

Artículo 4°.- Proceso de autorización ante la Superintendencia

Las empresas que deseen utilizar el método estándar alternativo o los métodos avanzados, deberán presentar a la Superintendencia una solicitud de autorización suscrita por el Gerente General, la cual deberá ir acompañada de los siguientes documentos:

- Copia certificada del acuerdo del Directorio u órgano social equivalente donde conste la decisión de solicitar la autorización correspondiente a la Superintendencia.
- Declaración de cumplimiento de los requisitos establecidos en el presente reglamento, adjuntando un Informe que describa la forma en que la empresa cumple con cada requisito, según el método que solicite. Dicho informe deberá presentarse conforme al formato publicado por la Superintendencia en el Portal del Supervisado, debiendo mantenerse la correspondiente información de sustento a disposición de la Superintendencia.

En el caso del método estándar alternativo, luego de recibida la solicitud con los documentos requeridos, la Superintendencia emitirá su pronunciamiento en un plazo que no excederá de sesenta (60) días útiles.

En el caso de los métodos avanzados, luego de recibida la solicitud con los documentos requeridos, la Superintendencia iniciará un proceso de validación que podrá durar hasta dos (2) años, durante el cual se realizarán cálculos paralelos del requerimiento patrimonial. Luego de culminada la validación y habiendo obtenido la autorización de la SBS para el uso del método avanzado, las empresas autorizadas deberán aplicar durante los dos (2) primeros años pisos regulatorios para el cálculo de requerimiento patrimonial. Es decir, el requerimiento patrimonial por riesgo operacional no podrá ser menor que un porcentaje del requerimiento establecido antes de la aprobación del método avanzado. Los porcentajes a aplicar serán los siguientes: 90% durante el primer año y 80% durante el segundo año.

CAPITULO II

METODO DEL INDICADOR BÁSICO

Artículo 5°.- Definición del indicador de exposición por riesgo operacional

Este método de cálculo considera como indicador de exposición el "margen operacional bruto" de la empresa, el cual se define como la suma de los ingresos financieros y los ingresos por servicios menos los gastos financieros y los gastos por servicios.

En tal sentido, para calcular el margen operacional bruto, se utilizarán las siguientes cuentas contables:

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

Para el cálculo del requerimiento patrimonial, se utilizará el saldo anualizado del margen operacional bruto, es decir, el total de margen obtenido durante los últimos 12 meses. Para ello, se utilizarán los saldos anualizados de las cuentas contables señaladas en el cuadro anterior. La anualización de los saldos se realizará conforme al procedimiento descrito en el Anexo A.

Artículo 6°.- Cálculo del requerimiento patrimonial

El requerimiento patrimonial por riesgo operacional según el método del indicador básico será equivalente al promedio de los saldos anualizados de los márgenes operacionales brutos de la empresa, considerando los últimos 3 años, multiplicado por un factor fijo.

Si el margen operacional bruto correspondiente a alguno de los tres últimos años es cero o es un número negativo, dicho(s) año(s) no debe(n) ser considerado(s) en el cálculo del promedio, en cuyo caso se calculará sobre la base del número de años cuyo margen operacional bruto sea positivo.

La fórmula de cálculo a utilizar es la siguiente:

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

donde:

R : Requerimiento patrimonial por riesgo operacional

MO_i : Saldo anualizado del margen operacional bruto correspondiente al año i, en los casos que sea positivo

α : Factor fijo igual a 15%
n : Número de años en los que el saldo anualizado del margen operacional bruto fue positivo, considerando los 3 últimos años.

Las empresas deberán presentar a la Superintendencia el cálculo del requerimiento patrimonial por riesgo operacional según el método del indicador básico en el formato señalado en el Anexo D. Esta información deberá ser remitida mensualmente vía SUCAVE en un plazo que no exceda de 15 días calendario de concluido el mes a que corresponde dicho cálculo.

Artículo 7°.- Consideraciones adicionales

Las empresas que cuenten con menos de 36 meses de operación realizarán el cálculo del requerimiento patrimonial por riesgo operacional según lo siguiente:

a) Durante los primeros 12 meses de operación, el requerimiento patrimonial será equivalente al 15% del margen operacional bruto acumulado durante el periodo en que viene operando.

   La fórmula es la siguiente:

   $R = MO \times \alpha$

   Donde:

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

   Si el margen operacional bruto acumulado es cero o negativo, el requerimiento patrimonial, según el método del indicador básico, será cero. No obstante, deberá tenerse en cuenta lo señalado en la Primera Disposición Final del presente Reglamento.

b) A partir del mes 13 y hasta el mes 23 de operación, el requerimiento patrimonial por riesgo operacional será igual al 15% del saldo anualizado del margen operacional bruto considerando sólo un período completo que incluya los últimos doce meses.

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

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

   Donde:

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

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

CAPITULO III

MÉTODO ÉSTANDAR ALTERNATIVO

Artículo 8°.- Requisitos mínimos para el uso del método estándar alternativo

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

a. El Directorio y la Gerencia General deben participar activamente en la gestión del riesgo operacional.

b. La empresa debe contar con una función de gestión del riesgo operacional cuyas responsabilidades se encuentren claramente especificadas, y que consideren como mínimo los aspectos señalados en el Reglamento para la Gestión del Riesgo Operacional.

c. La empresa debe contar con un programa de capacitación profesional dirigido a perfeccionar los conocimientos, aptitudes y otras competencias del personal especializado en la gestión del riesgo operacional.

d. La empresa debe contar con una metodología de gestión del riesgo operacional que sea conceptualmente sólida y que se encuentre implementada en su totalidad.

e. La empresa debe contar con recursos suficientes para aplicar su metodología de gestión de riesgo operacional, tanto en sus principales áreas de negocio como en sus áreas de apoyo y de control.

f. La empresa debe establecer reportes periódicos sobre su exposición al riesgo operacional, que incluyan las pérdidas importantes ocurridas, dirigidos a las gerencias de las unidades de negocio y de apoyo, gerencia general y al Directorio. La empresa debe establecer procedimientos para tomar acciones apropiadas según la información incluida en dichos reportes.

g. La empresa debe establecer procedimientos que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operacional, y debe establecer políticas para tratar los casos de incumplimiento.

h. La empresa debe establecer incentivos monetarios y no monetarios a la apropiada gestión del riesgo operacional, incluidos en el sistema de evaluación de desempeño de la Gerencia y los principales participantes en dicha gestión.

i. La empresa debe contar con una base de datos de eventos de pérdida por riesgo operacional, con las características señaladas en la normativa vigente.

j. La empresa deberá implementar un sistema de gestión de la continuidad del negocio conforme a la normativa vigente, que tenga como objetivo asegurar un nivel aceptable de operatividad de sus procesos críticos, ante eventos que puedan afectar la continuidad de sus operaciones.

k. La empresa deberá contar con un sistema de gestión de la seguridad de la información conforme a la normativa vigente, orientado a garantizar la integridad, confidencialidad y disponibilidad de su información.

l. La evaluación de la gestión del riesgo operacional deberá contar con una revisión cuando menos anual, por parte de la Unidad de Auditoría Interna. Estas revisiones deben considerar las actividades de las áreas de negocio y de apoyo, así como la función de gestión del riesgo operacional, de acuerdo a su plan de trabajo.

m. La empresa deberá contar con una revisión independiente de la gestión del riesgo operacional realizada por una sociedad de auditoría externa o una firma nacional o extranjera, que acredite contar con el conocimiento y experiencia requerida, que no se encuentre relacionada mediante vínculos de gestión o propiedad. Tratándose de una sociedad de auditoría externa, la revisión independiente deberá ser realizada por una sociedad o equipo distinto del que emitió el informe anual de los estados financieros, durante los dos años anteriores al inicio de la revisión. Cuando la revisión independiente sea efectuada por otras firmas distintas a las sociedades de auditoría externa, estas no deberán haber realizado actividades de consultoría relacionadas a la gestión del riesgo operacional en la empresa, durante los dos años anteriores al inicio de la revisión.

   El Comité de Auditoría Interna de la empresa deberá aprobar la contratación de la sociedad de auditoría externa o firma encargada de la referida revisión.

   La revisión deberá evaluar cuando menos los requisitos indicados en el presente artículo, y los criterios detallados en el informe a que hace referencia el artículo 4°, que deberá ser actualizado por la Gerencia, según la última versión publicada en el Portal del Supervisado a la fecha del inicio de la revisión.

   La revisión independiente deberá efectuarse al menos cada tres años contados desde la fecha en que se emita la Resolución de Autorización para el uso del método estándar alternativo. Sólo en los años que se realizan dichas revisiones, se puede dejar sin efecto lo requerido en el artículo 18° del Reglamento para la Gestión del Riesgo Operacional.

   Asimismo, las empresas deberán informar a la Superintendencia acerca de las revisiones independientes, cuando menos treinta (30) días antes del inicio de la revisión. La Superintendencia podrá solicitar que dicha revisión incluya procedimientos extendidos en las áreas que estime necesarias, asociadas a la gestión del riesgo operacional, de seguridad de información y de continuidad del negocio. Adicionalmente, podrá solicitar en cualquier momento, adelantar la revisión esperada dentro del ciclo de tres años previstos.[5]

Artículo 9°.- Determinación de líneas de negocio

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

Línea de negocio	Definición
Finanzas corporativas	Realización de operaciones de financiamiento estructurado y participación en procesos de titulización; underwriting; asesoramiento financiero a empresas corporativas, grandes y

[5] Literal modificado por la Resolución SBS N° 13525-2010 del 20/10/2010.

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

Artículo 10°.- Definición de los indicadores de exposición por riesgo operacional

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

a. **Indicador de exposición para las líneas de negocio distintas a banca comercial y banca minorista:**
   Para estas líneas de negocio se utilizará como indicador de exposición al margen operacional anualizado de cada línea. Para ello, debe utilizarse la siguiente fórmula:

   $IE_i = Ingresos_i – Gastos_i$

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

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

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

- Para la información correspondiente a enero-junio 2010, así como para la información correspondiente al año 2009 y anteriores se utilizará la agrupación de cuentas establecida en el Anexo B1 del presente Reglamento.
- Para la información correspondiente a julio 2010 y siguientes se utilizará la agrupación de cuentas establecida en el Anexo B2 del presente Reglamento. [6]

b. Indicador de exposición para las líneas de banca comercial y banca minorista:

Para estas líneas de negocio se utilizará como indicador de exposición el saldo de los créditos y las inversiones, multiplicado por un factor fijo.

Para su cálculo, deberán considerarse los saldos de créditos e inversiones durante los últimos 12 meses, conforme a la siguiente fórmula:

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

Donde:

IE: Indicador de exposición anual para la línea de negocio banca comercial o banca minorista

m: 0,035 (Factor fijo)

C_i: Monto del saldo de créditos e inversiones para el mes i para Banca Comercial o Banca Minorista, según corresponda.

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

- Para la información correspondiente a enero-junio 2010, así como para la información correspondiente al año 2009 y anteriores se utilizará la agrupación de cuentas establecida en el Anexo B1 del presente Reglamento.
- Para la información correspondiente a julio 2010 y siguientes se utilizará la agrupación de cuentas establecida en el Anexo B2 del presente Reglamento.[7]

[6] Párrafo modificado por la Resolución SBS N° 14353-2009 del 30/10/2009
[7] Párrafo modificado por la Resolución SBS N° 14353-2009 del 30/10/2009

Artículo 11°.- Cálculo del requerimiento patrimonial

Se obtienen los indicadores de exposición correspondientes a cada una de las líneas de negocio para los 3 últimos años, y luego éstos son multiplicados por un factor fijo (β) asociado con cada línea según se muestra en el siguiente cuadro:

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

Luego, para cada uno de los años se suman los valores obtenidos para cada línea de negocio (6 valores por cada año). Finalmente, se obtiene el promedio de las sumas obtenidas. El promedio resultante constituirá el requerimiento patrimonial por riesgo operacional.

Si la suma de los productos para un año determinado resulta ser negativa, entonces se considerará el valor de 0 para ese año, en el cálculo del promedio.

El siguiente cuadro muestra el procedimiento de cálculo:

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

Donde:

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

Si : Suma de los productos obtenidos para el año i

Las empresas deberán presentar a la Superintendencia el cálculo del requerimiento patrimonial por riesgo operacional según el método estándar alternativo en el formato señalado en el Anexo 5. Esta información deberá ser remitida mensualmente vía SUCAVE en un plazo que no exceda de 15 días calendario de concluido el mes a que corresponde dicho cálculo.

Artículo 12°.- Consideraciones adicionales

Las empresas que cuenten con menos de 36 meses de operación al momento de utilizar el método estándar alternativo, realizarán el cálculo del requerimiento patrimonial por riesgo operacional según lo siguiente:

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

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

En este caso, el requerimiento patrimonial será equivalente a la suma de los resultados del producto de los factores fijos (β) señalados en el artículo 11° del presente Reglamento por los indicadores de exposición calculados conforme a lo señalado al inicio de este párrafo.

La fórmula es la siguiente:

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

Donde:

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

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

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

CAPITULO IV

MÉTODOS AVANZADOS

Artículo 13°.- Métodos avanzados

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

Artículo 14°.- Uso parcial de los métodos avanzados

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

- El uso de ambos métodos, en conjunto, tiene como alcance la totalidad de las operaciones de la empresa.
- Se satisfacen los requisitos para acceder a métodos avanzados para aquellas operaciones que serán consideradas en la aplicación del método avanzado seleccionado; de igual manera, se satisfacen los requisitos del método estándar alternativo a utilizar en las demás operaciones.
- En la fecha de aplicación del método avanzado, una parte significativa del riesgo operacional de la empresa está recogida en dicho método.
- La empresa presenta a la Superintendencia un plan que especifique el calendario a seguir para aplicar el método avanzado en todas las operaciones de la empresa (con excepción de aquellas poco significativas).

Artículo 15°.- Requisitos mínimos para el uso de métodos avanzados

Las empresas que deseen emplear los métodos avanzados deberán cumplir con los requisitos cualitativos y cuantitativos establecidos en los artículos 16° y 17° del presente Reglamento.

Artículo 16°.- Requisitos cualitativos

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

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

b) El sistema de medición del riesgo operacional de la empresa deberá estar integrado a sus procesos habituales de gestión de riesgos. La información que se obtenga de dicho sistema deberá ser utilizada como parte integral del proceso de monitoreo y control del perfil de riesgo operacional de la empresa. En ese sentido, esta información deberá ser incorporada en los

reportes sobre riesgos, reportes a la gerencia, la asignación de capital y el análisis de riesgos. La empresa deberá implantar técnicas para asignar capital por riesgo operacional a sus principales líneas de negocio y para establecer incentivos para la mejora de la gestión de estos riesgos en toda la entidad.

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

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

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

f) La revisión del sistema de medición del riesgo operacional que lleven a cabo los auditores externos deberá verificar que los procesos de validación interna operen de manera satisfactoria y que el flujo y el procesamiento de datos asociados al sistema de medición del riesgo sean transparentes y accesibles.

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

h) Otros que determine la Superintendencia.

Artículo 17°.- Requisitos cuantitativos

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

a) Criterio de solidez

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

b) Criterios detallados

1. El sistema interno de medición del riesgo operacional deberá ser consistente con el alcance de la definición de riesgo operacional señalada en la normativa emitida por la Superintendencia, y con los tipos de eventos de pérdida definidos en el Anexo Nº 3 de la presente norma.

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

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

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

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

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

c) Datos internos

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

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

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

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

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

   - Los datos internos de pérdida de la empresa deberán ser completos, es decir, deben incluir la totalidad de las actividades y exposiciones importantes existentes en todos los subsistemas y todas las ubicaciones geográficas asociadas. La empresa deberá ser capaz de justificar que las actividades o exposiciones excluidas, tanto en forma individual como conjunta, no tienen un efecto significativo sobre las estimaciones generales de riesgo. La empresa deberá establecer un umbral mínimo adecuado de pérdida bruta para la recopilación de datos internos de pérdida.

   - Además del dato referido al monto de la pérdida bruta, la empresa deberá recopilar datos sobre la fecha del evento de pérdida, cualquier recuperación del monto de la pérdida bruta, así como información descriptiva acerca de las causas del evento de pérdida. El nivel de detalle de la información descriptiva deberá estar en proporción con la cantidad de la pérdida bruta.

   - La empresa deberá desarrollar criterios específicos para la asignación de datos de pérdidas procedentes de: (a) eventos sucedidos en una función centralizada (por ejemplo, en un departamento de tecnologías de información); (b) eventos relacionados con una actividad que incluya más de una línea de negocio; y (c) eventos relacionados a lo largo del tiempo.

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

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

d) Datos externos

El sistema de medición del riesgo operacional de la empresa deberá utilizar datos externos relevantes (ya sean datos públicos y/o datos agregados del sector), especialmente cuando existan motivos para creer que la empresa está expuesta a pérdidas poco frecuentes, pero potencialmente severas. Estos datos externos deberán incluir información sobre el monto real de la pérdida, el volumen de operaciones de la entidad donde se produjo el evento de pérdida, las causas y circunstancias de los eventos de pérdida y cualquier otra información que permita evaluar la importancia del evento de pérdida para otras empresas. La empresa deberá contar con un proceso sistemático para determinar las situaciones en las que deberán utilizarse los datos externos y las metodologías utilizadas para incorporar estos datos (por ejemplo, aplicación de ajustes por tamaño, ajustes cualitativos o en el desarrollo de mejoras en el análisis de escenarios). Las condiciones y prácticas para el uso de los datos externos deberán ser revisadas anualmente, documentadas y sometidas a revisiones periódicas independientes a la empresa o su grupo de control.

e) Análisis de escenarios

La empresa deberá utilizar análisis de escenarios basados en las opiniones de expertos, junto con datos externos, para evaluar su exposición a pérdidas severas. Este enfoque se apoya en el conocimiento de gerentes experimentados y de expertos en gestión de riesgos para obtener evaluaciones razonables de las pérdidas severas que podría sufrir la entidad. Las evaluaciones realizadas por los expertos podrían ser expresadas como parámetros de una distribución estadística estimada de las pérdidas. Además, el análisis de escenarios debe utilizarse para evaluar el impacto de las desviaciones que se produzcan respecto a los supuestos de correlación incorporados en el sistema de medición del riesgo operacional de la empresa, en particular, para evaluar las pérdidas potenciales procedentes de eventos simultáneos de pérdida. Estas evaluaciones deben ser validadas y revisadas a través de su comparación con la experiencia real de pérdidas, con el fin de asegurar su razonabilidad.

f) Factores del entorno de negocio y de control interno

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

- La elección de cada factor deberá ser justificada por su influencia significativa en la exposición o mitigación del riesgo, sobre la base de la experiencia e incluyendo la opinión experta del personal de las áreas de negocio afectadas. Cuando sea posible, los factores deben traducirse en medidas cuantitativas que permitan su verificación.

- Deberá considerarse adecuadamente la sensibilidad de las estimaciones de riesgo de la empresa ante variaciones en los factores y su peso relativo. Además de identificar las variaciones en el

riesgo debido a mejoras en los controles, la metodología también debe identificar incrementos potenciales del riesgo atribuibles a una mayor complejidad de las actividades o a un incremento en el volumen de negocios.

- La metodología y cada elemento de su aplicación, incluidos los supuestos que sustenten cualquier ajuste a las estimaciones empíricas, deberán ser documentados y sometidos a revisiones independientes por parte de la empresa.

- El proceso y los resultados obtenidos deberán ser validados mediante su comparación con la experiencia real de pérdidas internas, con datos externos relevantes y con los ajustes oportunos introducidos.

Artículo 18°.- Reconocimiento de los seguros

Las empresas que estén autorizadas a aplicar un método avanzado podrán reconocer el efecto reductor del riesgo que generan los seguros en el cálculo del requerimiento patrimonial por riesgo operacional. Dicho reconocimiento se limitará al 20% del requerimiento patrimonial calculado con dicho método avanzado.

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

a) El proveedor del seguro deberá contar con una clasificación de riesgo apropiada, y haber tenido dicha clasificación durante los dos semestres anteriores, de acuerdo con lo siguiente:

   - Si el proveedor del seguro se encuentra establecido en el país, la clasificación mínima aceptable será "A", otorgada por empresas debidamente registradas en la Superintendencia y en la Comisión Nacional Supervisora de Empresas y Valores (CONASEV).
   - Si el proveedor del seguro no se encuentra establecido en el país, la clasificación mínima aceptable será la "BBB-" de Standard & Poor's o equivalente, otorgada por empresas clasificadoras de riesgo del exterior de primera categoría que cuenten con autorización de funcionamiento en alguno de los países que conforman el G10.
   - Si existiera discrepancia entre diferentes clasificaciones otorgadas al proveedor del seguro, debe considerarse la más conservadora.

b) Los contratos de seguro a considerar deberán tener un plazo de vencimiento no menor de un año. Para contratos que tengan un plazo residual de vencimiento inferior a un año, la empresa deberá aplicar los descuentos proporcionales necesarios que reflejen el plazo residual decreciente del contrato, hasta un recorte completo del 100% para contratos con un plazo residual de 90 días o menos.

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

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

puede excluir la cobertura de multas u otras penalidades ocasionadas por la acción de la Superintendencia.

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

f) El proveedor del seguro deberá ser un tercero. En el caso de seguros brindados por empresas del mismo grupo económico, la exposición deberá estar reasegurada por un tercero independiente que satisfaga los criterios de admisión señalados anteriormente.

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

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

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

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

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

DISPOSICIONES FINALES

Primera.- Requerimiento adicional
La Superintendencia podrá exigir a las empresas un requerimiento patrimonial mayor al calculado con el método al que la empresa ha sido autorizada a utilizar cuando los niveles de requerimiento de patrimonio efectivo no resulten adecuados a la naturaleza y escala de las operaciones, perfil de riesgo y sistema de gestión de riesgos de la empresa.

Segunda.- Revocatoria de autorización
Si la Superintendencia determina que una empresa que ha sido autorizada a utilizar el método estándar alternativo o los métodos avanzados, deja de satisfacer los requisitos de autorización asociados con dicho método, podrá revocar la autorización otorgada y exigirle que utilice un método más simple para algunas o todas sus operaciones, hasta que cumpla con las condiciones estipuladas por la Superintendencia para poder volver al método del que fuera revocado, lo que se comunicará mediante Oficio.

Tercera.- Vigencia
La presente norma entrará en vigencia el 1 de julio de 2009. Para la aplicación del método estándar alternativo a partir de dicha fecha, las empresas podrán presentar su solicitud de autorización de conformidad con lo señalado en la presente norma, a partir de su publicación.

ANEXO A

ANUALIZACIÓN DE SALDOS

La anualización se deberá aplicar a los saldos de las cuentas de ingresos y gastos que se requieran para el cálculo del requerimiento de patrimonio efectivo por riesgo operacional según los métodos del Indicador Básico y Estándar Alternativo, conforme a lo establecido en la presente norma.

La fórmula es la siguiente:

Saldo anualizado (j, i) = Saldo (j,i) + Saldo (diciembre, i-1) – Saldo (j,i-1)
Donde:

j: mes
i: año

Así por ejemplo, si en julio de 2009, se desea calcular los márgenes operacionales brutos correspondientes a los últimos 3 años bajo el método del indicar básico, se deberán obtener previamente los saldos anualizados de las cuentas contables señaladas en el artículo 5° del presente Reglamento, de la siguiente manera:

Saldo anualizado (julio, 2009) = Saldo (julio, 2009) + Saldo (diciembre, 2008) – Saldo (julio, 2008)

Saldo anualizado (julio, 2008) = Saldo (julio, 2008) + Saldo (diciembre, 2007) – Saldo (julio, 2007)

Saldo anualizado (julio, 2007) = Saldo (julio, 2007) + Saldo (diciembre, 2006) – Saldo (julio, 2006)

ANEXO N° 2A

CALCULO DE LOS INDICADORES DE EXPOSICIÓN DE LAS LÍNEAS DE NEGOCIO

(Hasta el 31 de diciembre de 2009) [8]

[8] En concordancia con lo establecido en la Resolución SBS N° 14353-2009 del 30/10/2009, el Anexo N° 2A tendrá vigencia hasta el 30 de junio de 2010.

Líneas de negocio distintas a banca comercial y banca minorista

Para obtener los ingresos y gastos de los últimos 12 meses por cada línea de negocio, deben sumarse los saldos anualizados de las siguientes cuentas del Manual de Contabilidad, según corresponda a cada línea de negocio[9]:

Ingresos

Línea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
Finanzas corporativas	Intereses por créditos sindicados	5104.01.01.13
	Ing. por op. contingentes: contratos de underwriting Ing. por servicios financieros diversos: suscripción y colocaciones garantizadas de valores	5201.08 + 5202.24
	Ing. por servicios financieros diversos: asesoría financiera	5202.15
Negociación y ventas	Intereses por disponibles	5101
	Intereses y comisiones por fondos interbancarios	5102 + 5107.02
	Ingresos por inversiones a valor razonable con cambios en resultados y commodities	5103.01 + 5103.02 + 5103.06
	Diferencia de cambio	5108
	Reajuste por indexación	5109.01
	Ingresos por valorización de inversiones a valor razonable con cambios en resultados, commodities, productos financieros derivados y obligaciones relacionadas con inversiones negociables y a vencimiento	5109.11 + 5109.12 + 5109.15 + 5109.16 + 5109.17 + 5109.18
	Otros ingresos	5109.21 + 5109.24
	Ingresos por servicios financieros diversos: compraventa de ME (spot y futuro)	5202.18 + 5202.19

[9] El procedimiento para anualizar saldos es descrito en el Anexo N° 1 del presente Reglamento.

Línea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
	Ingresos por servicios financieros diversos: otros inst. financieros derivados	5202.25
Liquidación y pagos	Ingresos por servicios financieros diversos: cobranzas	5202.02
	Ingresos por servicios financieros diversos: giros	5202.07
	Ingresos por servicios financieros diversos: transferencias	5202.08
	Ingresos por servicios financieros diversos: órdenes de pago	5202.12
	Ingresos por servicios financieros diversos: cobro de tributos	5202.16
Otros servicios	Ingresos de cuentas por cobrar	5105
	Comisiones por cuentas por cobrar y otros	5107.05 + 5107.09
	Otros ingresos financieros diversos	5109.19
	Ingresos por operaciones contingentes: litigios, demandas pendientes y otras contingencias	5201.09
	Ingresos por servicios financieros diversos: custodia de valores, alquiler de cajas de seguridad	5202.03+5202.13
	Ingresos por servicios financieros diversos: fideicomisos y comisiones de confianza	5202.04 + 5202.05
	Ing. por servicios financieros diversos: estudios técnicos y legales	5202.14
	Ingresos por servicios financieros diversos: compraventa de valores	5202.17
	Ingresos por servicios financieros diversos: servicios de caja	5202.21
	Otros ingresos por servicios financieros diversos	5202.29
	Ingresos por arrendamientos	5203
	Ventas de bienes y servicios	5700

Gastos

Línea de negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
Negociación y ventas	Intereses y fluctuación de obligaciones relacionadas con inversiones negociables y a vencimiento	4101.05 + 4109.18
	Intereses por fondos interbancarios	4102
	Comisiones por fondos interbancarios	4107.02
	Diferencia de cambio y rendimiento aleatorio	4108 + 4109.02
	Reajuste por indexación	4109.01
	Gastos por valorización de inversiones a valor razonable con cambios en resultados y commodities	4109.11 + 4109.12 + 4109.15
	Fluctuación de valor de productos financieros derivados y otros	4109.16 + 4109.17 + 4109.21 + 4109.24
	Gastos por servicios financieros diversos: compraventa de ME (spot y futuro)	4202.10 + 4202.11
	Gastos por servicios financieros diversos: otros instrumentos financieros derivados	4202.25

Para calcular los gastos de las demás líneas de negocio, se utilizará un factor de ponderación por cada línea, que permitirá obtener un monto aproximado de los gastos. Dicho factor se calculará de la siguiente manera:

$F_i = I_i / TI$

Donde:

F_i : Factor de ponderación de la línea i

I_i : Ingresos anualizados de la línea i, según distribución de cuentas contables señalada en la sección anterior.

TI : Total de ingresos calculados de la siguiente forma: Ingresos financieros (cuenta 5100) más los ingresos por servicios (cuentas 5200 + 5700) menos los ingresos de la línea Negociación y ventas. Se utilizarán los saldos anualizados de las cuentas contables señaladas.

Para estimar los gastos de cada línea, se aplicará la siguiente fórmula:

$G_i = F_i * TG$

Donde:

G_i : Gastos anualizados de la línea i

F_i : Factor de ponderación de la línea i

TG : Total de gastos calculados de la siguiente forma: gastos financieros (cuenta 4100) más gastos por servicios (4200 + 4900) menos los gastos de la línea Negociación y ventas. Se utilizarán los saldos anualizados de las cuentas contables señaladas.

Banca comercial

Banca Comercial	Cuentas
Créditos Comerciales	1401.01+ 1403.01 + 1404.01 + 1405.01+ 1406.01
Menos Sindicados	1401.01.13 + 1404.01.13 + 1405.01.13 + 1405.01.19.13 + 1406.01.13 + 1406.01.19.13
Menos Ingresos Diferidos	2901.01 + 2901.02 + 2901.04.01.01 + 2901.04.01.04 + 2901.04.03.01 + 2901.04.03.04 + 2901.04.04.01 + 2901.04.04.04 + 2901.04.05.01 + 2901.04.05.04 + 2901.04.06.01 + 2901.04.06.04
Más Inversiones Disponibles para la Venta e Inversiones a Vencimiento	1303+1304+1305
Más Inversiones en Subsidiarias y Asociadas	1700

Banca minorista

Banca Minorista	Cuentas
Créditos MES, Consumo e Hipotecarios para Vivienda	1401 - 1401.01+ 1403 - 1403.01 + 1404 - 1404.01 + 1405 - 1405.01+ 1406 - 1406.01
Menos Ingresos Diferidos	2901.04 - 2901.04.01.01 - 2901.04.01.04 - 2901.04.03.01 - 2901.04.03.04 - 2901.04.04.01 - 2901.04.04.04 - 2901.04.05.01 - 2901.04.05.04 - 2901.04.06.01 - 2901.04.06.04

ANEXO N° 2B

CÁLCULO DE LOS INDICADORES DE EXPOSICIÓN DE LAS LÍNEAS DE NEGOCIO[10]

(A partir del 01 de julio de 2010)

Líneas de negocio distintas a banca comercial y banca minorista

Para obtener los ingresos y gastos de los últimos 12 meses por cada línea de negocio, deben sumarse los saldos anualizados de las siguientes cuentas del Manual de Contabilidad, según corresponda a cada línea de negocio[11]:

Ingresos

Línea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
Finanzas corporativas	Ing. por financiación estructurada[12]	5104.01.10.30 + 5104.01.10.31 + 5104.01.10.32 + 5104.01.10.33 + 5104.01.10.34 + 5104.01.11.30 + 5104.01.11.31 + 5104.01.11.32 + 5104.01.11.33 + 5104.01.11.34 +5104.01.12.30 + 5104.01.12.31 + 5104.01.12.32 + 5104.01.12.33 + 5104.01.12.34
	Ing. por op. contingentes: contratos de underwriting Ing. por servicios financieros diversos: suscripción y colocaciones garantizadas de valores	5201.08 + 5202.24

[10] Denominación modificada por la Resolución SBS N° 14353-2009 del 30/10/2009

[11] El procedimiento para anualizar saldos es descrito en el Anexo N° 1 del presente Reglamento.

[12] Subcuentas analíticas incorporadas por la Resolución SBS N° 14353-2009 del 30/10/2009.

Línea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
	Ing. por servicios financieros diversos: asesoría financiera	5202.15
Negociación y ventas	Intereses por disponibles	5101
	Intereses y comisiones por fondos interbancarios	5102 + 5107.02
	Ingresos por inversiones a valor razonable con cambios en resultados y commodities	5103.01 + 5103.02 + 5103.06
	Diferencia de cambio	5108
	Reajuste por indexación	5109.01
	Ingresos por valorización de inversiones a valor razonable con cambios en resultados, commodities, productos financieros derivados y obligaciones relacionadas con inversiones negociables y a vencimiento	5109.11 + 5109.12 + 5109.15 + 5109.16 + 5109.17 + 5109.18
	Otros ingresos	5109.21 + 5109.24
	Ingresos por servicios financieros diversos: compraventa de ME (spot y futuro)	5202.18 + 5202.19
	Ingresos por servicios financieros diversos: otros inst. financieros derivados	5202.25
Liquidación y pagos	Ingresos por servicios financieros diversos: cobranzas	5202.02
	Ingresos por servicios financieros diversos: giros	5202.07
	Ingresos por servicios financieros diversos: transferencias	5202.08
	Ingresos por servicios financieros diversos: órdenes de pago	5202.12
	Ingresos por servicios financieros diversos: cobro de tributos	5202.16
Otros servicios	Ingresos de cuentas por cobrar	5105
	Comisiones por cuentas por cobrar y otros	5107.05 + 5107.09
	Otros ingresos financieros diversos	5109.19
	Ingresos por operaciones contingentes: litigios, demandas pendientes y otras contingencias	5201.09
	Ingresos por servicios financieros diversos: custodia de valores, alquiler de cajas de seguridad	5202.03+5202.13

Línea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
	Ingresos por servicios financieros diversos: fideicomisos y comisiones de confianza	5202.04 + 5202.05
	Ing. por servicios financieros diversos: estudios técnicos y legales	5202.14
	Ingresos por servicios financieros diversos: compraventa de valores	5202.17
	Ingresos por servicios financieros diversos: servicios de caja	5202.21
	Otros ingresos por servicios financieros diversos	5202.29
	Ingresos por arrendamientos	5203
	Ventas de bienes y servicios	5700

Gastos

Línea de negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
Negociación y ventas	Intereses y fluctuación de obligaciones relacionadas con inversiones negociables y a vencimiento	4101.05 + 4109.18
	Intereses por fondos interbancarios	4102
	Comisiones por fondos interbancarios	4107.02
	Diferencia de cambio y rendimiento aleatorio	4108 + 4109.02
	Reajuste por indexación	4109.01
	Gastos por valorización de inversiones a valor razonable con cambios en resultados y commodities	4109.11 + 4109.12 + 4109.15
	Fluctuación de valor de productos financieros derivados y otros	4109.16 + 4109.17 + 4109.21 + 4109.24
	Gastos por servicios financieros diversos: compraventa de ME (spot y futuro)	4202.10 + 4202.11
	Gastos por servicios financieros diversos: otros instrumentos financieros derivados	4202.25

Para las demás líneas de negocio se deberá aplicar una fórmula que permita obtener un monto aproximado de los gastos. Para ello, se utilizará un factor de ponderación por cada línea, el cual se calculará de la siguiente manera:

$F_i = I_i / TI$

Donde:

F_i : Factor de ponderación de la línea i

I_i : Ingresos anualizados de la línea i, según distribución de cuentas contables señalada en la sección anterior.

TI : Total de ingresos calculados de la siguiente forma: Ingresos financieros (cuenta 5100) más los ingresos por servicios (cuentas 5200 + 5700) menos los ingresos de la línea Negociación y ventas. Se utilizarán los saldos anualizados de las cuentas contables señaladas.

Para estimar los gastos de cada línea, se aplicará la siguiente fórmula:

$G_i = F_i * TG$

Donde:

G_i : Gastos anualizados de la línea i

F_i : Factor de ponderación de la línea i

TG : Total de gastos calculados de la siguiente forma: gastos financieros (cuenta 4100) más gastos por servicios (4200 + 4900) menos los gastos de la línea Negociación y ventas. Se utilizarán los saldos anualizados de las cuentas contables señaladas.

Banca comercial

Banca Comercial	Cuentas
Créditos a Bancos Multilaterales de Desarrollo	1401.05 + 1404.05 + 1405.05 + 1406.05
Créditos Soberanos	1401.06 + 1404.06 + 1405.06 + 1406.06
Créditos a Entidades del Sector Público	1401.07 + 1403.07 + 1404.07 + 1405.07 + 1406.07
Créditos a Intermediarios de Valores	1401.08 + 1403.08 + 1404.08 + 1405.08 + 1406.08
Créditos a Empresas del Sistema Financiero	1401.09 + 1404.09 + 1405.09 + 1406.09
Créditos Corporativos	1401.10 + 1403.10 + 1404.10 + 1405.10 + 1406.10
Créditos a Grandes Empresas	1401.11 + 1403.11 + 1404.11 + 1405.11 + 1406.11
Créditos a Medianas Empresas	1401.12 + 1403.12 + 1404.12 + 1405.12 + 1406.12

Menos Financiación Estructurada[13]	1401.10.30 + 1401.10.31 + 1401.10.32 + 1401.10.33 + 1401.10.34 + 1401.11.30 + 1401.11.31 + 1401.11.32 + 1401.11.33 + 1401.11.34 + 1401.12.30 + 1401.12.31 + 1401.12.32 + 1401.12.33 + 1401.12.34 + 1403.10.30 + 1403.10.31 + 1403.10.32 + 1403.10.33 + 1403.10.34 + 1403.11.30 + 1403.11.31 + 1403.11.32 + 1403.11.33 + 1403.11.34 + 1403.12.30 + 1403.12.31 + 1403.12.32 + 1403.12.33 + 1403.12.34 + 1404.10.30 + 1404.10.31 + 1404.10.32 + 1404.10.33 + 1404.10.34 + 1404.11.30 + 1404.11.31 + 1404.11.32 + 1404.11.33 + 1404.11.34 + 1404.12.30 + 1404.12.31 + 1404.12.32 + 1404.12.33 + 1404.12.34 + 1405.10.19.30 + 1405.10.19.31 + 1405.10.19.32 + 1405.10.19.33 + 1405.10.19.34 + 1405.10.30+ 1405.10.31 + 1405.10.32 + 1405.10.33 + 1405.10.34 + 1405.11.19.30 + 1405.11.19.31 + 1405.11.19.32 + 1405.11.19.33 + 1405.11.19.34 + 1405.11.30 + 1405.11.31 + 1405.11.32 + 1405.11.33 + 1405.11.34 + 1405.12.19.30 + 1405.12.19.31 + 1405.12.19.32 + 1405.12.19.33 + 1405.12.19.34 + 1405.12.22.30 + 1405.12.22.31 + 1405.12.22.32 + 1405.12.22.33 + 1405.12.22.34 + 1405.12.30 + 1405.12.31 + 1405.12.32 + 1405.12.33 + 1405.12.34 + 1406.10.19.30 + 1406.10.19.31 + 1406.10.19.32 + 1406.10.19.33 + 1406.10.19.34 + 1406.10.30+ 1406.10.31 + 1406.10.32 + 1406.10.33 + 1406.10.34 + 1406.11.19.30 + 1406.11.19.31 + 1406.11.19.32 + 1406.11.19.33 + 1406.11.19.34 + 1406.11.30 + 1406.11.31 + 1406.11.32 + 1406.11.33 + 1406.11.34 + 1406.12.19.30 + 1406.12.19.31 + 1406.12.19.32 + 1406.12.19.33 + 1406.12.19.34 + 1406.12.30 + 1406.12.31 + 1406.12.32 + 1406.12.33 + 1406.12.34
Menos Ingresos Diferidos	2901.01 + 2901.02 + 2901.04.01.03 + 2901.04.01.04 + 2901.04.01.05 + 2901.04.01.06 + 2901.04.01.07 + 2901.04.01.08 + 2901.04.01.12 + 2901.04.01.13 + 2901.04.01.14 + 2901.04.01.15 + 2901.04.01.16 + 2901.04.01.17 + 2901.04.03.03 + 2901.04.03.04 + 2901.04.03.05 + 2901.04.03.06 + 2901.04.03.07 + 2901.04.03.08 + 2901.04.03.12 + 2901.04.03.13 + 2901.04.03.14 + 2901.04.03.15 + 2901.04.03.16 + 2901.04.03.17 + 2901.04.04.03 + 2901.04.04.04 + 2901.04.04.05 + 2901.04.04.06 + 2901.04.04.07 + 2901.04.04.08 + 2901.04.04.12 + 2901.04.04.13 + 2901.04.04.14 + 2901.04.04.15 + 2901.04.04.16 + 2901.04.04.17 + 2901.04.05.03 + 2901.04.05.04 + 2901.04.05.05 + 2901.04.05.06 + 2901.04.05.07 + 2901.04.05.08 + 2901.04.05.12 + 2901.04.05.13 + 2901.04.05.14 + 2901.04.05.15 + 2901.04.05.16 + 2901.04.05.17 + 2901.04.06.03 + 2901.04.06.04 + 2901.04.06.05 + 2901.04.06.06 + 2901.04.06.07 + 2901.04.06.08 + 2901.04.06.12 +

[13] Cuentas analíticas y subcuentas analíticas incorporadas por la Resolución SBS N° 14353-2009 del 30/10/2009.

	2901.04.06.13 + 2901.04.06.14 + 2901.04.06.15 + 2901.04.06.16 + 2901.04.06.17
Más Inversiones Disponibles para la Venta e Inversiones a Vencimiento	1303+1304+1305
Más Inversiones en Subsidiarias y Asociadas	1700

Banca minorista

Banca Minorista	Cuentas
Créditos a Microempresas	1401.02 + 1403.02 + 1404.02 + 1405.02 + 1406.02
Créditos de Consumo Revolventes y No-Revolventes	1401.03 + 1404.03 + 1405.03 + 1406.03
Créditos Hipotecarios para Vivienda	1401.04 + 1404.04 + 1405.04 + 1406.04
Créditos a Pequeñas Empresas	1401.13 + 1403.13 + 1404.13 + 1405.13 + 1406.13
Menos Ingresos Diferidos	2901.04.01.01 + 2901.04.01.02 + 2901.04.01.09 + 2901.04.01.10 + 2901.04.01.11 + 2901.04.01.18 + 2901.04.03.01 + 2901.04.03.09 + 2901.04.03.10 + 2901.04.03.18 + 2901.04.04.01 + 2901.04.04.02 + 2901.04.04.09 + 2901.04.04.10 + 2901.04.04.11 + 2901.04.04.18 + 2901.04.05.01 + 2901.04.05.02 + 2901.04.05.09 + 2901.04.05.10 + 2901.04.05.11 + 2901.04.05.18 + 2901.04.06.01 + 2901.04.06.02 + 2901.04.06.09 + 2901.04.06.10 + 2901.04.06.11 + 2901.04.06.18

ANEXO C

TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Tipo de evento	Definición	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 (realizadas intencionalmente), robo, malversación, falsificación, soborno, apropiación de cuentas.
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, falsificación, daños por ataques informáticos, robo de información.
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad o discriminación.	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos; casos relacionados con las normas de higiene y seguridad en el trabajo; indemnización a los trabajadores.
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.	Incumplimiento de los contratos con los clientes, divulgación de información privada de clientes, abuso de información confidencial, incumplimiento de las normas de conocimiento del cliente, prácticas restrictivas de la competencia, manipulación del mercado, lavado de dinero, publicidad impropia, defectos en el producto o servicio.
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo).
Interrupción del negocio y fallos en los sistemas	Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas	Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.

Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Ejecución errónea de modelos, errores contables, fallo en la gestión de las garantías, incumplimiento en el envío de reportes obligatorios, reportes inexactos, incumplimiento de normas tributarias, registros incorrectos de clientes, litigios con proveedores.