UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL

MODELO DE GESTIÓN DEL RIESGO OPERACIONAL DE UN BANCO: ANÁLISIS DIAGNÓSTICO SEGÚN EL COMITÉ DE BASILEA

TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN GESTIÓN Y DIRECCIÓN DE EMPRESAS

JOSÉ IGNACIO AGUILAR BELMAR

PROFESOR GUÍA:
ENRIQUE JEHOSUA JOFRE ROJAS

MIEMBROS DE LA COMISIÓN:
ANTONIO AGUSTÍN HOLGADO SAN MARTÍN
GERARDO OCTAVIO DÍAZ RODENAS

SANTIAGO DE CHILE
2015

RESUMEN

Las pérdidas por riesgo operacional en las instituciones financieras representan a toda pérdida por fallas derivadas de las personas, sistemas, procesos o factores externos, donde se incluye el riesgo legal y se excluye el riesgo estratégico y el de reputación.

Esta definición si bien tiene más de una década, aún presenta diversas dificultades en su aplicación y gestión dentro de las instituciones tanto chilenas como extranjeras, siendo países como España en Europa y Colombia en Sudamérica los que llevan la delantera en este tema de alta complejidad.

A través de un diagnóstico de la organización analizada, identificando principalmente las mayores brechas con respecto a las mejores prácticas de Basilea II, lo dispuesto por la Ley general de bancos y la Superintendencia de Bancos e Instituciones Financieras, este trabajo, primero ejecuta la Matriz de Gestión y Solvencia y posteriormente propone un modelo de gestión de riesgo operacional y de una metodología para llevar los distintos ámbitos a procesos de estandarización de datos y procesos para ofrecer garantías frente a la exposición al riesgo operacional y aportar en la utilización del método avanzado del VaROp (AMA) que a través del modelo interno de cálculo, permite reducir en un porcentaje importante el cálculo realizado a través del método de Indicador Básico (BIA).

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES Y GRÁFICOS

1. INTRODUCCIÓN

A partir de la década de los ’90, a pesar de haberse observado un significativo avance en entidades de distintos países en materia de medición del Riesgo Operativo (RO), las prácticas aplicadas por las instituciones para la administración y gestión del RO eran ampliamente heterogéneas, como así también las bases de datos empleadas. Sumado al hecho de que el acceso a las bases de datos de las entidades era restringido, no había una definición que estandarizara el concepto de Riesgo Operativo[1]; factores que dificultaron un desarrollo teórico de prácticas para la medición del RO ampliamente aceptadas.

El Comité de Supervisión Bancaria de Basilea (BCBS o BIS por sus siglas en inglés) ha trabajado conjuntamente con la industria financiera y en particular con la banca, para avanzar en el desarrollo de la medición del RO. Así en Junio 2004 finalmente se acordó definir al Riesgo Operativo como “El riesgo de pérdida debido a la inadecuación o fallas en los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación”. La definición tiene importancia estratégica pues a medida en que se vuelve más amplia y abarca más fuentes potenciales de pérdida, la administración del RO va desplazándose del ámbito departamental a la gerencia “senior”, implicando la creación de una línea funcional para supervisar el RO en todo el banco. En consecuencia se estaría pasando a

[1] Cevallos F.: Metodologías y sistemas de información requeridos para la medición y mitigación del riesgo operativo. Tesis de grado ingeniero comercial. Escuela Politécnica del Ejército. Departamento de Ciencias Económicas, Administrativas y Comercio. Sangolquí, Ecuador, 2008.

considerar la gestión de este tipo de riesgos como una disciplina integral, al igual que el riesgo de crédito o el riesgo de mercado, siendo este un elemento realmente novedoso que introdujo Basilea II.

Debido a que todas las entidades bancarias deben tener una provisión técnica mínima con respecto su exposición al RO, es decir, que deben disponer de un capital mínimo en caja por este ámbito, este trabajo, según sus características específicas, propondrá una metodología para llevar los distintos ámbitos a procesos de estandarización de datos y procesos para ofrecer garantías frente a la exposición al riesgo operacional y aportar en la utilización del método avanzado del VaROp (AMA) que a través del modelo interno de cálculo, permite reducir en un porcentaje importante el cálculo realizado a través del método de Indicador Básico (BIA).

Actualmente el Banco cuenta con una Gerencia de Riesgo Operacional desde el año 2004, y que desde el 2011 pertenece a la división de Riesgo Corporativo, cuenta con una política aprobada por el directorio y marco metodológico de sus funciones.

2. OBJETIVOS

2.1. Objetivo General

El objetivo principal de este trabajo es realizar un análisis a una institución financiera chilena y proponer un modelo de gestión de riesgo operacional realizable o replicable en cualquier institución financiera, de esta forma realizar le efectiva mitigación de los riesgos operacionales presentes y así disminuir los gastos asociados a las pérdidas operativas, basados en la metodología y buenas prácticas propuestas por el comité de supervisión Basilea II.

2.2. Objetivos Específicos

- Realizar la Matriz de Autoevaluación de Gestión y Solvencia de Riesgo Operacional de la RAN 1-13 de la Sbif.
- Identificar los puntos que no cumplen satisfactoriamente con la RAN 1-13.
- Analizar y Establecer el modelo de gestión para Riesgo Operacional.
- Constituir los principios metodológicos del modelo de gestión.
- Crear un modelo de medición para la efectividad y diseño de los controles.
- Fundar un modelo de cálculo de capital de riego operacional.

3. METODOLOGIA

Determinar la situación actual del Banco, para esto se realizará un análisis de los distintos elementos necesarios, como el gobierno corporativo, las políticas, los modelos, procesos y estructura.

Se seleccionarán las mejores prácticas propuestas por Basilea II y los entes reguladores tanto nacionales como internacionales.

Finalmente se entregaran recomendaciones para disminuir las brechas que presente el Banco, así cubrir los aspectos que manifiesten mayores deficiencias.

4. DIAGNOSTICO

4.1. Diagnóstico Interno. Alto Nivel.

Para la realización del diagnóstico interno se utilizó la Matriz de Autoevaluación de Gestión y Solvencia – RAN 1-13[2] (en Anexo N° 1), de la Superintendencia de Bancos e Instituciones Financieras, que recoge las buenas prácticas en los ámbitos de los distintos riegos presentes en los bancos.

"El presente Capítulo contiene las disposiciones relativas a la clasificación que de los bancos, según su solvencia y gestión, debe mantener en forma permanente esta Superintendencia, de acuerdo con lo establecido en el Título V de la Ley General de Bancos. Adicionalmente, en el Capítulo se incorporan los aspectos esenciales de gestión del capital incluidos en el nuevo acuerdo de Basilea (Basilea II)."

En el numeral 3.2 de este documento se señala lo siguiente "En los literales siguientes se describe brevemente la orientación de la evaluación, considerando para el efecto las siguientes agrupaciones de materias:

A) Administración del riesgo de crédito y gestión global del proceso de crédito.

B) Gestión del riesgo financiero y operaciones de tesorería.

C) Administración del riesgo operacional.

D) Administración de los riesgos de exposiciones en el exterior y control sobre las inversiones en sociedades.

E) Administración de la estrategia de negocios y gestión del capital.

F) Gestión de la calidad de atención a los usuarios y transparencia de información.

[2] Sbif, 2013. Recopilación Actualizada de Normas (RAN) – Capitulo 1-13, Clasificación de gestión y solvencia, Circular N° 3.558, 26p.

G) Prevención del lavado de activos y del financiamiento del terrorismo.

H) Gestión de la función de auditoría interna y rol del comité de auditoría.

Las materias indicadas en las letras A), B), C) y D) se relacionan principalmente con el seguimiento oportuno de los riesgos. Las señaladas en las letras E) y F) están relacionadas especialmente con la capacidad para enfrentar escenarios de contingencia y finalmente aquellas mencionadas en las letras G) y H) están relacionadas con el control interno, aun cuando este último aspecto también está inserto en aquellas materias incorporadas al seguimiento oportuno de riesgos.

Respecto a los sistemas de información para toma de decisiones a que se refiere la ley, ellos están presentes, en general, en todas las materias."

Este trabajo de tesis centra principalmente su atención en el punto C) Administración de riesgo operacional, donde se ha desarrollado una encuesta de 83 preguntas que se dividen en nueve ámbitos desarrollados por el evaluador, estos son los siguientes:

- Administración y Evaluación de Riesgos
- Continuidad del Negocio
- Estrategias
- Políticas y Procedimientos
- Servicios Externos / Proveedores
- Auditoría
- Control y Monitoreo
- Organización
- Tecnologías de Información y Sistemas

La encuesta recoge la opinión del Gerente General y de once divisiones, con esto se puede asegurar que las respuestas recibidas son del más alto nivel del banco.

Cada pregunta será respondida con una calificación de 1 a 5 con la siguiente escala, también definida en la RAN 1-13.

CALIF.	DESCRIPCIÓN	SIGNIFICADO
1	EN CUMPLIMIENTO TOTAL	La entidad cumple integralmente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. **No existen deficiencias apreciables**.
2	EN CUMPLIMIENTO MATERIAL	La entidad cumple en forma significativa con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. Aún cuando se identifican algunas debilidades en procesos específicos de alguna función, ellas se pueden considerar menores y **no requieren esfuerzos importantes por parte de la institución para superarlas**.
3	EN CUMPLIMIENTO ACEPTABLE	La entidad cumple satisfactoriamente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. Se identifican algunas debilidades en procesos específicos de ciertas funciones, las cuales deben ser corregidas oportunamente para evitar un deterioro paulatino de la solidez de la institución. **La solución de tales debilidades se considera necesaria.**
4	EN CUMPLIMIENTO INSATISFACTORIO	La entidad no cumple en forma razonable con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. Se identifican debilidades en los procesos que componen diversas funciones, entre las que se encuentran algunas relevantes. **La corrección de estas debilidades debe ser efectuada con la mayor prontitud.**
5	EN INCUMPLIMIENTO	La entidad incumple materialmente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. **La solución de tales debilidades se considera indispensable.**

Tabla 1: Calificaciones de la RAN 1-13, Sbif. 1

El tiempo dispuesto para este proceso fue de dos meses y se realizó entre junio y julio de 2014, donde se recibieron en total 123 respuestas de los distintos encuestados, con los siguientes resultados:

Distribución de Calificaciones (N° y %):

	Calificación 1		Calificación 2		Calificación 3		
N° de preguntas	46	55%	31	37%	6	7%	**83**

Tabla 2: Calificaciones distribución, elaboración propia.

Según los resultados obtenidos más del 50% de las respuestas se considera en cumplimiento total, lo que señala que existen ámbitos donde no existen deficiencias apreciables y el banco cumple integralmente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión, lo que es una buena noticia de cara a esta evaluación.

Las notas promedio según ámbito son las siguientes:

Ámbito Especifico	Promedio Calificaciones
Administración/Evaluación Riesgos	**1,60**
Auditoria	**1,00**
Continuidad del Negocio	**2,17**
Control y Monitoreo	**2,33**
Estrategias	**1,83**
Organización	**1,75**
Políticas y Procedimientos	**1,38**
Servicios Externos / Proveedores	**2,75**
Tecnologías de Información y Sistemas	**1,27**
Promedio	**1,52**

Tabla 3: Tabla Resultados Promedios de Calificaciones, elaboración propia.

- Auditoría: Donde se declara que la revisión realizada por la División Contraloría es independiente de las divisiones que reportan a la administración. La División reporta directamente al Comité de Directores y Auditoria, no teniendo participación funcional en las actividades propias del negocio bancario. Asimismo, la auditoría interna considera en sus evaluaciones el cumplimiento y la eficacia de las políticas y procedimientos.

- Administración: El banco en el año 2013 completó la evaluación del 100% de los procesos, utilizando una metodología cuantitativa del riesgo residual. La que permite realizar la estimación de pérdidas esperadas e inesperadas para todos los riesgo de los proceso.

Los ámbitos con peor calificación son:

- Servicios Externos: Se ha avanzado mucho en la gestión de los riesgos operacionales en términos de proveedores. No obstante, en el caso de las Sociedades de apoyo al giro (14 servicios) y las ETV se tomó la decisión de avanzar de forma sustancial en el alcance y profundidad de las verificaciones y monitoreos de estos actores.

- Continuidad: Durante el 2014 se estableció un programa de pruebas considerando los 2 escenarios principales, falla en infraestructura física y tecnológica, avanzando en el camino a prueba de escenarios en conjunto, sin embargo aún se cree necesario avanzar en la mejora continua de las

metodologías como por ejemplo, la implementar la evaluación cuantitativa del impacto.

- Control y Monitoreo: Los indicadores claves deben ir mutando de acuerdo a la evolución de los riesgos.

Preguntas peor evaluadas:

De la encuesta realizada 6 preguntas fueron consideradas como en cumplimiento aceptable, donde el banco cumple satisfactoriamente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. Además se identifican algunas debilidades en procesos específicos de ciertas funciones, las cuales deben ser corregidas oportunamente para evitar un deterioro paulatino de la solidez de la institución. Por estas razones, se requiere tomar medidas de acción para pasar al menos al cumplimiento material en un tiempo lo más acotado posible.

Ámbito	Pregunta de Evaluación	Calif. Pregunta	Fundamento
Servicios Externos / Proveedores	El banco lleva a cabo verificaciones y monitoreos a las actividades entregadas a terceras partes que realizan procesos críticos.	**3**	Se ha avanzado mucho en la gestión de los riesgos operacionales en términos de proveedores. No obstante, en el caso de las Sociedades de apoyo al giro (14 servicios) y las ETV se tomó la decisión de avanzar de forma sustancial en el alcance y profundidad de las verificaciones y monitoreos de estos actores.

Ámbito	Pregunta de Evaluación	Calif. Pregunta	Fundamento
Continuidad del Negocio	El banco ha desarrollado una metodología formal que considera, la evaluación de impacto y criticidad de sus servicios y productos, la definición de estrategias de prevención, contención y recuperación.	**3**	El banco ha avanzado en la cobertura de la metodología en la organización, definiendo la priorización para productos y servicios críticos frente a una contingencia mayor. No obstante es necesario avanzar en la mejora continua de las metodologías como por ejemplo, la implementar la evaluación cuantitativa del impacto.
Continuidad del Negocio	El Banco realiza pruebas sobre los planes de continuidad de negocio establecidos, y estos son acordes con el tamaño y complejidad de las operaciones.	**3**	El banco ha avanzado en el nivel de pruebas tanto en ámbito tecnológico como en el operacional, no obstante en necesario avanzar en el alcance (cobertura) y profundidad del plan de pruebas.
Control y Monitoreo	El banco ha identificado indicadores apropiados que entreguen alertas de un aumento del riesgo y de futuras pérdidas.	**3**	Los indicadores claves deben ir mutando de acuerdo a la evolución de los riesgos.
Organización	Todos los niveles del personal asumen y comprenden sus responsabilidades respecto a la administración del riesgo operacional.	**3**	El banco tiene definido los roles y responsabilidades sobre la gestión de riesgo operacional, no obstante es necesario fortalecer el nivel de madurez de conocimiento y responsabilidad sobre la gestión de riesgo Operacional.
Políticas y Procedimientos	La entidad ha hecho participe a las personas que laboran dentro de la organización sobre las normas y/o políticas legales que influencian directamente en los riesgos legales.	**3**	A través de los programas de entrenamiento a Jefaturas, los planes comunicacionales y los procedimientos establecidos la Organización hace partícipe a sus trabajadores sobre las normas y/o políticas que influencian riesgos legales, sin embargo es necesario reforzar la divulgación y capacitación de estos temas a nuestros colaboradores a todo el nivel de la organización.

Tabla 4: Peores Preguntas según Calificaciones, elaboración propia.

4.2. Diagnóstico Interno. Según Basilea II.

En esta segunda parte se aborda el diagnostico interno desde la perspectiva de las buenas prácticas de Basilea II, declaradas en el documento Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework.

Para realizar esta revisión se realizó un petitorio de Políticas, Procedimientos, Normas, Manuales y otros Documentos que permitan conocer el estado actual del banco frente a las buenas prácticas descritas en Basilea II.

Esta etapa esta divida en tres principales temas, estos son:

- Gobierno Corporativo.
- Modelo de Riesgo Operacional.

Para esto se ha realizado un Petitorio por cada tema, que permite realizar un diagnóstico de la situación actual de la Institución y luego analizar las brechas presentes frente a las mejores prácticas definidas por el comité Basilea.

4.2.1. Modelo de Gobierno Corporativo.

Actualmente el banco cuenta con una estructura organizacional del Riesgo Operacional dividida en tres grandes grupos, los Comités[3] realizados desde nivel de Alta Gerencia hasta niveles de departamento, la Gerencia de Riesgo Operacional, finalmente el último nivel y más grande

[3] La información correspondiente a las principales funciones y responsabilidades de los comités realizados se encuentran en la Memoria anual del Banco.

corresponde a la distribución en la organización de la responsabilidad de coordinadores y gestores de riesgo operacional (gestión semi-descentralizada), estos 37 coordinadores y 85 gestores se distribuyen a través de las distintas divisiones presentes en el Banco y tienen responsabilidades establecidas frente a la gestión del riesgo operacional presente en la institución.

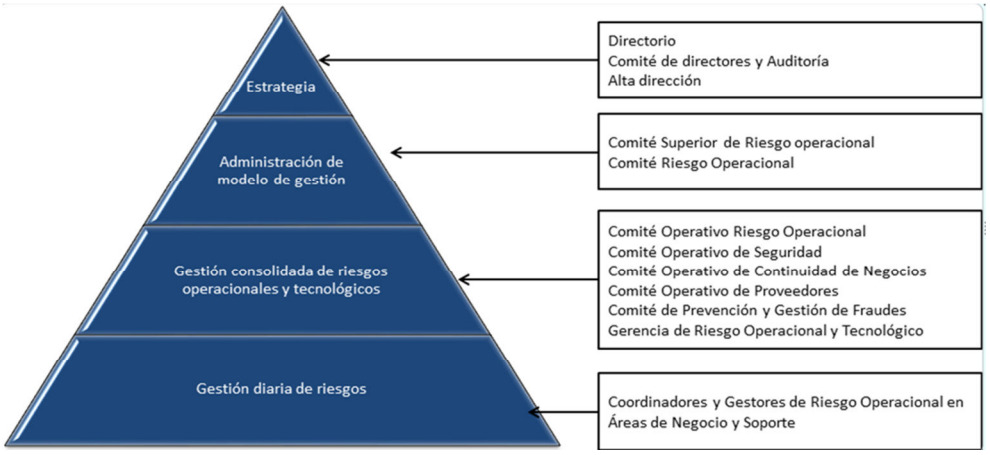

Ilustración 1: Gobierno Corporativo, elaboración propia

4.2.2. Estructura Organizativa de Riesgo Operacional

Se describe a continuación la estructura organizativa definida para la función de gestión y control del riesgo operacional para la organización, de acuerdo al siguiente organigrama.

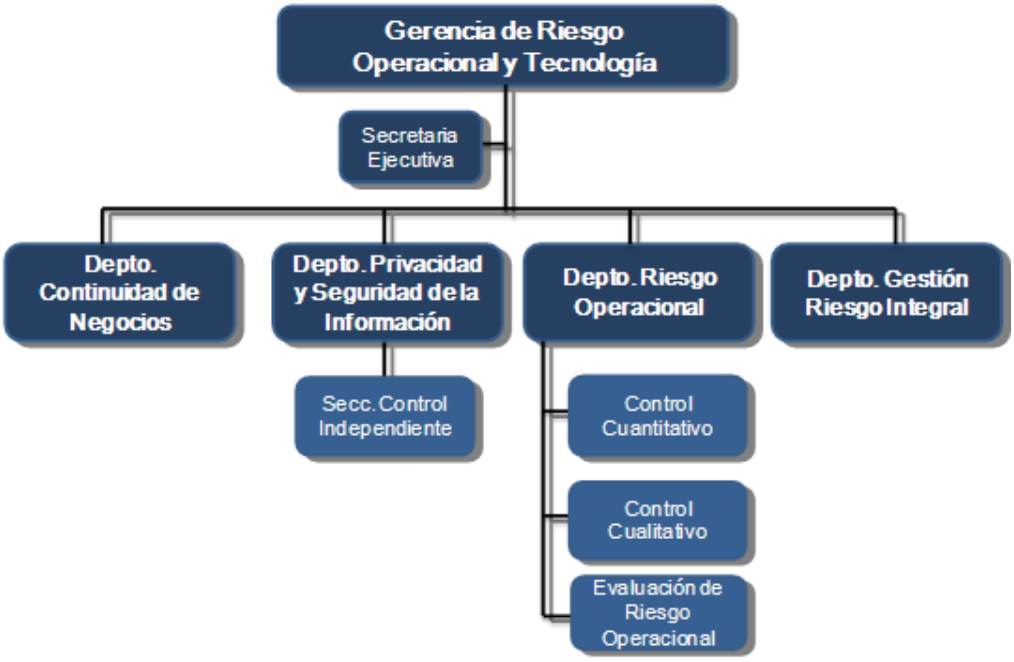

Ilustración 2: Organigrama, elaboración propia

Cada departamento cumple una función fundamental en la gestión de riesgo operacional, a continuación se describen las principales funciones de cada uno:

- **Departamento de Continuidad de Negocios**: Tiene como principal función elaborar un Plan de Continuidad del Negocio, con el objetivo de establecer un modelo, marco metodológico y procedimientos para asegurar la continuidad operacional del Banco y Filiales ante un evento catastrófico, de cara a los clientes, accionistas y terceros (stakeholders). Además cumplir con las obligaciones regulatorias.

- **Departamento de Privacidad y Seguridad de la Información:** Sus principales funciones se describen a continuación:
    - Impulsar en el Banco y Filiales el cumplimiento de las políticas, normas y procedimientos de seguridad de la información, basados en las leyes y regulaciones vigentes, mejores prácticas de mercado y necesidades del negocio.
    - Proponer, organizar y supervisar el programa de capacitación y entrenamiento de seguridad de la información para los colaboradores del Banco y filiales.
    - Proponer, impulsar y hacer seguimiento al Plan Anual de Seguridad de la Información y generar nuevas iniciativas de seguridad de la información que fortalezcan la estrategia del negocio.
    - Comunicar e involucrar a la organización en las iniciativas de seguridad de la Información, a fin de asegurar su efectiva implementación a nivel de la organización.
    - Analizar el riesgo asociado a la implementación de los distintos proyectos, productos y servicios y entregar las recomendaciones para el tratamiento de riesgos y vulnerabilidades.
    - Apoyar en la investigación, evaluación y recomendación de soluciones o herramientas que refuercen y fortalezcan la seguridad de la información en la Organización.

- Apoyar en la definición, desarrollo e implementación de planes de mejoras en el ámbito de seguridad de la información, para los distintos procesos, productos y servicios en la organización.
- Mantener informado a las gerencias y Comités responsables de supervisar los niveles de riesgo de seguridad de la información y tecnología.
- Manejar una visión integral de la seguridad de la información de la Organización, teniendo roles y responsabilidades en otras políticas relacionadas a seguridad de la información.

- **Departamento de Riesgo Operacional:** Establece directrices y asegura el perfecto funcionamiento y coordinación de todas y cada una de las áreas involucradas en la gestión de RTO, en cumplimiento de las directrices Comité de Riesgo Operacional y la Alta Administración. En concreto:
  - Gestionar modelo de riesgo operacional del grupo, con énfasis en los procesos críticos y riesgos relevantes, considerando lineamientos globales, mejores prácticas y requerimientos de los supervisores.
  - Identificar y evaluar los riesgos operacionales relevantes con el objeto de monitorear y controlar el nivel de exposición de riesgo operacional.
  - Establecer bases sólidas y formales para la gestión del riesgo operacional, comunes y en coordinación con otras instancias internas.

- Gestionar en la organización, los distintos procesos de autoevaluación de gestión de riesgo operacional y las requeridas por la normativa vigente (SBIF).
- Difundir a toda la organización políticas, mejores prácticas y procedimientos de gestión de riesgo operacional.
- Supervisar el registro y seguimiento de los eventos de RO de las Unidades y consolidar la información a nivel corporativo.
- Asegurar que se cubren adecuadamente las necesidades de reporting.
- Definición, supervisión y mantención de herramientas ad-hoc para la identificación, evaluación, limitación y control del riesgo operacional.

- **Departamento de Gestión de Riesgo Integral:** Una de las principales funciones de este departamento será analizar e informar a la organización de los principales focos de riesgos materiales y no materiales que deben ser gestionados de manera oportuna en los distintos procesos y servicios del Banco. Para ello, será responsable de establecer y conducir los procesos y herramientas que sean necesarios para identificar los puntos críticos de riesgo, a través de indicadores clave e informes de gestión, en base al resultado de los distintos procesos desplegados por el Área Riesgo Operacional, evaluación de Riesgo de nuevos Productos y Servicios y control y seguimiento de los planes de acción definidos por las unidades del Banco, en pos de administrar adecuada y oportunamente los riesgos detectados.

4.2.3. Modelo de Gestión de Riesgo Operacional

4.2.3.1. Visión General

Las distintas etapas del Modelo de Gestión de Riesgo Operacional y Tecnológico (ROT) implican:

- Identificar el riesgo operacional relevante a todas las actividades, productos, procesos y sistemas del banco, tanto existentes como de nueva definición.
- Medir y evaluar el riesgo operacional de forma objetiva, continuada y coherente con los estándares de Basilea II y la industria, y proponer objetivos y niveles de tolerancia al riesgo.
- Realizar un seguimiento continuo de las exposiciones de RO con el fin de detectar niveles de riesgo no asumidos, implantar procedimientos de control, mejorar el conocimiento interno y mitigar las pérdidas.
- Establecer medidas de mitigación para el ROT.
- Generar informes periódicos sobre la exposición al ROT y el nivel de control para la Alta Dirección y Áreas / Unidades del Grupo.
- Definir e implantar sistemas que permitan vigilar y controlar las exposiciones al ROT, integrados en la gestión del Grupo, aprovechando la tecnología existente y procurando la máxima automatización de las aplicaciones.
- Definir y documentar las políticas para la gestión del ROT, e implantar metodologías de gestión de este riesgo acordes con la normativa y las mejores prácticas.

4.2.3.2. Modelo Gráfico

El siguiente esquema recoge, a modo de resumen, el Modelo de Gestión de Riesgo Operacional.

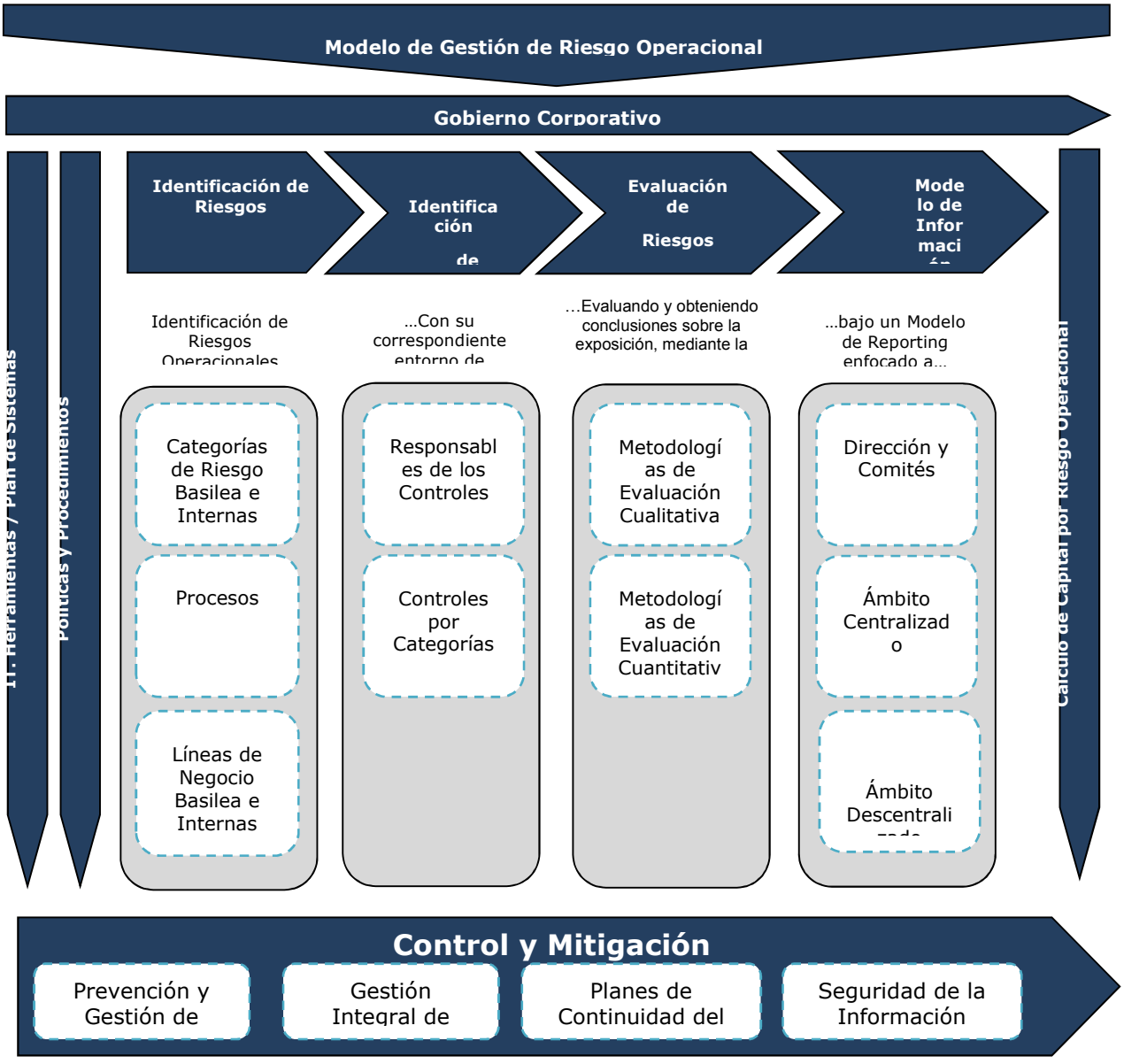

Ilustración 3: Modelo de Gestión, elaboración propia

4.2.3.3. Identificación de Riesgos

- **Categorías de Riesgo Basilea e Internas**[4]

El Nuevo Acuerdo de Capital de Basilea (Basilea II) establece que los riesgos operacionales que las Entidades deben identificar, medir y gestionar, deben clasificarse en las siguientes siete categorías de riesgo. A partir de las categorías principales definidas por Basilea II, se ha establecido un desglose en sub categorías de niveles inferiores que permitan alcanzar mayor detalle de agrupación. A continuación se detallan las categorías de riesgo Basilea II y las sub categorías correspondientes definidas:

1. **Fraude Interno:** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad/discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa.

2. **Fraude Externo:** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero.

3. **Prácticas Laborales y Seguridad en el Trabajo:** Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales.

[4] Jiménez Rodríguez E. 2013. El capital regulatorio por riesgo operacional, p86.

4. **Clientes, Productos y Prácticas del Negocio:** Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación) o de la naturaleza o diseño de un producto

5. **Daños en Activos Físicos:** Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos**.**

6. **Interrupción del Negocio y Fallos en los sistemas:** Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas.

7. **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.

- **<u>Procesos</u>**

  Cuando hablamos de procesos nos referimos a las diferentes etapas, actividades y al conjunto de tareas relacionadas de forma que componen de manera ordenada / escalonada la consecución de un resultado definido. En este sentido, es necesario asociar cada uno de los riesgos operacionales a un proceso concreto gestionado por un responsable que asume dicha exposición y define mitigantes para su reducción.

- **Líneas de Negocios Basilea e Internas**

A continuación se definen individualmente cada una de las ocho líneas de negocio, recogiendo las actividades y productos más importantes que se englobarían en las mismas. Para ello se incorporan las definiciones de las Líneas de Negocio a partir de lo definido por BIS II y la traslación de dichos negocios a la realidad de la organización.

Nivel 1	Nivel 2	Grupo de Actividades
Finanzas Corporativas	Finanzas Corporativas	Fusiones y adquisiciones, suscripción de emisiones, titulización, servicio de estudios, deuda (pública, alto rendimiento), acciones, sindicaciones, Ofertas Públicas Iniciales, colocaciones privadas en mercados secundarios.
	Finanzas de administraciones locales/ públicas	
	Banca Inversiones	
	Servicio de asesoramiento	
Negociación y Ventas	Ventas	Renta fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda, intermediación unificada (prime brockerage).
	Creación de Mercado	
	Posiciones Propias	
	Tesorería	
Banca Minorista	Banca Minorista	Préstamos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarías.
	Banca Privada	Préstamos y depósitos de particulares, servicios bancarios, fideicomisos y testamentarías y asesoramiento de inversión.
	Servicio de Tarjetas	Tarjetas empresas / Comerciales, de marca privada y minorista.
Banca Comercial	Banca Comercial	Financiación de proyectos, bienes raíces, financiación comercial, factoring, arrendamiento financiero, préstamos, garantías, letras de cambio.
Pagos y Liquidación	Clientes externos	Pagos y recaudaciones, transferencias de fondos, compensación y liquidación.
Servicios de Agencia	Custodia	Contratos, certificados de depósitos, operaciones de sociedades (clientes) para préstamos de valores.
	Agencia para Empresas	Agentes de emisiones y pagos
	Fideicomisos de empresas	Manejo de bienes en beneficio de un tercero.

Nivel 1	Nivel 2	Grupo de Actividades
Administración de Activos	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales cerrados, abiertos, participaciones accionarías.
	Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable.
Intermediación Minorista	Intermediación minorista	Ejecución y servicio completo.

Tabla 5: Resumen de Líneas de Negocio[5]

4.2.3.4. Identificación de Controles

- **Responsables de los controles**

  Los responsables de los controles son los dueños de los procesos que se ejecutan en cada línea de negocio. Estos responsables deben establecer controles efectivos que mitiguen los riesgos operacionales y tecnológicos que puedan afectar a los productos, procesos, actividades externalizadas y/o sistemas de información.

- **Controles por categoría**

  La gestión y el control del riesgo operacional debe ser parte integrante de las actividades diarias de la Entidad. Por tanto, las medidas para controlar este riesgo deben introducirse a lo largo de toda la Organización, y se concretarán en diferentes niveles que forman el Marco de Control de Riesgo Operacional:

  - Control a nivel individual.
  - Control de la Dirección.

[5] **La gestión del riesgo operacional: de la teoría a su aplicación, Ana Fernández-Laviada**

- Control de unidades especializadas, como Auditoría Interna, Auditoría externa, SBIF y otros organismos reguladores.

De este modo, cada riesgo identificado estará asociado a su correspondiente marco de control.

- **Control a Nivel Individual**

  Todo el personal es responsable de gestionar y controlar los riesgos operacionales de su competencia. En este sentido los valores corporativos (integridad personal, trabajo en equipo y profesionalidad), así como el conocimiento y comunicación de los posibles riesgos, son requisitos indispensables para la gestión y el control del Riesgo Operacional.

- **Control de la Dirección**

  Normalmente la Dirección tiene que delegar tareas y establecer niveles de autoridad dado el tamaño de la Entidad y la especialización necesaria en las distintas tareas. Sin embargo, la Dirección sigue siendo la responsable de las tareas delegadas. Por ello, es necesario que la misma establezca las adecuadas medidas de control en los procesos y sistemas de su competencia.

- **Control de unidades especializadas.**

  La Dirección puede decidir que no se realicen directamente ciertas tareas de control, debido a la necesaria segregación de funciones y a la especialización que se requiere para ejecutarlas. En estos casos, la Dirección delega estas

funciones a Unidades Especializadas. (Auditoría Interna, Auditoría externa, entidades reguladoras).

4.2.3.5. Evaluación de Riesgos y Controles

Existe un rango de posibles metodologías de identificación y medición del Riesgo Operacional y, en muchos casos, se tratan de técnicas complementarias, ya que ninguna de ellas cubre por sí sola todas las necesidades de análisis de la Entidad.

- **Metodologías de Evaluación Cualitativas**
  - Mapa de Riesgos y Controles

La construcción del Mapa de Riesgos Operacionales de los procesos de un Banco u Organización, se elaboró en conformidad al alcance determinado respecto a las líneas de negocio definidas en Basilea II.

Esta metodología contempla los procesos de la Organización, tomando como base la documentación existente sobre procesos y procedimientos desarrollados por la Gerencia de Riesgo Operacional en coordinación con los responsables de cada uno de los procesos.

La identificación de los riesgos operacionales asociados a los procesos es una responsabilidad básica de los gestores de dichos procesos y la Gerencia de Riesgo Operacional participa aportando las directrices metodológicas y de criterio para facilitar dicho proceso de identificación.

Adicionalmente y como parte de la documentación asociada a la identificación de riesgos operacionales se procederá a identificar y describir los factores mitigantes

más relevantes asociados a dichos riesgos operacionales. Por factores mitigantes se entienden aquellas características de la gestión del negocio, de la ejecución del proceso o elementos adicionales que permiten la mitigación del riesgo, ya sea evitando que el riesgo suceda o bien, reduciendo el impacto de pérdida dada su ocurrencia.

Los controles son el elemento más característico a considerar dentro de los factores mitigantes pero se incluirán otros elementos adicionales que faciliten la reducción de la exposición al riesgo.

Estos mapas facilitarán posteriormente el establecimiento de recomendaciones sobre controles en aquellos procesos o actividades con mayor exposición al riesgo.

En la descripción del riesgo se incorpora la siguiente información:

- Proceso en el que se origina el riesgo.
- Descripción del Riesgo.
- Vínculo con el Nivel I y II de la categorización de eventos de riesgo definida por la Organización.
- Descripción de los impactos como pérdidas que se producirían en la materialización del riesgo.
- Vínculo a la Línea de negocio correspondiente.
- Afectación a otros riesgos.

- Identificación y descripción de los principales controles que mitigan la ocurrencia o el impacto del riesgo operacional.

- **Cuestionarios de Auto-Evaluación**

El cuestionario de auto-evaluación permite obtener una primera estimación cuantitativa (basada en datos subjetivos proporcionados por los responsables) del riesgo operacional existente, que podrá ser complementada posteriormente con las técnicas cuantitativas que se desarrollen a partir de los datos recogidos en la base de datos de pérdidas operacionales de la organización.

Los principales objetivos de la elaboración de cuestionarios de auto-evaluación son: identificar todos aquellos riesgos que puedan tener un impacto económico material en el proceso analizado, obtener información sobre el impacto y la frecuencia de los riesgos identificados, obtener información sobre la existencia y efectividad de los controles existentes y la posibilidad de establecer controles adicionales y por último monitorizar el desarrollo y seguimiento de los planes de mejora continua.

- **Definición de Pérdidas a Efectos del Cuestionario de Autoevaluación**

  Un aspecto fundamental del cuestionario a efectos de la cuantificación de los riesgos es la definición de la pérdida (también mencionada como “impacto” o “severidad”). En concreto, la definición de “impacto” considerada por la Organización es la siguiente:

  “...Todos los costos externos derivados del evento operacional en que no se hubiera incurrido de no haberse producido el evento, excluyendo los siguientes”:

Medidas preventivas que sean adoptadas en relación con el evento (ej. incrementar la formación a determinados empleados)

a) Mejora de controles (ej. establecer un chequeo por parte de una tercera persona)
b) Planes de inversión (ej. costo por reingeniería del proceso)
c) Ingreso dejado de generar[6] (ej. aquellos ingresos no obtenidos por imposibilidad de operar durante una caída de sistemas)
d) Pérdida reputacional[7] (ej. sucesivos retrasos en la liquidación pueden llevar a la pérdida de clientes)
e) Costo de oportunidad (ej. tiempo que los empleados dedican a solventar incidencias producidas por errores operacionales en vez de destinarlo a otras actividades)

En este sentido, entre **los costos a considerar** se incluirían, entre otras, las siguientes tipologías:

a) Indemnizaciones: Pagos a clientes y/o terceras partes por pérdidas operacionales de las cuales la entidad es responsable (ej. intereses por retrasos en liquidaciones, etc.)
b) Pérdidas de recursos: Pérdidas derivadas de la imposibilidad de llevar a cabo una demanda legal contra un tercero para la recuperación de un activo debido

6 Se excluyen los ingresos dejados de generar, ya que Basilea establece que no deben afectar al consumo de capital. No obstante y cuando por motivos de gestión se solicite, se podrá realizar una aproximación a los mismos a través de una columna adicional en el cuestionario.
Adicionalmente se incorporan en la valoración como riesgo operacional aquellos ingresos dejados de generar que con un origen de riesgo operacional implica un derecho de cobro en un contrato formalizado con un cliente/contraparte comercial y que se deja de cobrar de forma inconsciente.
7 Si bien la pérdida reputacional no ha de computarse a efectos del "impacto", el cuestionario realiza una primera aproximación a la misma a través de escalas cualitativas.

a un error operacional (ej. pagos realizados a una contrapartida incorrecta no devueltos, errores en la documentación legal que impiden la reclamación a terceros, etc.)

c) Castigos: Reducción directa del valor de los activos financieros como resultado de un evento operacional (ej. fraudes, pérdidas por contrataciones no autorizadas, pérdidas derivadas de contrataciones con contrapartes con líneas excedidas, etc.)

d) Acciones regulatorias: Multas o costos derivados de cualquier penalización regulatoria

e) Pérdidas o daños en los activos: Reducción en el valor de activos físicos de la entidad debido a accidentes (negligencias, accidentes, fuegos, etc.)

f) Contingencias legales: Costos incurridos en litigios en relación a eventos de riesgo operacional acontecidos (ej. gastos de abogados, etc.)..."

- **Valoración de los factores mitigantes (controles)**

  Se considera para su identificación y valoración una definición en **sentido amplio** de los factores mitigantes, es decir, todos aquellos sistemas, procesos o aspectos organizativos que, aplicándose en el momento de la valoración del riesgo, se realizan interna o externamente con el fin de mitigar los riesgos operacionales identificados. Habitualmente, dichos factores mitigantes son mencionados como **controles**, si bien, siempre que se utilice el concepto control en este documento tiene que ser considerado con el concepto amplio comentado anteriormente.

Por lo tanto, los factores mitigantes pueden cubrir los siguientes aspectos:

- Sistemas e infraestructura (ej. control de precios en la plataforma de contratación, etc.)
- Procesos y procedimientos (ej. procedimientos de cuadres entre información procedente de dos fuentes, validación de datos contra soporte físico, etc.)
- Personas y organización (ej. segregación de funciones, etc.)

Adicionalmente, se identifican e incluyen en el inventario de riesgos (asociados a cada riesgo al que mitigan) todos aquellos controles que posean un poder mitigante que se considere relevante (en este sentido, pueden excluirse según el criterio de Riesgo Operacional, de acuerdo con el área analizada, aquellos controles que en cada caso se determine que por lo reducido de su ámbito de aplicación y/o escaso poder mitigante están por debajo de un cierto nivel de materialidad).

Por lo tanto, la identificación y evaluación de los controles no pretende ser exhaustiva, sino permitir una evaluación cualitativa representativa del entorno de control de los riesgos identificados.

Por último, la valoración descrita en los párrafos anteriores posee una utilidad básicamente de gestión, ya que la cuantificación del riesgo operacional bajo la metodología cualitativa incorpora de manera implícita el efecto de los mitigantes. En este sentido, la valoración de los riesgos se ha de realizar “neta” del efecto de los controles, por lo que la estimación de la frecuencia, impacto medio, peor escenario e impacto reputacional del riesgo se realiza

considerando la existencia de los controles identificados con la efectividad evaluada.

A continuación se detalla la metodología aplicada:

Se utiliza una escala de medición desde dos ópticas:

- Por un lado se evalúa la **efectividad del control**, entendida como el "poder mitigante" de dicho control ya sea para evitar la ocurrencia del riesgo, ya sea, para su rápida detección o por su efecto limitante del impacto por el mismo;

- Por otro lado se valora la **cobertura**, entendida como el grado de implantación de dicho control en el seno de la Organización para el conjunto de las operaciones a las que puede afectar ese riesgo. De esta forma, se permite identificar aquellos controles que siendo relevantes no están implantados en la organización, identificándose de este modo posibles acciones de mejora (Planes de Acción).

Esta valoración se presenta en las siguientes escalas cualitativas:

Nivel	Descripción Cobertura
0	No existe
1	Existe y no se aplica
2	Se aplica ocasionalmente
3	Se aplica con frecuencia
4	Se aplica siempre

Tabla 6: Escala de valorización Controles – Cobertura, elaboración propia.

Nivel	Descripción Efectividad
0	Muy Baja
1	Baja
2	Media
3	Alta
4	Muy Alta

Tabla 7: Escala de valorización Controles – Efectividad, elaboración propia.

Se entenderá como “efectividad” el grado de detección de los controles de las "incidencias/errores" que generan las pérdidas. En ese sentido, la valoración deberá desarrollarse en base a las siguientes consideraciones:

- Muy baja: El control se aplica pero su grado de detección de errores para impedir que sucedan o facilitar su resolución es muy limitada (entre el 0 y el 25%).

- Baja: El control se aplica pero su grado de detección de errores para impedir que sucedan o facilitar su resolución es limitada, pero facilita la detección del evento entre un 25 y un 50% de los casos.

- Media: El control se aplica y su grado de detección de errores y facilita la detección del evento entre un 50 y un 75% de los casos.

- Alta: El control se aplica y su grado de detección de errores y facilita la detección del evento en más de 75% de los casos.

- Muy Alta/Completa: el control permite siempre identificar que el riesgo ha sucedido o puede suceder y mitigar el efecto de las pérdidas.

  En lo que respecta a controles ex – post, esto es, aquellos que se realizan a posteriori de suceder el riesgo y que permiten detectarlo pero la pérdida es posible que ya se esté produciendo, habría que considerar en la valoración el efecto temporal.

  Esto es, un control 'on-line' que detecta el 100% de la operativa errónea en el momento que sucede e impida que suceda puede recibir la evaluación de "Muy Alta".

  Un control ex - post que detecta también el 100% de la operativa pero que se aplica en "d+1" (y lo que hace es limitar la pérdida a 1 día) debe recibir una valoración como máximo de "Alta", si el control es en "d+7" (semanal) o en "d+30" (mensual) el control debe recibir evaluaciones de Media o incluso de Baja (dependiendo de la naturaleza del riesgo).

  Al momento de valorar la "cobertura" del control se deberá tener en consideración la "base de operaciones" sobre el cual es aplicado. Por ejemplo, si el control es aplicado frecuentemente, pero no da cobertura a todas las operaciones deberá valorarse como "Se aplica con frecuencia".

- **Consideraciones en la determinación de la efectividad de los controles**

  En líneas generales, "la efectividad del control" se determinará en función de los resultados obtenidos en la valoración de su **cobertura** y **efectividad**, a

continuación se presenta una gráfica que nos muestra el resultado según la valoración del control:

En síntesis, un **resultado Efectivo** se obtendrá siempre y cuando la cobertura del control sea valorada como 'se aplica siempre' o 'se aplica con frecuencia', mientras que la efectividad ha sido valorada como "Alta" o "Muy Alta".

- **Valoración del impacto reputacional en riesgos operacionales**

La metodología cualitativa implantada en la organización incluye asimismo la valoración del posible impacto reputacional de aquellos riesgos operacionales que han sido identificados.

La medición de este impacto ofrece un componente de información adicional importante para la Organización. Sin embargo, el riesgo reputacional es altamente subjetivo y de difícil cuantificación.

La valoración de este riesgo se realiza a través de una categorización cualitativa basada en una adaptación de la escala establecida por la British Banker Association (BBA). Esta categorización incluye un factor subjetivo en una escala del 0 al 5, expresando la relación y el daño reputacional asociado con el evento de pérdida operacional.

La descripción de los grados de esta escala aplicada por la Organización es la siguiente:

- **Valoración del impacto en clientes** de la manifestación del riesgo. Se evaluará en función de la siguiente escala:

Nivel	Descripción
0	No es percibida por el cliente.
1	Defecto ligero. No provoca molestias al Cliente, pero algunos Clientes pueden sentir la necesidad de pedir aclaraciones al Banco.
2	El Cliente se ha de contactar necesariamente con el Banco o desplazarse a la oficina para solucionar el problema. La resolución es fácil y no genera complicaciones.
3	Igual que el caso anterior, pero la resolución del problema es complejo y se puede demorar en el tiempo y generar molestias adicionales al Cliente.
4	Importantes molestias al Cliente. Además de las gestiones con el Banco, habrá que hacer gestiones con terceros implicados en el error, justificar el error, hacer cartas, etc. Incluye costos económicos directos.
5	Consecuencias nefastas. Igual que el caso anterior, pero con la pérdida inmediata del Cliente y la posibilidad de imputar responsabilidades legales al Banco.

Tabla 8: Valorización de Impacto en Clientes, elaboración propia.

- **Valoración del impacto reputacional en <u>otros grupos de interés y mediático</u> del riesgo**: una categorización cualitativa basada en una adaptación de la escala establecida por la British Banker Association (BBA). Esta categorización incluye un factor subjetivo en una escala del 0 al 5, expresando la relación y el daño reputacional asociado con el evento de pérdida operacional.

  La descripción de los grados de esta escala propuesta es la siguiente:

Nivel	Descripción
0	Sin efecto externo.

Nivel	Descripción
1	Sin cobertura mediática, ligero incremento en reclamaciones de clientes.
2	Cobertura mediática local o del sector financiero, incremento en reclamaciones de clientes, posible pérdida de alguna cuenta de clientes.
3	Cobertura mediática a escala nacional, incremento acusado en reclamaciones de clientes, alguna pérdida de clientes, solicitud de información del regulador (informal), posible implicación de directivos de la Entidad.
4	Cobertura mediática nacional acusada y limitada a nivel internacional, pérdida seria de clientes, investigación formal del regulador, implicación de directivos de la Entidad.
5	Cobertura mediática nacional e internacional acusada, pérdida de clientela a gran escala, alta implicación de la dirección de la Entidad.

Tabla 9: Valorización de Impacto Reputacional, elaboración propia.

- **Obtención de resultados**

  Los resultados básicos obtenidos a partir de los cuestionarios son:

  - **Modelización:** A partir de la valoración de escenarios efectuada se modelan las distribuciones de frecuencia de ocurrencia de los eventos y severidad de los mismos, y se obtiene por agregación (convolución) de éstas la distribución de pérdidas operacionales. A tal fin se emplea el método no paramétrico de simulación de Monte Carlo.

  - **Resultados del modelo:** Se obtiene para cada riesgo, como resultado, una pérdida esperada o pérdida recurrente (como producto entre la frecuencia de ocurrencia del evento y su impacto medio) y un Valor en Riesgo (VaR) con un

margen de confianza del 99,9%, que respectivamente estiman la pérdida potencial esperada e inesperada.

- **Conversión a escala cualitativa:** Tanto el dato de pérdida recurrente como el de exposición potencial se convierten a una escala cualitativa conforme a la cual se presentan los resultados a las distintas áreas. Se fijan, por tanto, intervalos y se le asigna un valor cualitativo, con lo que se hablará de exposición potencial y pérdidas recurrentes baja, media, alta y muy alta.

- **Evaluación de controles** asociados a los diferentes riesgos.

- Valoración de la **existencia de riesgo reputacional** asociado al riesgo que se está evaluando, así como determinación del **grado** que representa dicho riesgo reputacional.

- **<u>Mecanismos de Validación</u>**

  El resultado de un cuestionario no deja de ser una valoración subjetiva de la persona entrevistada, por lo que la Organización deberá asegurar que los cuestionarios estén bien definidos y sean llevados a cabo con rigor y de forma imparcial.

  Para ello se desarrollarán una serie de mecanismos de validación basados en los siguientes procedimientos:

  Revisión de la Gerencia de Riesgo Operacional y Tecnológico y Comité Experto (Comité Operativo de Riesgo Operacional y Comité de Riesgo

Operacional) en la utilización de criterios homogéneos de valoración a lo largo de toda la Organización.

Contraste de las respuestas obtenidas con fuentes de información diversas (informes de Auditoría de oficinas, informes y experiencia de Auditoría Informática, etc.).

Evaluación de la razonabilidad de la estimación de pérdidas esperadas asociadas a los procesos con los registros de pérdidas registrados a la fecha.

Revisión por parte de los responsables de la División de la evaluación/valoración de la exposición al Riesgo Operacional desarrollada por las distintas unidades que dependen de dicha División.

Validación en el tiempo. A través de la realización de revisiones periódicas donde se estabilizarán las evaluaciones iníciales dado el conocimiento previo y la propia expansión de la cultura de riesgo operacional y de fuentes de información en paralelo que faciliten un mayor número de datos.

Por último, la Gerencia de Auditoría Corporativa en el ejercicio de sus funciones realiza revisiones periódicas tanto sobre las metodologías como sobre los procedimientos de evaluación.

- **Criterios en la Actualización de la Evaluación Cualitativa**

El proceso de identificación y evaluación cualitativa del Riesgo Operacional en la Organización no es estático en el tiempo, sino que requerirá de reevaluaciones periódicas, presentando por tanto un carácter iterativo.

Una vez cerrada la evaluación de una División o Filial bajo la metodología cualitativa y presentadas las conclusiones, las propias Divisiones / Filiales involucradas en el proceso serán responsables de identificar todos aquellos cambios que puedan influir en su perfil de Riesgo Operacional, incluyendo:

- Modificaciones/ Actualizaciones en los procesos
- Aparición de nuevos controles y/o cambios relevantes en el entorno de control
- Grado de automatización
- Tendencias del entorno (mercado, normativa legal, proveedores, etc.) que la afecten
- Aplicación de directrices estratégicas o políticas de la Entidad
- Desarrollo de nuevas técnicas de mitigación en los riesgos operacionales
- Etc.

Y, como consecuencia de ello, colabora con la Gerencia de Riesgo Operacional en la detección de **nuevos riesgos** de relevancia que debiesen incluirse en los inventarios correspondientes.

Riesgo Operacional repite de manera iterativa el **análisis cualitativo** de los distintos procesos con una **periodicidad anual** de revisión de acuerdo a su criticidad y/o modificaciones detectadas, debiendo ser reportadas por las Divisiones/Filiales todas las circunstancias antes mencionadas de cara a la actualización de la documentación (por ejemplo, inventarios de riesgos y controles). En este sentido, la Gerencia de Riesgo Operacional colabora con las Divisiones de Negocio y de Soporte en la actualización de los inventarios de riesgos con el fin de recoger los posibles cambios ocurridos en el perfil de riesgo de las mismas.

La Gerencia de Riesgo Operacional, asimismo, se encarga de poner a disposición de las Divisiones o Filiales los **cuestionarios de auto-evaluación** de riesgos operacionales, criticidad y outsourcing, para su re-evaluación.

Con los resultados obtenidos se actualiza la evaluación del Riesgo, cuyos datos son comparados por la Gerencia de Riesgo Operacional con los análisis de ejercicios anteriores para la obtención de conclusiones adicionales sobre la **evolución** del riesgo.

Asimismo, en este análisis se presta particular atención a la identificación **de proyectos de mitigación** del riesgo, mediante:

- La identificación de los principales riesgos de la División de Negocio, Soporte o Filial (y su evolución en el tiempo).
- La identificación y consenso sobre posibles planes de mejora para la mitigación de estos riesgos.
- El seguimiento de las recomendaciones incluidas en el documento de conclusiones sobre Riesgo Operacional.

- Tratamiento de Servicios a terceros

Tanto la Superintendencia de Bancos e Instituciones Financieras, a través de la norma 119 – capítulo 20/7, como el Comité de Basilea muestra una particular atención a la identificación y gestión de los riesgos operacionales derivados de la subcontratación de actividades a empresas externas de servicios, recomendando8 actuaciones específicas para el tratamiento de los riesgos de las empresas de servicios (outsourcing). Entre éstas se identifican

8 Documento de Sound Practices for the Management and Supervision of Operational Risk

recomendaciones como la firma de acuerdos legales con las empresas de servicios que detallen el reparto de responsabilidades entre las partes.

Por otra parte, The Joint Forum (grupo dependiente de BIS y formado por expertos del Basel Comitee on **Banking** Supervision (BCBS); International Organization of **Securities** Commissions (IOSCO); International Association of **Insurance** Supervisors (IAIS)), a través de la generación de un Papel Consultivo, define **las bases** que tomarán los organismos correspondientes (los citados anteriormente) como soporte en la definición de las normas que les compete. Así, la definición de outsourcing contemplada por este documento (y que asume la organización) considera "El uso de un tercero (empresa externa) por una Entidad regulada en la ejecución de actividades de manera continua que podría haber desarrollado ella misma internamente".

Quedan excluidos de esta definición de outsourcing los contratos de compra o adquisición de equipos, suministros y similares.

De acuerdo con la relevancia otorgada a este aspecto por los mencionados organismos, la Organización evalúa la actividad de las empresas subcontratadas, asegurándose de los estándares que deben cumplir los proveedores y por medio de planes de continuidad de proveedores.

Los riesgos identificados y evaluados que pueden ocasionar una interrupción del servicio (que han de ser evaluadas independientemente) son:

- Huelga

- Caídas de los sistemas propios de la empresa de servicios.
- Incumplimiento de la normativa vigente por la empresa de servicios.
- Problemas de viabilidad de la empresa de servicios (situaciones concursales, cese de la actividad por cualquier otro motivo).
- Desastres naturales acaecidos en la empresa de servicios.

En el caso en que se hayan contratado los servicios de terceros, en procesos que sean considerados relevantes o críticos, la Organización evaluará la actividad de las empresas subcontratadas, asegurándose de los estándares que deben cumplir los proveedores.

Las posibles pérdidas derivadas de errores, fraude o malas actuaciones de las empresas subcontratadas se incorporan directamente a los cuestionarios de procesos de las distintas unidades de la organización, no siendo por tanto objeto de evaluación en los cuestionarios específicos de outsourcing, que recoge tan sólo los impactos directos derivados de eventuales interrupciones del servicio prestado por estas empresas o por riesgos en la gestión de la relación con la Empresa de Servicios.

- **Indicadores Clave de Riesgo (ICR) y Alertas**
  - Definición y Objetivos

    Un Indicador Clave de Riesgo Operacional (ICR), es una métrica cuyo seguimiento permite detectar y anticipar, en su caso, variaciones en el nivel de riesgo operacional de un proceso, facilitando la toma de decisiones que permitan mitigar dicho riesgo, así como comprobar la eficacia de determinadas acciones de mejora.

Los principales objetivos de la implementación de ICR son:

- Medir e informar la exposición de riesgo asociados a los procesos del Banco.
- Informar tendencias y desviaciones identificando las principales causas de la evolución.
- Establecer niveles de alerta para la toma de decisiones por parte de las diferentes áreas.
- Seguimiento a desviaciones por medio de planes de acción.

- Clasificación de los ICR y Criterios de Asignación

La metodología de clasificación por tipologías de los diferentes indicadores permitirá establecer criterios objetivos para la organización en la evaluación de la relevancia de los mismos así como facilitar un tratamiento agregado por tipologías.

Para ello, la organización a cada ICR lo clasificará de forma individual en las tipologías y según los criterios expuestos a continuación.

Se reconocen dos criterios complementarios de clasificación:

- Clasificación en función del resultado de su gestión

Esta clasificación se alcanza habitualmente en función del riesgo o las características del riesgo con el que se encuentra relacionado el indicador.

A.1. Eficiencia (reducción de Pérdidas Esperadas)

Son indicadores que detectan y, en determinados casos, anticipan posibles incrementos de riesgo que tendrían un efecto significativo sobre la **pérdida esperada**. Es decir, aquellos que de algún modo dan señales

o indicios sobre riesgos que presentan una alta frecuencia en su ocurrencia e impacto individual medio-bajo.

Estos indicadores habitualmente están relacionados con errores / incidencias recurrentes en las prácticas bancarias o con operativa que se encuentra sujeta a fraude externo de forma habitual.

El detalle de los criterios a emplear como referencia para determinar que un indicador se encuentra orientado fundamentalmente a la gestión de la Eficiencia se encuentra detallado en “Procedimientos de Indicadores Clave de Riesgo”.

A.2. Capital (control sobre Pérdidas Inesperadas)

Son indicadores que detectan y, en determinados casos, anticipan posibles incrementos de riesgo que tendrían un efecto significativo sobre la **pérdida inesperada.** Se focalizan en aquellos eventos de baja frecuencia y muy alto impacto (multiplicador elevado) que configuran finalmente la forma de la cola de la distribución de pérdidas y, por lo tanto, la cifra final de valor en riesgo.

Están relacionados con la detección de sucesos anómalos o excepcionales que de alguna forma quedan fuera del desenvolvimiento normal de las actividades de negocio.

El detalle de los criterios a emplear como referencia para determinar que un indicador de Riesgo Operacional tiene afectación a capital se

encuentra detallado en el “Procedimientos de Indicadores Clave de Riesgo”.

- Clasificación en función de las características del Indicador

La metodología de clasificación según la función de las características del indicador se detalla a continuación:

B.1. Genéricos (o volumétricos)

Son aquellos que recogen la evolución del volumen de la operativa en general, sin considerar las características particulares en la ejecución de un determinado proceso.

Se trata de indicadores de volumen de transacciones, operaciones, saldos de inversión, etc. que pueden presentar un mayor carácter predictivo si cuantifican la operativa que se desarrolla de forma manual o de especial riesgo.

El criterio establecido como referencia en la clasificación bajo esta categoría responde a lo siguiente:

- Métricas que definen las dimensiones de un proceso, organización, instalación, etc. por: el número de veces que se ejecuta el proceso, número de Unidades/oficinas/cajeros/clientes de una organización, número de servidores de una instalación e importes asociados (volúmenes, MIPs instalados, etc.).

- Métricas que miden la actividad de un proceso por los diferentes flujos que afectan a su situación final: número e importe de apertura de cuentas, cancelaciones anticipadas, cajeros instalados en el año, etc.

B.2. Orientados a procesos: Son indicadores específicos que se centran en los riesgos inherentes a los procesos de negocio.

Se puede distinguir entre **cuatro tipologías** de indicadores:

B.2.1. Indicadores relacionados con **errores o pérdidas consumadas (Loss - oriented):**

- Se definen tomando como base un hecho (error / incidencia) ya sucedido. Esta tipología de indicadores no tiene una propiedad predictiva del riesgo (anticipación de un incremento de Riesgo Operacional) sino que ofrecen una plataforma de análisis de los posibles fallos que se hayan producido en los procesos de negocio.

- No en todos los casos dichos errores desembocan en pérdidas operacionales directas, incluyen por tanto las denominadas cuasi-pérdidas.

- Se clasificarán en esta categoría los ICR que estén vinculados a eventos de Riesgo Operacional ya acaecidos en el tiempo que puede o no haberse materializado en pérdida. De forma similar se han podido producir o no recuperaciones sobre dichos eventos.

B.2.2. Indicadores orientados al **factor causal del riesgo (Risk – oriented)**

- Se definen considerando la causa que puede provocar un riesgo en un proceso con el fin de predecir la exposición al mismo.

- Se clasificarán en esta categoría los ICR que estén vinculados a:

  - Factores que puedan suponer un aumento/reducción del riesgo operacional;

  - Incidencias operacionales que no supongan una pérdida por sí sola pero que pueden constituir un factor causal de la ocurrencia de un determinado riesgo.

- Fases en su construcción:

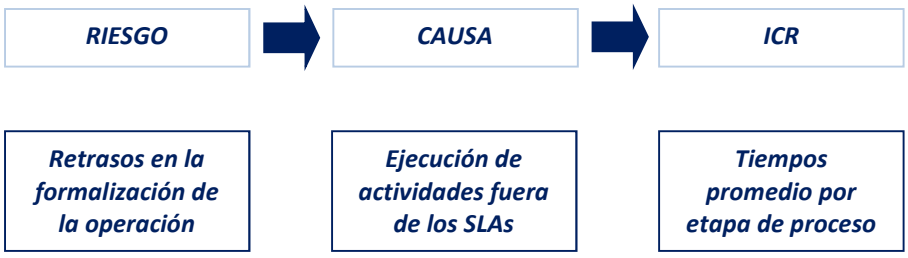

Ilustración 5: Fases de Construcción ICR B2.2., elaboración propia.

- Por último, los criterios establecidos como referencia en la clasificación bajo esta categoría responden a lo siguiente:

  - Indicadores que traten características relacionadas con factores del entorno o de los recursos empleados en la ejecución del proceso y que puedan afectar a un determinado riesgo – Ej. experiencia media de los empleados.

- Indicadores que segmenten la operativa por una determinada característica o los activos del Banco para identificar aquellos que presentan un mayor riesgo – Ej. oficinas pendientes de acometer el proceso de renovación si bien por antigüedad debería haberse emprendido.

B.2.3. Indicadores relacionados con **defectos en el entorno de control (Control – oriented)**

- Se definen considerando los fallos potenciales o reales en los controles establecidos sobre los Riesgos Operacionales de la Entidad.

- Se clasificarán en esta categoría los indicadores que tengan como objetivo el seguimiento del desarrollo, el alcance o la eficacia/ineficacia de un factor mitigante.

- Fases en su construcción:

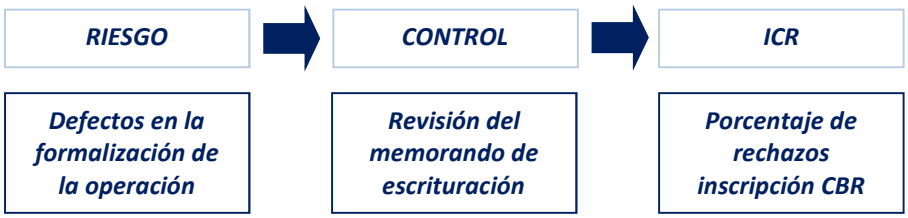

Ilustración 6: Fases de Construcción ICR B2.3., elaboración propia.

- Los criterios establecidos en la clasificación bajo esta categoría responden a lo siguiente:

- Métricas que traten sobre características de los factores mitigantes (controles) relacionados con determinados riesgos

- Métricas relacionadas con el grado de cobertura (% sobre total operativa), eficacia (% de detección de riesgos) y capacidad de resolución (número de veces que se evita que el riesgo se materialice) de los controles establecidos sobre los riesgos.

- Se consideran todo tipo de factores mitigantes incluidos los seguros.

B.2.4. Indicadores orientados a la identificación de **puntos de riesgo (RPA):**

- Su definición requiere un análisis exhaustivo de los procesos con el fin de detectar los puntos de vulnerabilidad de los mismos que puedan devenir en un riesgo.

- Estos indicadores pueden no guardar una relación obvia con un riesgo concreto y su definición requiere de un conocimiento profundo de los procesos de negocio.

- Detectan prácticas no habituales o que puedan ser originadas por una problemática que implique riesgo operacional.

- Categorización de los ICRs en función del objetivo de la métrica.

Los objetivos del indicador de Riesgo Operacional pueden clasificarse mediante dos dimensiones distintas:

1. **Afectación**: El indicador puede pretender cuantificar variaciones en la frecuencia de aparición de eventos de pérdida, en variaciones en la severidad asociadas a las mismas o en ambas. Ejemplos:

   - **Frecuencia:** número de tarjetas con los que cuenta la entidad. (cabe esperar que la variación en el número de tarjetas acarree una variación en el número de eventos de pérdidas registradas –p.e. fraude externo).

   - **Severidad:** Importe medio de los hurtos al descuido en las oficinas ocurridos en los últimos 6 meses (un incremento en el importe medio de las pérdidas registradas puede ser un indicativo de un aumento en la severidad del riesgo).

2. **Tipo de vinculación con el riesgo**: El indicador puede tener sentido por sí mismo (número o porcentaje que representa) o puede que sólo sea indicativo en términos de Riesgo Operacional si se producen variaciones significativas del mismo. Ejemplos:

   - **Directa:** número de atracos en sucursales en los últimos 6 meses. (directamente relacionado con las pérdidas).

   - **Variación significativa:** número de reclamaciones recibidas por parte de clientes relativas a Banca Electrónica (en la operativa normal de la Entidad se recibe un número significativo de éstas, relacionado con las incidencias diarias del propio negocio, pero si el número de éstas aumenta considerablemente en un corto periodo puede ser indicador de

que puede existir un fallo en la definición de un producto, en el software que gestiona la operativa, en el proceso de ejecución, etc…).

- Relevancia Asociada a los ICRs

Los indicadores considerados más significativos para la gestión se marcarán como relevantes[9] con objeto de focalizar los esfuerzos por parte de la organización en aquéllos más significativos.

La categorización mostrada en los apartados anteriores permite asimismo actuar como una referencia en la identificación de los indicadores relevantes. Así, la Unidad de Riesgo Operacional establece como criterios de referencia a la hora de aplicar la relevancia, aquellos indicadores relevantes los vinculados a **capital** (control sobre pérdidas inesperadas), y de carácter **predictivo** - orientados al factor causal de riesgo, relacionados con defectos en el entorno de control o dirigidos a la identificación de puntos de mejora[10].

En cualquier caso podrán ser considerados indicadores relevantes aquellas métricas de carácter subjetivo, que por sus características puedan aportar un alto valor en la gestión del Riesgo Operacional.

Se pueden incorporar como relevantes indicadores para seguir situaciones o acciones puntuales que surjan en el tiempo, a instancias de los gestores, de responsables de las Direcciones, de la Unidad de Riesgo Operacional o

9 Implica la realización de un seguimiento centralizado por parte de la Unidad de Riesgo Operacional, como elemento adicional al propio seguimiento que realizan las propias Áreas de Negocio
10 Ver mayor detalle de criterios en la determinación de ICRs relevantes, en "Procedimiento de Indicadores Clave de Riesgo".

del Comité Global de Riesgos, sobre los que se ha considerado conveniente realizar un seguimiento especial.

En sentido contrario, si indicadores catalogados como relevantes dejan de serlo por las circunstancias de su evolución, se les podrá eliminar esta condición. Las incorporaciones, modificaciones y bajas las ejecuta la Unidad de Riesgo Operacional, que revisa la idoneidad de las mismas de forma consensuada con cada responsable que las propone.

- **Metodologías de Evaluación Cuantitativas**
- **Base de Datos de Eventos de Pérdida**

La Base de Datos de Eventos de Pérdida (en adelante BDP), es una herramienta cuantitativa para el registro de eventos de pérdida por Riesgo Operacional y Tecnológico, experimentados en cada División, Área, Departamento o Unidad de la organización.

El objetivo fundamental de la BDP es la captura de la totalidad de las pérdidas por RO registradas además en Contabilidad a través de las cuentas de pérdidas Basilea II Nivel 2. La BDP debe estar alineada con la política definida para Riesgo Operacional y el Manual de Castigos.

5. CONCLUSIONES

La aplicación de Basilea II presenta diversos desafíos a las entidades que quieran con este requerimiento de capitales, Chile es un país que a mediados del 2004 recién comenzaba a dar sus primeros pasos formando unidades de Riesgo Operacional en los distintos Bancos de la plaza por requerimiento expreso de la Superintendencia de Bancos e Instituciones Financieras, estamento que en ese entonces también se encontraba en una etapa inicial, con el paso de los años, este regulador comenzó a exigir mayor lineamiento con las directrices Basilea, lo que llevo a las distintas instituciones a tomar medidas para el cumplimento de estas solicitudes. Cada año las exigencias aumentan ya que existe mayor experiencia tanto por regulador como el regulado.

El banco analizado, si bien se encuentra en un buen pie, aún requiere avanzar en distintos lineamientos donde aún se encuentra en un nivel bajo. El avanzar requiere del compromiso de toda la organización, siendo lo más importante contar con el apoyo de la alta administración, ya que esta debe velar por la correcta aplicación de las políticas y metodologías, la complejidad de esto requiere contar con herramientas que aún la institución no tiene disponibles, como lo es una herramienta TI para el registro, seguimiento, monitoreo y control de los riesgos inherentes y residuales.

5.1. Recomendaciones.

La complejidad de realizar los cálculos de las pérdidas por Riesgo Operacional es similar a las de Riesgo de Mercado, ya que las variables son muchas y su interacción compleja, es por esto que se requiere contar en principio con una metodología, como la propuesta en este trabajo, donde se decida la estrategia a seguir por la institución para llevar a cabo la gestión del riesgo operacional. Una vez realizado esto, se debe contar con el apoyo de la Alta Administración para su puesta en marcha, será la Alta Administración responsables del seguimiento del plan de trabajo.

Luego se recomienda realizar una inversión en alguna herramienta que permita aplicar la metodología, actualmente en el Mercado existe una amplia gama de Software que permite realizar esta tarea.

Algo que no se encontró en la revisión y es vital para la aplicación de medidas mitigantes previas a la pérdida son los KRI, se recomienda trabajar fuertemente en la creación de un panel de control de riesgo operacional que permita a la institución realizar acciones preventivas previas a la materialización de las pérdidas.

Finalmente y luego de realizar un levantamiento de las pérdidas internas de la organización se requiere contar con una base de datos externa, la cual representa nuevos desafíos, ya que los procesos y productos entre cada institución pueden ser diametralmente distintos.

Con estos cambios se espera que la institución logré un alto nivel de gestión de sus riesgos operacionales, lo que conlleva directamente a mejorar la calidad de sus procesos, eficiencia operacional, reducción de costos y reducción de pérdidas.

6. BIBLIOGRAFÍA

BIS, 2003. Sound Practices for the Management and Supervision of Operational Risk - final document. 14p

Cevallos F., 2008, Metodologías y sistemas de información requeridos para la medición y mitigación del riesgo operativo 208p.

BIS, 2005. Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework. 284p.

Pacheco, D. 2009. Riesgo Operacional: Conceptos y Mediciones. 55p.

Held, G. 2012. Suficiencia de capital de los bancos: Estándares del Comité de Basilea. 19p.

Troncoso B., M. Z. 2006. Proposición de una metodología para la evaluación de Riesgo Operacional en las Instituciones Financieras acorde a la recomendación del Comité de Basilea: Una aplicación al caso chileno. 83p.

Fernández A., Martínez G., 2006. Bases del marco conceptual del riesgo operacional: Fin de una etapa. VI Jornadas sobre predicción de la insolvencia empresarial.

Sbif, 2013. Recopilación Actualizada de Normas (RAN) – Capitulo 1-13, Clasificación de gestión y solvencia, Circular N° 3.558, 26p.

Fernández-Laviada, Ana, 2008. La gestión del riesgo operacional: de la teoría a su aplicación, 609p.

Jiménez Rodríguez E. 2013. El capital regulatorio por riesgo operacional, 86p.

Acuña, P., Villa, N., 2006. Aspectos Teóricos y prácticos del muestreo no estadístico en la Auditoría. 116p.

ANEXO Y APENDICES

Anexo N°1:

DEFINICIONES DE CATEGORIAS
(Artículo 60 Ley General de Bancos)

Clasificaciones vigentes		CATEGORIAS según el nivel de gestión anterior:		
Nivel de gestión	Nivel de solvencia	Nivel A (o sin clasificación)	Nivel B	Nivel C
A	A	I	I	I
A	B	II	II	II
B	A	II	II	II
B	B	II	III	III
C	A	III	III	IV
C	B	III	III	IV
Cualquiera	C	V	V	V

Ilustración 7: Definiciones de Categorías de la Matriz de Autoevaluación de Gestión y Solvencia. Sbif RAN 1-13, Anexo N°1.

Anexo N°2: Preguntas de la Matriz de Autoevaluación 2014, Clasificación de Gestión y Solvencia, Riesgo Operacional:

CódigoP	Ámbito	Pregunta de Evaluación
01.001	Administración y Evaluación de Riesgos	El directorio y la Alta administración demuestran tener claro conocimiento de las leyes que pudiesen afectar al negocio y por lo cual se comprometen de alguna forma en mantener un comportamiento intachable.
01.002	Administración y Evaluación de Riesgos	Existe una función dentro de estructura organizacional encargada de la administración del riesgo operacional.
01.003	Administración y Evaluación de Riesgos	La entidad administra los riesgos operacionales considerando los impactos que pudieran provocar en la institución (severidad de la pérdida) y la probabilidad de ocurrencia de los eventos.
01.004	Administración y Evaluación de Riesgos	La entidad conoce y se actualiza acerca de las normativas y/o leyes internacionales, que puedan influir directamente en los negocios en que participa (Exportaciones, Importaciones, etc.)
01.005	Administración y Evaluación de Riesgos	La entidad cuenta con respaldos necesarios sobre documentaciones sensibles (contratos, pagares, títulos, cartas de crédito, boletas de garantía etc.), con el fin de proteger tanto a sus clientes como así mismos.
01.006	Administración y Evaluación de Riesgos	La entidad realiza evaluaciones del riesgo operacional inherente a todos los tipos de productos, actividades, procesos y sistemas.
01.007	Administración y Evaluación de Riesgos	La entidad se asegura que antes de introducir nuevos productos, emprender nuevas actividades, o establecer nuevos procesos y sistemas, el riesgo operacional inherente a los mismos esté sujeto a procedimientos de evaluación.
01.008	Administración y Evaluación de Riesgos	La institución es capaz de cuantificar los impactos de las pérdidas asociadas al riesgo operacional y constituir prudencialmente los resguardos necesarios.

CódigoP	Ámbito	Pregunta de Evaluación
02.001	Auditoría	La función de auditoría está en posición de evaluar en forma independiente el cumplimiento de las políticas, la eficacia de los procedimientos y los sistemas de información.
03.002	Continuidad del Negocio	El banco cuenta con una metodología o procedimiento formal, que informe y capacite al personal sobre las políticas y planes de continuidad de negocio, como así también que facilite a cada Área o Unidad de Negocio de la Organización contar con la información necesaria para desarrollar dichos planes?
03.003	Continuidad del Negocio	El Banco ha desarrollado pruebas de continuidad de negocio bajo el escenario de contingencia tecnológica (DRP).
03.004	Continuidad del Negocio	El banco ha desarrollado un marco metodológico para la administración de las contingencias tecnológicas (DRP) y éste se encuentra alineado a las estrategias de Negocio de la institución.
03.005	Continuidad del Negocio	El banco ha desarrollado una metodología formal que considera, la evaluación de impacto y criticidad de sus servicios y productos, la definición de estrategias de prevención, contención y recuperación.
03.006	Continuidad del Negocio	El Banco realiza pruebas sobre los planes de continuidad de negocio establecidos, y estos son acordes con el tamaño y complejidad de las operaciones.
03.007	Continuidad del Negocio	El banco y sus divisiones, tienen planes de continuidad del negocio Operacionales, que consideren diversos escenarios y supuestos que pudieran impedir que cumpla toda o parte de sus obligaciones.
04.001	Control y Monitoreo	El banco ha identificado indicadores apropiados que entreguen alertas de un aumento del riesgo y de futuras pérdidas.
04.002	Control y Monitoreo	El banco ha integrado a sus actividades normales el monitoreo del riesgo operacional

CódigoP	Ámbito	Pregunta de Evaluación
04.003	Control y Monitoreo	La institución ha implementado un proceso para controlar permanentemente la organización de nuevas políticas, procesos y procedimientos, que permiten detectar y corregir sus eventuales deficiencias de manera de reducir la frecuencia y severidad de los eventos de pérdida.
05.001	Estrategias	La entidad bancaria ha adoptado una estrategia y sistema de gestión de calidad respecto de sus productos, servicios, e información que suministra a sus clientes, reguladores y a otros entes.
05.002	Estrategias	La estrategia de riesgo operacional ha sido implementada a través de toda la organización bancaria.
05.003	Estrategias	La estrategia definida considera el nivel de tolerancia al riesgo del banco, incluyendo líneas específicas de responsabilidad
05.004	Estrategias	La estrategia definida es consistente con el volumen y complejidad de sus actividades.
05.005	Estrategias	La Institución tiene definida una estrategia de administración del riesgo operacional.
05.006	Estrategias	Las decisiones sobre nuevos negocios u operaciones con contrapartes radicadas en el exterior, son tomadas sobre la base de un análisis previo de todos los riesgos inherentes, cubriéndose en consecuencia, sistemáticamente, el riesgo país, el riesgo de crédito, el riesgo financiero, el riesgo legal y el riesgo operativo que derive de las peculiaridades de las operaciones.
07.001	Organización	Existe alguna dependencia que se encargue del control interno con el fin de obtener un seguimiento del control de las políticas que son propias del riesgo legal, como así también la formalización y liberación de las garantías.
07.002	Organización	Existe un gobierno corporativo que administre el modelo de Gestión de Riesgo Operacional y una función específica encargada de la coordinación e implementación del Modelo.

CódigoP	Ámbito	Pregunta de Evaluación
07.003	Organización	La entidad cuenta con alguna división o similar se encargue de gestionar y publicar los hechos más relevantes relacionados con el ámbito legal y sus riesgos.
07.004	Organización	Todos los niveles del personal asumen y comprenden sus responsabilidades respecto a la administración del riesgo operacional.
08.001	Políticas y Procedimientos	La entidad cuenta con un marco metodológico de riesgo Operacional basado en las mejores prácticas, que permita identificar, gestionar y mitigar los Riesgos.
08.002	Políticas y Procedimientos	La entidad elabora procedimientos y cualquiera similar que permita tener un correcto seguimiento de los convenios, contratos y otros de esta índole.
08.003	Políticas y Procedimientos	La entidad ajusta de acuerdo a las necesidades o contingencias los manuales, procedimientos y cualquiera similar que permita tener un correcto seguimiento de los convenios, contratos y otros de esta índole.
08.004	Políticas y Procedimientos	La entidad aplica manuales, procedimientos y cualquiera similar que permita tener un correcto seguimiento de los convenios, contratos y otros de esta índole.
08.005	Políticas y Procedimientos	La entidad ha creado políticas, y/o procedimientos en que se reconozca la existencia de un riesgo legal de cualquier grado o competencia
08.006	Políticas y Procedimientos	La entidad ajusta de acuerdo a las necesidades o contingencias las políticas, y/o procedimientos en que se reconozca la existencia de un riesgo legal de cualquier grado o competencia
08.007	Políticas y Procedimientos	La entidad aplicada políticas, y/o procedimientos en que se reconozca la existencia de un riesgo legal de cualquier grado o competencia
08.008	Políticas y Procedimientos	La entidad ha elaborado manuales, guías o documentos oficiales en los cuales se deje claramente establecidos los deberes y/o derechos que deben cumplir los clientes al adquirir productos y/o servicios del banco

CódigoP	Ámbito	Pregunta de Evaluación
08.009	Políticas y Procedimientos	La entidad ajusta de acuerdo a las necesidades o contingencias los manuales, guías o documentos oficiales en los cuales se deje claramente establecidos los deberes y/o derechos que deben cumplir los clientes al adquirir productos y/o servicios del banco
08.010	Políticas y Procedimientos	La entidad aplica manuales, guías o documentos oficiales en los cuales se deje claramente establecidos los deberes y/o derechos que deben cumplir los clientes al adquirir productos y/o servicios del banco
08.011	Políticas y Procedimientos	La entidad ha hecho participe a las personas que laboran dentro de la organización sobre las normas y/o políticas legales que influencian directamente en los riesgos legales.
08.012	Políticas y Procedimientos	La entidad ha reconocido y definido las leyes y/o normas jurídicas que representan un mayor riesgo legal.
08.013	Políticas y Procedimientos	El Banco tiene una definición de lo que entiende por riesgo operacional y lo ha reconocido como un riesgo gestionable.
08.014	Políticas y Procedimientos	La entidad ajusta según las necesidades las políticas para la administración de los riesgos aprobadas por el directorio o la administración superior.
08.015	Políticas y Procedimientos	La entidad aplica las políticas para la administración de los riesgos aprobadas por el directorio o la administración superior.
08.016	Políticas y Procedimientos	Las políticas atienden la importancia de los riesgos considerando el volumen y complejidad de las operaciones.
09.001	Tecnologías de Información y Sistemas	¿Existe un comité de dirección que vigile la función de TI y sus actividades? ¿El Comité está compuesto por miembros que representen a la alta gerencia, mandos medios y de la unidad de "TI"?

CódigoP	Ámbito	Pregunta de Evaluación
09.002	Tecnologías de Información y Sistemas	¿Existen en los Centro de Procesamiento de Datos, equipos, procedimientos y personal que permiten mantener las condiciones medioambientales adecuadamente, incluyendo la extinción de fuego, servicio ininterrumpido eléctrico, aire acondicionado, piso falso, entre otros?
09.003	Tecnologías de Información y Sistemas	¿La Organización de TI monitorea el progreso contra el plan estratégico y reacciona de acuerdo con el establecimiento de los objetivos?
09.004	Tecnologías de Información y Sistemas	¿Son las estrategias de TI y los temas en curso formalmente comunicados a la alta gerencia y al directorio, por ejemplo a través de reuniones periódicas de un directivo de "TI"?
09.005	Tecnologías de Información y Sistemas	Confía la Gerencia TI, en la evaluación continua de riesgos, como una herramienta que proporciona información sobre el diseño y la implementación de controles internos, y en la definición del plan estratégico, y en los mecanismos de monitoreo y evaluación?
09.006	Tecnologías de Información y Sistemas	El banco cuenta con una adecuada planificación a largo plazo para la infraestructura tecnológica y dispone de los recursos necesarios para el desarrollo normal de sus actividades y para que los nuevos proyectos previstos se concreten oportunamente.
09.007	Tecnologías de Información y Sistemas	El banco cuenta con una estructura que permite administrar la seguridad de la información en términos de resguardar su confidencialidad, integridad y disponibilidad.
09.008	Tecnologías de Información y Sistemas	El Banco dispone de los recursos necesarios para el desarrollo normal de sus actividades y para que los nuevos proyectos previstos se concreten oportunamente.
09.009	Tecnologías de Información y Sistemas	El banco realiza inversiones en tecnología de procesamiento y seguridad de la información, que permiten mitigar los riesgos operacionales y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.

CódigoP	Ámbito	Pregunta de Evaluación
09.010	Tecnologías de Información y Sistemas	El plan de auditoría está basada sobre la evaluación de riesgos de TI?, ¿El plan incluye la totalidad de los procesos de TI? por ejemplo controles generales y de aplicación, ciclos de vida del desarrollo de sistemas?
09.011	Tecnologías de Información y Sistemas	Es evaluado el personal de TI Periódicamente? (con el objeto de validar que la continuidad del servicio esté asegurado por personal capacitado e idóneo)
09.012	Tecnologías de Información y Sistemas	Es evaluado el personal de TI Periódicamente? (con el objeto de validar que la función de TI está asegurada con el número de personal para lograr los objetivos)
09.013	Tecnologías de Información y Sistemas	Están documentados los estándares, y son debidamente comunicados a todo el equipo de TI?
09.014	Tecnologías de Información y Sistemas	Existe un mecanismo de control de acceso al Centro de Procesamiento de Datos solo a personal autorizado, y se les exige identificarse en forma apropiada con medios de autenticación?
09.015	Tecnologías de Información y Sistemas	Existe un plan para mantener la calidad de las actividades de TI basadas sobre los planes organizacionales y de TI?
09.016	Tecnologías de Información y Sistemas	Existe un procedimiento de manejo de la administración de incidentes y problemas, y además que genere los planes de acción necesarios?
09.017	Tecnologías de Información y Sistemas	Existe una documentación, para todos los procesos, actividades y controles significativos de TI?
09.018	Tecnologías de Información y Sistemas	Existe una evaluación de la seguridad de información, para los sistemas o Centro de Procesamiento de Datos críticos, basado en la prioridad e importancia para la organización?
09.019	Tecnologías de Información y Sistemas	Existen procedimientos para realizar seguimientos oportunamente, a las tareas de control de Auditoria Ti?

CódigoP	Ámbito	Pregunta de Evaluación
09.020	Tecnologías de Información y Sistemas	Fiscalía cuenta con los sistemas necesarios, para el cumplimiento de requerimientos legales, regulatorios u otros relacionados?
09.021	Tecnologías de Información y Sistemas	La administración de TI ha comunicado las políticas y procedimientos que gobiernan las actividades de TI en la Organización
09.022	Tecnologías de Información y Sistemas	La administración de TI ha formulado, desarrollado y documentado políticas y procedimientos que gobiernan las actividades de TI en la Organización ?
09.023	Tecnologías de Información y Sistemas	La administración de TI comunica sus actividades , desafíos y riesgos en forma regular al Gerente General y al Gerente de Gestión y Control Financiero ? Es la información también compartida con el directorio?
09.024	Tecnologías de Información y Sistemas	La administración periódicamente realiza la revisión de sus políticas, procedimientos y normas para reflejar los cambios en las condiciones de negocio?
09.025	Tecnologías de Información y Sistemas	La administración tiene procedimientos vigentes para investigar y evaluar las desviaciones de cumplimiento de las normas TI e introduce acciones correctivas?
09.026	Tecnologías de Información y Sistemas	La entidad emite reportes con la información pertinente a la Alta Administración y Directores.
09.027	Tecnologías de Información y Sistemas	La Gerencia de TI realiza monitoreos al desempeño y niveles de servicio, a los sistemas de información y redes?
09.028	Tecnologías de Información y Sistemas	La Gerencia de TI, ha establecido indicadores que permitan medir diariamente el desempeño de las actividades de TI, y la vez entrega información o reporte sobre las deficiencias?
09.029	Tecnologías de Información y Sistemas	La Gerencia de TI, recibe reportes de control interno de proveedores de servicios (Ej., obtener y revisar reportes de SAS 70, u otros informes de la auditoria independientes)?

CódigoP	Ámbito	Pregunta de Evaluación
09.030	Tecnologías de Información y Sistemas	La Organización de TI suscribe una Metodología de aprendizaje continuo y proporciona el entrenamiento necesario y el desarrollo de habilidades para los miembros de la organización?
09.031	Tecnologías de Información y Sistemas	La organización tiene un departamento de Auditoría Interna, que cumpla el rol de evaluar las actividades y controles de los sistemas de información?
09.032	Tecnologías de Información y Sistemas	Los controles internos, son evaluados periódicamente, usando auto evaluaciones o auditorias independientes, para examinar si los controles internos están operando satisfactoriamente?
09.033	Tecnologías de Información y Sistemas	Los sistemas de información permiten hacer un monitoreo continuo de la exposición a los riesgos operacionales.
09.034	Tecnologías de Información y Sistemas	Los sistemas de información poseen la cobertura y profundidad necesarias para servir en forma eficiente al proceso de toma de decisiones de la Alta administración y Directorio.
09.035	Tecnologías de Información y Sistemas	Monitorea la organización los cambios en las prácticas o controles TI, como los eventos internos para el cumplimiento de requerimientos legales, regulatorios u otros relacionados?
09.036	Tecnologías de Información y Sistemas	Proporciona la Organización educación y programas de entrenamiento continuos que incluyan la conducta ética, prácticas de seguridad de sistemas , estándares de confidencialidad , estándares de integridad y responsabilidades de seguridad a todo el personal, como así también políticas para la protección de los recursos de información ?
09.037	Tecnologías de Información y Sistemas	Se ha realizado una evaluación del impacto, el cual considera las fallas sobre los sistemas de información financiera?

CódigoP	Ámbito	Pregunta de Evaluación
10.001	Servicios Externos / Proveedores	El banco cuenta con políticas para administrar los riesgos asociados a las actividades entregadas a terceras partes y lleva a cabo verificaciones y monitorios a las actividades de dichas partes.
10.002	Servicios Externos / Proveedores	El banco lleva a cabo verificaciones y monitoreos a las actividades entregadas a terceras partes que realizan procesos críticos.

Anexo N°3: Resumen de petitorios realizados por la Superintendencia de Bancos e Instituciones Financieras para el análisis de situación actual de un Banco:

	Petitorio
1	**Gobierno Corporativo**
1.1	Estructura de Riesgo Operacional (Comités, Organigrama, Colaboradores Internos, Auditoría)
1.2	Funciones de los distintos Comités existentes.
1.3	Funciones de las Unidades de Riesgo Operacional
1.4	Funciones de los distintos responsables de la gestión de Riesgo Operacional
1.5	Funciones de la Auditoría de Riesgo Operacional
1.6	Actas y estatutos de los Comités de Riesgo Operacional existentes.
2	**Modelo Riesgo Operacional**
2.1	Modelo de gestión actualizado de Riesgos Operacionales incluyendo documentación acerca de las instancias de aprobación
2.2	Metodología de Evaluación de Riesgo Operacional
2.3	Metodología de Evaluación de Riesgos Tecnológicos.
2.4	Metodología de Evaluación de Proveedores Críticos
2.5	Metodología de Gestión de Activos de Información.
2.6	Metodología de Evaluación de nuevos productos o nuevos servicios.
2.7	Programa Revisión Anual Evaluación de Riesgo Operacional
2.8	Programa Revisión Anual Evaluación de Riesgos Tecnológicos.
2.9	Programa Revisión Anual Evaluación de Proveedores Críticos
2.10	Programa Revisión Anual Gestión de Activos de Información.

	Petitorio
2.11	Plan de Capacitación respecto Evaluación de Riesgo Operacional
2.12	Plan de Capacitación respecto Evaluación de Riesgos Tecnológicos.
2.13	Plan de Capacitación respecto Evaluación de Proveedores Críticos
2.14	Plan de Capacitación respecto Gestión de Activos de Información.
2.15	Políticas de Riesgo Operacional vigentes y copias de actas del Directorio con aprobaciones de eventuales modificaciones.
2.16	Mapa de Procesos, identificando aquellos considerados como críticos para la gestión integral de riesgo operacional.
2.17	Mapa de Procesos incorporando LA PRIORIZACIÓN, estado de avance por proceso y etapa en que se encuentra.
2.18	Matrices de riesgo y controles generadas producto de la aplicación del modelo de gestión de riesgos
2.19	Base de datos de eventos de pérdida y base de registros de incidentes de riesgo operacional (detallar la información contenida en cada campo).
2.20	Avances en la identificación de áreas fuentes de incidentes.
2.21	Fuentes de información para base de incidentes operacionales
2.22	Relación de Procesos v/s Pérdidas
2.23	Nómina de Indicadores claves de riesgos generados por el área de riesgo operacional y su grado de implementación (objetivos del indicador, umbrales, unidad de medida, etc.)
2.24	Nómina de planes de acción del año con su estado de implementación.
2.25	Nómina de empresas asesoras y descripción detallada de los trabajos realizados.
3	**Informes de Gestión**
3.1	Informes de gestión de Riesgo Operacional (incluir su distribución)
3.2	Informes de gestión de Riesgos Tecnológicos (incluir su distribución)
3.3	Informes de revisión de Proveedores Críticos (incluir su distribución)

	Petitorio
3.4	Informes de levantamiento de Activos de Información (incluir su distribución)
3.5	Informes de revisión de nuevos productos o nuevos servicios (incluir su distribución)

Anexo N°4: Tipología de Evento de Pérdida

Basilea Nivel 1	Basilea Nivel 2	Categoría Interna Nivel 3
FRAUDE INTERNO	ACTIVIDADES NO AUTORIZADAS	TRANSACCIONES REGISTRADAS INCOMPLETAS O NO REGISTRADAS, INTENCIONALMENTE
		TRANSACCIONES INGRESADAS SIN AUTORIZACIÓN
		USO INDEBIDO DE FACULTADES Y PODERES
		DIVULGACIÓN DE INFORMACIÓN PRIVILEGIADA
		APERTURA DE PRODUCTO SIN AUTORIZACIÓN DEL CLIENTE, CON FIN DE LUCRO
		INCUMPLIMINETO DE LÍMITES CON FIN DE LUCRO
		MANEJO DE LA POSICIÓN CON FIN DE LUCRO
	ROBO Y FRAUDE	USO FRAUD DE CLAVES DE ACCESO Y/O NIVELES DE AUTORIZACIÓN
		DEPÓSITOS O PAGO NO INGRESADO INTENCIONALMENTE
		DIFERENCIAS O DESCUADRATURAS EN CAJA POR DESFALCO / MALVERSACIÓN
		ROBO DE BIENES Y/O ACTIVOS
		FALSIFICACIÓN DE DOCUMENTOS o CLONACION DE PRODUCTOS (TARJETAS)
		EXTORSIÓN Y SOBORNO
		COMERCIALIZACIÓN DE INFORMACIÓN PRIVILEGIADA
		ROBO FÍSICO DE LA PROPIEDAD INTELECTUAL
		NO ENTERO DE IMPUESTOS / EVASIÓN INTENCIONAL POR PARTE DE LA INSTITUCIÓN
FRAUDE EXTERNO	ROBO Y FRAUDE	ROBOS Y ATRACOS PERPETRADOS CONTRA ACTIVOS DEL BANCO
		USO FRAUDULENTO DE TARJETA DE DÉBITO O CRÉDITO, EN COMPRAS, POR TITULAR
		USO FRAUDULENTO DE TARJETA DE DÉBITO O CRÉDITO, EN GIROS, POR TITULAR
		USO FRAUDULENTO DE TARJETA DE DÉBITO O CRÉDITO, EN COMPRAS, POR TERCEROS
		USO FRAUDULENTO DE TARJETA DE DÉBITO O CRÉDITO, EN GIROS, POR TERCEROS
		USO FRAUDULENTO DE CHEQUES, POR CLIENTE

Basilea Nivel 1	Basilea Nivel 2	Categoría Interna Nivel 3
		USO FRAUDULENTO DE TRANSFERENCIAS(INTERNET), POR CLIENTE
		USO FRAUDULENTO CHEQUES, POR TERCEROS (INCLUYE ONP Y FIRMA DISCONFORME), CAJA
		USO FRAUDULENTO CHEQUES, POR TERCEROS (INCLUYE ONP Y FIRMA DISCONFORME), CANJE
		USO FRAUDULENTO DE TRANSFERENCIAS(INTERNET), POR TERCEROS
		FALSIFICACIÓN DE DOCUMENTOS (VV, CHEQUES, BG, PAGARE)
		PAGO DE VALE VISTA CON DOCUMENTOS FALSIFICADOS (CI, Poder)
		PRODUCTOS OTORGADOS A TERCEROS POR SUPLANTACIÓN DE IDENTIDAD
		USO Y/O DIVULGACIÓN DE INFORMACIÓN PRIVILEGIADA
		ESPIONAJE INDUSTRIAL
		EXTORSIÓN Y SOBORNO
		SECUESTROS Y RESCATES
		CONTRABANDO
		DEVOLUCIÓN DE COMISIONES, ASOCIADO A FRAUDE
		DEVOLUCIÓN DE IMPUESTOS, ASOCIADO A FRAUDE
		DEVOLUCIÓN INTERESES, ASOCIADO A FRAUDE
	SEGURIDAD DE SISTEMAS	FRAUDE A TRAVÉS DE SISTEMAS
		ROBO DE INFORMACIÓN
		DAÑOS POR HACKEO
		ACCESO NO AUTORIZADO A SISTEMA
PRACTICAS LABORALES Y SEGURIDAD EN EL TRABAJO	RELACIONES CON EMPLEADOS	DEFICIENCIA EN LA CONTRATACIÓN Y RETENCIÓN DE RR.HH., INCLUIDA COBERT DE VACANTES
		DESPIDOS IMPROCEDENTES
		HUELGAS
		RETRIBUCIÓN DE BENEFICIOS SOCIALES
		INCUMPLIMIENTO DE CONTRATO DE TRABAJO
	AMBIENTE DE SEGURIDAD	INCUMPLIMIENTO DE REGLAS DE SEGURIDAD LABORAL
		INCUMPLIMIENTO DE REGLAS DE HIGIENE LABORAL
		DESTRUCCIÓN MALEVOLA DE BIENES, SABOTAJE
		RESPONSABILIDAD GENERAL COMO RESBALONES Y CAIDAS

Basilea Nivel 1	Basilea Nivel 2	Categoría Interna Nivel 3
PRACTICAS LABORALES Y SEGURIDAD EN EL TRABAJO	DIVERSIDAD Y DISCRIMINACION LABORAL	DISCRIMINACIÓN DE TODO TIPO
		DIFAMACIÓN E INVASIÓN DE LA INTIMIDAD
		ACOSO PERSONAL
CLIENTES, PRODUCTOS Y PRÁCTICAS DE NEGOCIO	APLICABILIDAD, DIVULGACIÓN PUBLICA DE INFORMACIÓN Y NEGOCIO FIDUCIARIO	INCUMPLIMIENTO FIDUCIARIO/ INFRACCIÓN DE NORMAS
		APLICABILIDAD O DIVULGACIÓN PUBLICA DE INFORMACIÓN
		INCUMPLIMIENTO DE PRIVACIDAD
		VENTAS AGRESIVAS
		RESPONSABILIDAD DEL PRESTAMISTA
		CONVENIENCIA (KYC - KNOW YPOUR CUSTUMER)
	PRACTICAS DE NEGOCIO O DE MERCADO IMPROPIAS	INCUMPLIMIENTO DE LA NORMATIVA DE LA COMPETENCIA
		DISCRIMINACIÓN
		DUMPING
		VENTA ENGAÑOSA Y OCULTACIÓN DE RIESGOS
		LAVADO DE DINERO
		OTRAS ACTIVIDADES ILÍCITAS
		RESPONSABILIDAD HEREDADA DE EVENTOS ANTERIORES A LA ADQUISICIÓN O FUSIÓN
	DEFECTOS EN PRODUCTOS	PRODUCTOS DEFECTUOSOS (Cheques, VV u otro producto mal emitido)
		GASTOS NO CUBIERTOS POR SEGURO DE DESGRAVAMEN
	SELECCION DE CLIENTES, PATROCINIO Y LIMITES DE EXPOSICION	ERROR EN LA INVESTIGACIÓN Y SELECCIÓN DE CLIENTES DE ACUERDO A PAUTAS
		CLIENTES CON LIMITES DE RIESGO EXCEDIDOS
	ACTIVIDAD DE ASESORAMIENTO	ASESORAMIENTO DEFICIENTE A CLIENTES POR EJECUTIVO DE CARTERA
		ACTIVIDAD CON CLIENTES NO AUTORIZADOS / TERCERAS PARTES
	DECISION COMERCIAL	DEVOLUCIÓN DE CARGO DESCONOCIDO POR CLIENTE, POR GESTIÓN COMERCIAL
		DEVOLUCIÓN DE COMISIONES, POR GESTIÓN COMERCIAL

Basilea Nivel 1	Basilea Nivel 2	Categoría Interna Nivel 3
		DEVOLUCIÓN DE IMPUESTOS, POR GESTIÓN COMERCIAL
		DEVOLUCIÓN INTERESES, POR GESTIÓN COMERCIAL
		DEVOLUCIÓN DE CARGOS, POR CHEQUE DESCONOCIDO POR CLIENTE, (Firma no visiblemente disconforme)
		DEVOLUCIÓN POR RETENCIÓN O TOMA NUEVO PRODUCTO
		DEVOLUCIÓN DE SEGUROS, POR GESTIÓN COMERCIAL
		DEVOLUCIÓN A CLIENTE POR BILLETE FALSO
		DEVOLUCIÓN A CLIENTE POR DIFERENCIA EN ATM (HUINCHA SIN ERROR)
		CASTIGO DE SALDO PARA CIERRE DE PRODUCTO - Instrucción Banco
		ROBO O HURTO AL INTERIOR DE OFICINAS O SUCURSALES (CLIENTE Y NO CLIENTE)
		DEVOLUCIÓN DE CARGO POR CIERRE DE NEGOCIO NO CONCRETADO
DAÑOS EN ACTIVOS FÍSICOS	DESASTRES NATURALES Y OTROS EVENTOS	PERDIDAS POR DESASTRES NATURALES O ACCIDENTES
		PERDIDAS POR ACCIONES ORIGEN EXTERNO (TERRORISMO, VANDALISMO, INTENTO DE ROBO)
		INDEMNIZACIÓN POR DAÑOS PERSONALES
		DAÑOS EN INSTALACIONES, EQUIPAMIENTO, CAJEROS AUTOMÁTICOS DISTINTOS A TERRORISMO, VANDALISMO O INTENTO DE ROBO
		OTROS (DESASTRES NATURALES Y OTROS EVENTOS)
INTERRUPCIÓN DEL NEGOCIO Y FALLOS EN SISTEMAS	SISTEMAS	CARGO ASOCIADO A DETENCIÓN DEL SISTEMA POR FALLAS DE HARDWARE
		CARGOS / COBROS INCORRECTOS A PRODUCTOS VIGENTES POR DEFICIENCIA DE SISTEMAS
		CARGOS A PRODUCTOS CERRADOS
		DATOS EN SISTEMAS NO ESTÁN UNIFICADOS
		CARGO ASOCIADO A DETENCIÓN DEL SISTEMA POR FALLAS DE SOFTWARE
		ERROR EN ENVIO / CARGA / MIGRACION DE INFORMACIÓN ENTRE SISTEMAS
		CARGO ASOCIADO A DETENCIÓN DEL SISTEMA POR FALLA EN LA IMPLEMENTACIÓN
		CARGO ASOCIADO A DETENCIÓN DEL SISTEMA POR ERRORES EN TELECOMUNICACIONES Y/O REDES

Basilea Nivel 1	Basilea Nivel 2	Categoría Interna Nivel 3
		CARGO ASOCIADO A DETENCIÓN DEL SIST POR HERRAMIENTAS EXT CON VERS ANTICUADAS O INCONSISTENTES
		CARGO ASOCIADO A DETENCIÓN DEL SISTEMA POR ARQUITECTURA INADECUADA
		ERROR EN INGRESO, REGISTRO O EMISIÓN DE ONP, PROTESTO O CTA CERRADA.
		DESCUADRATURA CTA CONTROL SIN UBICAR
EJECUCION, ENTREGA Y GESTION DE PROCESOS	CAPTURA DE TRANSACCIONES, EJECUCIÓN Y MANTENIMIENTO	CARGOS A PRODUCTOS DEL CLIENTE EN PROCESO DE CIERRE (NO CONSIDERADOS)
		CONVENIO DE PRODUCTO INGRESADO ERRÓNEAMENTE
		DIFERENCIAS O DESCUADRATURAS EN CAJA
		ERROR EN PROCESO DE APERTURA DE PRODUCTO
		ERROR EN INGRESO DE OPERACIÓN O INSTRUCCIÓN DE CLIENTE
		GESTIÓN NO REALIZADA, POR INCUMPLIMIENTO DE PLAZOS O PROCEDIMIENTOS
		CIERRE DE PRODUCTO INSTRUIDO Y NO REALIZADO
		CONVENIO DE PRODUCTO NO EFECTUADO
		DEMORA O ERROR EN ALZAMIENTOS DE PRENDAS O GARANTÍAS
		DEMORA EN ENTREGA DE DOCUMENTOS
		PAGO INSTRUIDO Y NO EFECTUADO
		TRASPASO DE FONDOS SOLICITADO Y NO EFECTUADO
		CARGO ERRÓNEO POR OPERACIONES DEFICIENTES DEL MODELO
	CAPTURA DE TRANSACCIONES, EJECUCIÓN Y MANTENIMIENTO	ERRORES OPERACIONALES EN PROCESO DE CONTABILIZACION
		PRODUCTOS ACTIVOS NO ENTREGADOS A CLIENTE
		DEMORA EN ACTIVACIÓN O ENTREGA DE PRODUCTO
		ERROR EN INGRESO DE OPERACIÓN EN CAJA
		FALTA INFO, INFO ERRÓNEA O ENGAÑOSA ENTREGADA POR ÁREA COMERCIAL A CLIENTE
		FALTA INFO, INFO ERRÓNEA O ENGAÑOSA ENTREGADA POR FONOBANK
		FALTA INFO, INFO ERRÓNEA O ENGAÑOSA EN INTERNET
		OP CURSADA SIN CONFIRMACION EXPRESA DEL CLIENTE

Basilea Nivel 1	Basilea Nivel 2	Categoría Interna Nivel 3
EJECUCION, ENTREGA Y GESTION DE PROCESOS	CONTROL Y REPORTES	INEXISTENCIA DE MECANISMO DE CONTROL
		DISEÑO INADECUADO DE MECANISMO DE CONTROL
		UTILIZACIÓN DEFICIENTE DE MECANISMO DE CONTROL
		ACLARACIÓN BANCARIA POR ERROR EN CHEQUE O LETRA MAL PROTESTADO
		DEVOLUCIÓN DE INTERESES, POR ERROR EN CHEQUE MAL PROTESTADO
		PAGO DE CHEQUE CADUCADO O CON ONP - ERROR EN CAJA O CANJE
		INCUMPLIMIENTO DE REPORTES OBLIGATORIOS
		REPORTES ERRÓNEOS O INEXACTOS
		ERROR EN INGRESO O REGISTRO DE ONP, PROTESTO, CTA CERRADA
		DIFERENCIA EN REMESA ENVIADA / RECIBIDA, A TRAVÉS DE ETV (BILLETE FALSO)
	ADMISION DE CLIENTES Y DOCUMENTACION	CONTRATO O DOCUMENTO LEGAL INEXISTENTE
		CONTRATO O DOCUMENTO LEGAL INCOMPLETO, DEFECTUOSO O ERRÓNEO
		PERDIDA DE CONTRATO O DOCUMENTO LEGAL EN APERTURA DE PRODUCTO
	GESTION DE CUENTAS DE CLIENTES	CARGO DEBIDO A REGISTROS DE CLIENTES INCORRECTOS, INCOMPLETOS O DESACTUALIZADOS
		CASTIGO POR CONTINGENCIA, OP SUPERA PERMANENCIA (90 DÍAS)
		RIESGO ACEPTADO POR GESTION DE CUENTAS
		CASTIGO DIRECTO POR CIERRE DE CTA CTE
		CARGO/COBRO ASOCIADO A AUMENTO DE CUPO DE PRODUCTO SIN INFORMAR A CLIENTE
		INCUMPLIMIENTO DE CONTRATOS
	FALLOS CON CONTRAPARTES DEL CLIENTE (NO CLIENTE)	PERDIDAS POR JUICIOS. INCUMPLIMIENTO DE LA NORMATIVA FISCAL
		INTERPRETACIÓN ERRÓNEA DE NORMA O LEYES
		PERDIDAS POR JUICIOS. INCUMPLIMIENTO DE LA NORMATIVA BANCARIA
		PERDIDAS POR JUICIOS. INCUMPLIMIENTO DE OTRAS NORMATIVAS
		PERDIDAS POR JUICIOS. INCUMPLIMIENTO DE CONTRATOS

Basilea Nivel 1	Basilea Nivel 2	Categoría Interna Nivel 3
		COMERCIALES
		PERDIDAS POR JUICIOS. INADECUADO USO DE DERECHOS DE PROPIEDAD INTELECTUAL
		PERDIDAS POR JUICIOS. OTROS CONFLICTOS, ADVENIMIENTO, INDEMNIZACION
		PERDIDAS POR RESOLUCIÓN DEFENSORÍA DEL CLIENTE / SBIF
	VENDEDORES Y PROVEEDORES	DEFICIENCIA EN EL SERVICIO DE PROVEEDORES
		DEVOLUCIÓN A CLIENTE POR ERROR DE DISPENSACIÓN DE ATM, OTRO Y MISMO BANCO
		DISPENSACIÓN DE BILLETES FALSOS EN ATM, OTRO Y MISMO BANCO
		CARGOS ERRÓNEOS POR DEFICIENCIA EN EL SERVICIO DE PROVEEDORES
		CONTROLES DEFICIENTES EN SERVICIO DE PROVEEDORES
		INCUMPLIMIENTO DE CONTRATOS DE PROVEEDORES
		CORTE DE SUMINISTROS DE PROVEEDORES
		CONFLICTOS CON VENDEDORES
CASTIGOS OTROS BASILEA II	OTROS CASTIGOS BASILEA II	CASTIGOS SIN CLASIFICAR POR ANTECEDENTES INSUFICIENTES
		CASTIGO SIN CLASIFICAR POR FALTA DE ANTECEDENTES
		CASTIGOS SIN CLASIFICAR POR MIGRACION

Fuente: Elaboración Propia (2012) identificación de Nivel 3 Interna.

Anexo N°2: Consideraciones en ASA para los préstamos de las líneas de negocio tradicional

Línea de Negocio Tradicional	Tipo de Préstamos Incluidos en ASA	Definición
Banca Minorista	Minoristas	Exposiciones a particulares (incluyendo líneas de sobregiro y de tarjetas de crédito), préstamos hipotecarios sobre residencias, entre otros.
	Micro/Pequeñas/Medianas empresas tratadas como minoristas	Todos los préstamos crediticios a micro/pequeñas/medianas empresas, según los criterios de exposición máxima individual que cada supervisor instruya para catalogarlas dentro de minoristas.
	Derechos de cobro adquiridos a minoristas	Financiación bancaria sobre valores adeudados a los clientes minoristas del banco por parte de terceros, por los bienes o servicios que les proporcionen.
Banca Comercial	Empresas	Préstamos a una empresa o sociedad.
	Soberanos	Préstamos a soberanos, bancos centrales, algunas organizaciones públicas y bancos de desarrollo.
	Bancos	Préstamos a otros bancos, financieras o sociedades de valores reguladas.
	Financiación	Préstamos para financiación de proyectos,

Línea de Negocio Tradicional	Tipo de Préstamos Incluidos en ASA	Definición
	especializada	bienes, materias primas, propiedades inmobiliarias generadores de renta/comerciales.
	Pequeñas y medianas empresas tratadas como empresas	Todos los préstamos crediticios a pequeñas y medianas empresas, según los criterios de exposición mínima individual que cada supervisor instruya para catalogarlas dentro de aquella categoría.
	Derechos de cobro adquiridos a empresas	Financiación bancaria sobre valores adeudados a empresas clientes del banco por parte de terceros, por los bienes o servicios que les proporcionan.
	Valor contable de títulos de la cartera de inversión	Valor de adquisición de los títulos mantenidos en la cartera de inversión (por lo tanto, con fin de mantenerlos hasta el vencimiento).

Fuente: Sbif