Qualitative techniques for managing operational risk

Delfiner, Miguel and Pailhé, Cristina
Central Bank of Argentina

05. January 2009

Técnicas cualitativas para la gestión del riesgo operacional

Miguel Delfiner y Cristina Pailhé[1]

Octubre 2008

Resumen

Un elemento fundamental para la identificación y evaluación de los riesgos operacionales (RO) es el uso de técnicas cualitativas. El uso de estas técnicas es importante ya que para la evaluación del RO, las decisiones de la entidad financiera afectan el perfil de riesgos de diversas maneras, ninguna de las cuales puede ser capturada única y directamente a través de un modelo de medición cuantitativo estático. El perfil de RO derivado exclusivamente de datos de pérdidas históricas podría verse modificado por las acciones correctivas implementadas por la entidad financiera con posterioridad a la ocurrencia de los eventos reflejados en esos datos. En este trabajo se presentan algunas de las herramientas más difundidas en la gestión del RO, entre ellas la auto-evaluación del RO, los indicadores de riesgo clave (KRIs), los procesos de asignación del riesgo, las tarjetas de puntaje (*scorecards*), y el análisis de escenarios. Estas técnicas son aún relativamente nuevas y las modalidades que finalmente adoptan en la práctica dependen en gran medida de las características de cada entidad. Dada esta falta de homogeneidad en la aplicación de las técnicas, este trabajo abunda en ejemplos que ilustran la aplicación y utilidad de esas herramientas.

Palabras clave: Riesgo operacional, auto-evaluación del riesgo, mapeo de riesgos, indicadores de riesgo, tarjetas de puntaje, análisis de escenarios.

[1] Miguel Delfiner (mdelfiner@bcra.gov.ar) es Analista Principal y Cristina Pailhé (cpailhe@bcra.gov.ar) es Gerente de Investigación y Planificación Normativa, Subgerencia General de Normas, BCRA. Las opiniones vertidas en este trabajo corresponden a los autores y no representan una posición oficial del Banco Central de la República Argentina. Se agradece especialmente a José Rutman por el apoyo brindado para la realización de este trabajo, y a Ana Mangialavori por sus comentarios. Los errores remanentes son exclusiva responsabilidad de los autores.

Indice

Acrónimos utilizados

Basilea II: “Nuevo Marco de Capitales” del Comité de Basilea
BCBS: Basel Committee on Banking Supervision.
BCRA: Banco Central de la República Argentina.
BEICF: Business Environment & Internal Control Factors
KCI: Key Control Indicator.
KPI: Key Performance Indicator.
KRI: Key Risk Indicator
KRIeX: Key Risk Indicator Exchange project.
LDA: Loss Distribution Approach.
ORX: Operational Risk exchange.
RDCA: Risk Driver and Control Approach.
RMG: Risk Management Group.
RO: Riesgo Operacional.
RCSA: Risk and control self assessments
RRHH: Recursos Humanos.
SBA: Scenario Based Approach.
TI: Tecnología Informática.

1. Introducción

En este trabajo se presentan algunas de las técnicas para la gestión del RO más difundidas, como la auto-evaluación del RO, los indicadores de riesgo (KRIs), los procesos de asignación del riesgo, las tarjetas de puntaje (scorecards), y el análisis de escenarios. Estas técnicas son aún relativamente nuevas y su aplicación depende en gran medida de las características de cada entidad. Sin embargo resultan un complemento fundamental a la creación de una base de datos interna y al uso de esos datos, como así también de aquellos provenientes de fuentes externas.

Por las características de estas técnicas, no existe una única metodología de aplicación generalizada, ni tampoco consensos definitivos respecto a la mejor forma de aplicarlas. Debido a ello, el objetivo de este documento es realizar una recopilación, para cada una de las metodologías presentadas, de diversos ejemplos de aplicación.

Las técnicas cualitativas de gestión del RO contribuyen entre otras cosas, a:

- Tener una visión *"forward looking":* las decisiones empresariales pueden afectar el perfil de RO de la entidad de diversas maneras (por ejemplo a través de cambios en los procedimientos de control, sistemas, RRHH, para mencionar algunas), ninguna de las cuales puede ser capturada total y directamente a través de un modelo de medición. Las metodologías que se basan en fundamentos estadísticos contendrían un sesgo, dado que la información histórica reflejará un riesgo y un ambiente de control que no necesariamente existe en el presente. Es por ello que el uso de algunas de las técnicas cualitativas (s*elf-assesment,* KRIs, etc.) brinda la posibilidad de anticiparse a eventos aún en el caso que no hayan sido observados en el pasado.
- Mitigar el RO: a través de la implementación de sistemas de control y seguimiento de procesos y productos.
- Incrementar la transparencia: ayuda a poner en evidencia los riesgos existentes.
- Asignar la responsabilidad de los riesgos identificados a determinadas personas o sectores.

Desde el ámbito regulatorio el uso de estas técnicas comenzó siendo impulsado por el BCBS en sus estándares de sanas prácticas de gestión del RO[2]. Publicados en el año 2003, esos *principios* de buenas prácticas para la administración del RO, establecen que la *identificación* del RO es fundamental para el posterior desarrollo de un sistema viable de control y seguimiento del mismo. Señala que además de la recolección de datos históricos de pérdidas operativas, internos de las entidades, estas también deben identificar y evaluar sus RO a través del uso de herramientas tales como:

- Indicadores de riesgo (o KRIs)
- Auto-evaluación o evaluación del RO, incluyendo el uso de "*scorecards*" que proveen un medio para trasladar las evaluaciones cualitativas obtenidas de las unidades de negocio, a una métrica cuantitativa.
- Asignación o "mapeo" de riesgos (*risk mapping*).

[2] BCBS (2003).

Por otro lado, en el "Nuevo Marco de Capitales" del Comité de Basilea (o Basilea II)[3] se destaca que las técnicas cualitativas para la gestión del RO permiten identificar los factores básicos del entorno de negocio y del control interno que pueden modificar el perfil de RO de las entidades financieras. El uso de estos factores hace que las evaluaciones del riesgo que realice la entidad estén más orientadas hacia el futuro; reflejen de forma más directa la calidad de los entornos operativos y de control de la institución; contribuyan a alinear las evaluaciones de capital con los objetivos de la gestión de riesgos y reconozcan de una manera más inmediata tanto la mejora como el deterioro de los perfiles de RO.

Estos factores también se conocen en la industria financiera como *"Business Environment & Internal Control Factors"* (o BEICFs), definidos como los indicadores del perfil de RO de una entidad financiera que reflejan una evaluación presente y "forward-looking" de los factores de riesgo de negocios subyacentes y del ambiente de controles internos[4]. Las herramientas usadas para este análisis incluyen las auto-evaluaciones de riesgo y control *("Requirement Risk and control self assessments"* o RCSA[5]), el uso de *Scorecards*, KRIs, KPIs, y asignación o mapeo de procesos.

En lo que sigue se describirán las técnicas cualitativas más difundidas para la gestión del RO. Debe tenerse en cuenta que a pesar de que las técnicas son presentadas en diferentes secciones, muchas veces se hallan interrelacionadas, puesto que pueden emplearse en conjunto, o debido a que una de ellas incluye el uso de otra.

En la sección 2 se presentan los procesos de auto-evaluación del RO que generalmente incluyen varias etapas. Entre ellas se pueden mencionar la identificación y evaluación del RO, que suelen incluir el procedimiento de asignación de riesgos (en inglés *risk-mapping*), y la evaluación de los controles del RO. La auto-evaluación es un procedimiento muy abarcativo y suele incluir alguna de las técnicas que se presentan en las otras secciones.

En la sección 3 se describe el proceso de asignación de riesgos *("risk-mapping")*, el que permite agrupar por tipo de riesgo a las distintas unidades de negocio, funciones organizativas o procesos. Se describen ejemplos de asignación de los riesgos a áreas de riesgos; a procesos y una asignación simultánea a ambos en conjunto con los productos de la entidad. La sección 4 se refiere al uso de indicadores de riesgo (KRIs), una de las metodologías mejor documentadas. Se trata de estadísticos o parámetros, a menudo de carácter financiero, que actúan como indicadores predictivos de cambios en el perfil de riesgo de un negocio. Se describe su utilidad, atributos y aplicaciones. Al final de dicha sección se ilustra la iniciativa de la *"KRI Library and Services"*[6] orientada a las compañías de servicios financieros interesadas en mejorar su administración del RO. Este proyecto se inició a través de un estudio de dos años de los KRI en la industria bancaria, y es liderado por un grupo conformado por representantes de bancos internacionales.

[3] BCBS (2004) párrafo 676.
[4] Seivold (2008).
[5] Se define al RCSA como un proceso a través del cual las diversas áreas de negocio identifican y evalúan los riesgos incurridos, el nivel de control que tienen sobre ellos, y las acciones de mejoras emprendidas. El punto inicial consiste en establecer un conjunto completo de definiciones de riesgo, seguido de una identificación de los mismos, lo que típicamente toma la forma de un mapa de riesgos en donde se exhiben los riesgos por área y su relativa frecuencia y severidad.
[6] KRIeX .

La sección 5 describe la técnica de tarjetas de puntaje (o *scorecards*) aplicada al RO, también conocida como *"Risk Drivers and Control Approach"* (RDCA). La técnica se refiere a un conjunto de sistemas expertos que tienen en común la evaluación de los generadores de riesgo, como así también, la evaluación de la amplitud y calidad del ambiente interno de controles de riesgos, todo ello a través del uso de cuestionarios.

Luego en la sección 6 se analiza el uso del *análisis de escenarios* para la gestión del RO. Los escenarios constituyen eventos hipotéticos que podrían ocurrir y deben ser representativos para cada entidad, teniendo en cuenta los factores de riesgo relevantes. Cada área organizacional puede evaluar el impacto de los escenarios y estimar las pérdidas resultantes. Por último, la sección 7 presenta las conclusiones.

2. Auto-evaluación del riesgo operacional

La *auto-evaluación de riesgos* puede describirse como un proceso de identificación y evaluación de los riesgos existentes en la entidad, sumado a una evaluación de los controles establecidos para su administración y mitigación[7]. Este proceso puede aplicarse a todos los riesgos (mercado, crédito, liquidez, etc.) aunque en el presente trabajo nos circunscribiremos al RO. La auto-evaluación es un componente crítico del marco de gestión del RO, pues en base a este proceso la entidad financiera puede comprobar la vulnerabilidad de sus operaciones y actividades ante el RO. Este proceso en general debe adecuarse al tamaño e importancia del riesgo para la entidad, ya que, por ejemplo, un riesgo específico puede ser crítico para una organización pequeña, pero de muy bajo impacto para una entidad más grande o de complejidad diferente.

El proceso de auto-evaluación es interno e incorpora información provista por la alta gerencia como así también por el personal de línea de la entidad financiera. Esta información está referida a procesos, actividades, funciones y proyectos, tanto a nivel de unidades de negocio como de toda la organización. La información se puede mantener actualizada a través "*workshops*"[8], reuniones y / o cuestionarios realizados con determinada frecuencia. Para que sean efectivos, es importante establecer un lenguaje común y una categorización del riesgo que permita analizar y consolidar los resultados de la auto-evaluación.

La implementación de esta técnica se facilita a través de la existencia de una función específica encargada de coordinar el proceso de autoevaluación y de proveer de entrenamiento apropiado para la identificación de los riesgos y los controles correspondientes.

La auto-evaluación del RO usualmente se compone de distintas etapas (identificación, evaluación, control y seguimiento) que se describirán en detalle en las siguientes secciones.

Entre los principales beneficios de la auto-evaluación de riesgos se pueden citar:

- Permite entender los riesgos inherentes en los procesos de negocio.
- Evalúa la efectividad de los controles internos.
- Revela áreas prioritarias de trabajo.

[7] Lloyds (2007)
[8] Ver Anexo II.

- Acuerda planes de acción para tratar riesgos que excedan el *nivel de riesgo tolerable* (p.ej. a través del tratamiento de debilidades identificadas en los controles internos).
- Permite adjudicar la propiedad de los riesgos y controles al personal mejor preparado para administrarlos.

2.1. Etapa 1: Identificación de los RO

El punto de inicio para la administración del RO en una entidad es la identificación de los riesgos clave y su vinculación con los objetivos del negocio y los controles establecidos para mitigarlos. Los resultados de este ejercicio se vuelcan típicamente a un registro de riesgos, que actúa como un repositorio central de la naturaleza y estado de cada uno de los riesgos clave y sus controles en todo momento. Un registro bien diseñado y que se mantiene actualizado puede ayudar a la entidad, ya que:

- Permite a la alta gerencia recibir información periódica de los principales riesgos y de cómo se están reportando.
- Contribuye con la auditoría interna y el área de *compliance* pues el registro provee un resumen de las actividades de control que pueden estar sujetas a revisión por parte de estas áreas.
- Permite mejorar la asignación del capital económico, pues este debe estar alineado con los riesgos asumidos por la entidad.
- Contribuye al cumplimiento de requisitos regulatorios.

En el Cuadro 1 a continuación se exhibe un resumen de un registro de riesgos y en el Anexo I se muestra en mayor detalle el tratamiento brindado a los dos primeros riesgos operacionales citados en el cuadro. En dicho cuadro también figura la evaluación que hace la entidad de cada uno de estos riesgos en función de la probabilidad de ocurrencia e impacto (ver sección 2.2.).

Cuadro 1: Resumen de un registro de riesgos operacionales*

	Riesgos operacionales	Propietario del riesgo	Impacto / Probabilidad			Gap =
			Inherente	Residual	Objetivo	Objet. - Inher.
1.1	Gestión ineficiente de la información / IT	xx	B1	A1	A1	Ninguno
1.2	Fallas ó pérdida de una infraestructura clave	xx	B1	A1	A1	Ninguno
1.3	Estructura de gobernancia no efectiva	xx	D2	B1	D1	↑ impacto
1.4	Cultura inapropiada y problemas con RRHH	xx	C2	B1	B1	Ninguno
1.5	Fallas en la definición y mantenimiento de estrategias	xx	D2	C1	C1	Ninguno
1.6	Fallas para ejecutar la actual estrategia	xx	D2	C1	C1	Ninguno
1.7	Pérdida de ventajas competitivas (p.ej. caída de ratings)	xx	D1	D1	D1	Ninguno
1.8	Pérdidas surgidas de la estructura de capital	xx	D2	C1	B1	↓ impacto
1.9	Capital inapropiado	xx	D2	C1	C1	Ninguno
1.10	Fraude financiero externo	xx	C2	B1	B1	Ninguno
1.11	Cambios de los requisitos regulatorios	xx	D2	C1	C1	Ninguno
1.12	Acción de los reguladores	xx	D1	C1	C1	Ninguno
1.13	Fraude financiero interno	xx	D2	C3	C1	↓ probabilidad
1.14	Tratamiento inadecuado de los reclamos	xx	C3	A1	A1	Ninguno

* Tomado de Lloyds (2007): Self-assesment tool 6.10.El impacto se mide en una escala A,B,C y D y la probabilidad de con una escala que va de 1 a 4. A modo de ejemplo el riesgo 1.6 mide C1, ó sea que a nivel residual tiene una baja probabilidad de ocurrencia pero alto impacto. El riesgo residual es el que subsiste luego de aplicar los controles que realiza la entidad financiera para su mitigación.

En el Anexo I también se exhiben otros ejemplos de registros de riesgos.

Algunas de las técnicas más utilizadas para identificar los riesgos son la elaboración de cuestionarios de auto-evaluación y la realización de reuniones grupales guiadas (o "*workshops*"). Estos métodos no son mutuamente exclusivos y generalmente se usan en conjunto.

Los cuestionarios de auto-evaluación en general consisten en un proceso *"bottom-up"*, a través del cual los gerentes de línea identifican y evalúan las áreas que presentan los mayores riesgos. Se provee a los gerentes y al personal más idóneo para identificar los riesgos, de un cuestionario estándar con instrucciones precisas, que una vez completado son compilados por el área encargada de la administración del RO. Se debe prestar especial atención a la consistencia entre las respuestas provistas, para lo cual es conveniente una fluida relación entre el área centralizada de administración del RO y las diversas líneas de negocio.

Otra herramienta muy difundida para la identificación del RO, es la realización de una serie de *"workshops"* para considerar cada categoría de riesgo, involucrando al personal más capacitado para su tratamiento. Se distribuye con anticipación el material relevante para ser revisado (objetivos del negocio, reportes regulatorios y de auditoría, evolución de los KRI's, evaluaciones de riesgo anteriores, mapas de riesgos y procesos, datos históricos de pérdida por RO, planes de administración del RO previos, etc.) y con posterioridad se establece una discusión estructurada en donde se trata de llegar a un consenso sobre los riesgos enfrentados por la entidad. En muchos casos participa un facilitador en las discusiones. En el Anexo II se ejemplifica a través de un diagrama, la organización de uno de estos *"workshops"*.

2.2. Etapa 2: Evaluación de los RO

Una vez identificados los tipos de RO relevantes, en general se establecen prioridades para enfrentarlos en función del ambiente de control existente en la entidad. Para ello se suelen utilizar plantillas estándar de evaluación del riesgo, que facilitan que el personal involucrado realice una descripción de los riesgos, identifique causas y disparadores del RO así como también analizar sus efectos (ver Anexo III).

Los riesgos pueden ser evaluados sobre una *base inherente* (antes de aplicar los controles) o sobre una *base residual*, esto es después de aplicar los controles existentes. Aspectos tales como el tipo de RO que se trate y los controles que tenga la entidad, pueden hacer que una u otra opción sea de mayor dificultad de ejecución.

Se suelen establecer ciertos estándares mínimos para permitir la agregación de los resultados en distintas clases de riesgos y líneas de negocios, aunque es necesario permitir cierto grado de discrecionalidad a ser aplicado por las diversas áreas. Por ejemplo se podrían evaluar los riesgos en función de su probabilidad e impacto; sin embargo esta tarea se podría ver dificultada por la naturaleza no-financiera de algunas variables, debido a lo cual, la evaluación casi siempre dependerá en parte de una opinión experta. El Cuadro 2 muestra un posible criterio para evaluar un riesgo en función de estas variables.

Cuadro 2: Criterios de evaluación del riesgo en función de su impacto y probabilidad*

Probabilidad – probabilidad que el riesgo ocurra dentro de los próximos12 meses basado en un puntaje de **1** a **4** en base a la experiencia de gestión del riesgo y la intuición del área encargada de la evaluación.	**1** probabilidad < 5% **2** probabilidad entre 5% y 25% **3** probabilidad entre 25% y 50% **4** probabilidad > 50%
Impacto – nivel a partir del cual el riesgo afecta la capacidad de la entidad para desarrollar su estrategia y objetivos basado en una calificación de **A** a **D**	**A** Sin impacto material. **B** Impacto material, sin generar riesgos significativos y duraderos a la entidad. **C** Riesgo significativo para la entidad. **D** Posible daño organizacional.

*Lloyds (2007): Self-assesment tool 6.4**.**

A pesar de que los criterios exhibidos en los cuadros 1 y 2 permitan establecer un nivel de riesgos para los RO considerados, la decisión final respecto a dicho nivel suele quedar a cargo de los profesionales de la gestión del RO basándose para ello en un análisis que incluye información adicional, tal como:

- Factores de riesgo inherente (p.ej. la naturaleza del negocio, nivel de complejidad, etc.).
- Exposición actual al riesgo (p.ej. auto-evaluaciones anteriores, reportes de auditoría, indicadores de riesgo, etc.).
- Resultados de auditoría (en base a *ratings* o el número de grandes riesgos identificados).
- Materialidad (en base a ingresos brutos, activos ponderados por riesgo, etc.).
- Estabilidad (p.ej. en función a los planes de negocios).

Más allá de la metodología por la cual se opte, en general se crean ordenamientos de los riesgos, lo que ayuda a identificar además las líneas de negocio cuyos riesgos dependen fuertemente de la efectividad de los controles establecidos. A su vez, es importante asignar los riesgos a personas que asuman responsabilidad por los mismos y que tengan la autoridad y cuenten con los recursos necesarios para administrarlos efectivamente. Sus roles pueden incluir:

- Identificar, mantener y comunicar información actualizada referida a los riesgos asignados.
- Monitorear los riesgos frente a posibles cambios en su probabilidad de ocurrencia o impacto, para lo que es importante:
    - mantener un vínculo permanente con el responsable de controlar esos riesgos, para establecer los controles y sistemas adecuados para administrar el riesgo,
    - recolectar y analizar datos relevantes que puedan indicar cambios en el perfil del riesgo, en cuyo caso corresponderá implementar las acciones apropiadas,
    - asegurar la efectiva implementación de los planes de acción para administrar el riesgo,
    - reportar la información regularmente al resto de la organización.
- Asumir la responsabilidad por la gestión efectiva de los riesgos asignados.

La información recolectada durante esta etapa se puede usar para agrupar las diferentes unidades de negocio, funciones organizativas o procesos, por tipo de riesgo a través de un procedimiento conocido como asignación de riesgos (ver Sección 3).

2.3. Etapa 3: Evaluación de los controles

Una vez identificados y evaluados, los riesgos deberían contrastarse con el actual ambiente de control a efectos de entender el perfil de riesgo residual de la entidad. Para esta tarea son útiles plantillas especialmente diseñadas para la evaluación de los controles.

Los controles podrán ser de carácter preventivo o de detección. Los controles preventivos (o "*front-line*") son controles de alto nivel orientados a prevenir las causas del riesgo en una etapa muy temprana. Algunos ejemplos incluyen el proceso de planeamiento del negocio, la existencia de una política prudencial para la captación de nuevos empleados, o guías provistas por la casa matriz de una entidad. En cambio los controles de detección (o "*back-stop*") suelen ser menos frecuentes y llevarse a cabo con una periodicidad mensual o trimestral. Se debe hacer un balance entre ambos tipos de controles en función de los riesgos existentes, siempre teniendo en cuenta que es preferible prevenir pérdidas a detectarlas.

Como en el caso de los riesgos, es vital asignar los controles a personas responsables de los mismos, quienes se ocupan de:

- ✓ Generar un ambiente de control eficiente para gestionar la frecuencia e impacto del riesgo (en conjunto con el responsable del riesgo).
- ✓ Proveer y transmitir información relativa a la efectividad de los controles al responsable del riesgo y a otros interesados.
- ✓ Recolectar y analizar información vinculada a la efectividad de los controles, y su conversión en información indicativa.
- ✓ Generar e implementar las acciones correctivas necesarias en virtud de la información recolectada.
- ✓ Reportar a las instancias establecidas las debilidades o interrupciones de los controles.

Se debe tener presente que un control puede no estar diseñado para eliminar totalmente el riesgo. Ello puede deberse a que existen otros controles que ya consideran el riesgo, que la entidad este dispuesta a asumir ese riesgo, o que directamente sea antieconómico eliminarlo.

A continuación se presenta un ejemplo de evaluación del diseño y el desempeño de un control para un riesgo en particular (ver cuadro 3).

Cuadro 3: Parámetros de evaluación del diseño y el desempeño de un control*

Diseño	**Verde**	diseñado para eliminar el riesgo.
	Amarillo	diseñado para reducir los principales efectos del riesgo.
	Ámbar	diseñado para reducir algún aspecto del riesgo.
	Rojo	mal diseñado, provee poca protección aún cuando este bien implementado.
Desempeño	**Verde**	el control es aplicado en forma correcta de acuerdo a como fuera diseñado.
	Amarillo	el control esta operativo pero a veces no es aplicado de la forma correcta.
	Ámbar	el control a veces se aplica.
	Rojo	el control no se aplica, o se aplica en forma incorrecta.

*Lloyds (2007): Self-assesment tool 6.5.

En el Anexo III se exhibe un ejemplo de una plantilla diseñada para que el propietario del riesgo pueda evaluar un riesgo y sus controles en base a los criterios exhibidos hasta ahora. Luego de completar una evaluación inicial o inherente, la plantilla permite incluir una detallada evaluación de los controles que pudieran reducir el riesgo e informar sobre la existencia de pólizas de seguro que cubran parcial o totalmente el riesgo. Acto seguido se evalúa el riesgo residual teniendo en cuenta los controles existentes, tras lo cual se analiza la efectividad de los mismos. Finalmente, se determinan los objetivos en referencia al riesgo en cuestión, y las acciones para lograrlos.

3. Asignación de riesgos (o *risk-mapping*)

La asignación o mapeo de riesgos ("*risk mapping*") es el proceso a través del cual se agrupan por tipo de riesgo las diferentes unidades de negocio, funciones organizativas o procesos. Ello puede dejar al descubierto ámbitos que presenten deficiencias así como ayudar a determinar las prioridades para su gestión[9]. Puede ser ejecutado en forma indistinta a un nivel alto o bajo con el objetivo de identificar "qué puede fallar" en un proceso determinado y sus resultados pueden ser representados visualmente a través de un diagrama de flujo de proceso, o de un mapa de riesgos o "*heat map*".

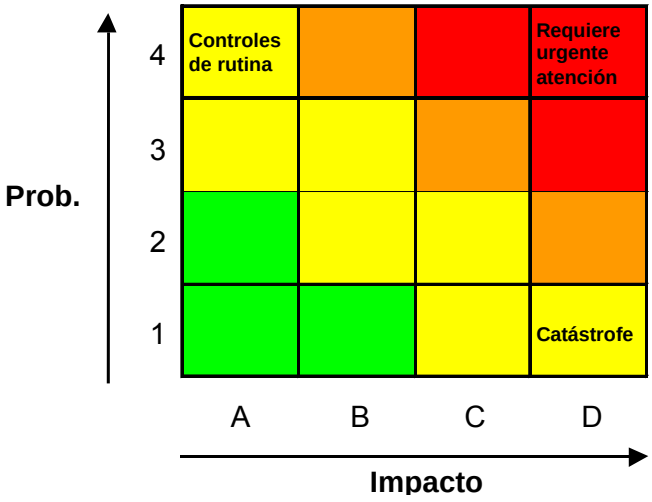
Según Scandizzo[10], al concepto de asignación de riesgos tradicionalmente se lo suele vincular, por una parte, con diversas maneras de administrar el RO y, por la otra, con la formulación de los pasos necesarios para auditar la auto-evaluación de riesgos. Sin embargo la literatura no ofrece muchos indicios de cómo llevar a cabo este proceso. A diferencia de los riesgos de crédito y de mercado, los RO no pueden no ser producto – específicos y no estar circunscriptos a una única unidad de negocios. Por lo tanto no es suficiente con analizar el RO a un nivel de unidad de negocio, puesto que los errores en cierta parte de un proceso pueden materializarse como pérdidas en unidades de negocio distintas a la responsable del error.

Hay varias maneras de realizar una asignación de riesgos, siendo una técnica habitual su representación a través de una figura bidimensional cuyas dimensiones son la probabilidad y el impacto. Este mapa permite desagregar los riesgos de acuerdo a estas dos dimensiones, pero no da indicaciones sobre las medidas a tomar para modificar el perfil existente de

[9] BCBS (2003).
[10] Scandizzo (2003).

riesgos. A modo de ejemplo consideremos el cuadro 3 de la sección 2.3. En base a este cuadro se puede construir un gráfico conocido como "*heat map*". Los colores se representan en función de la tolerancia al riesgo de la entidad y el resultado es una herramienta gráfica muy simple que permite resaltar aquellos riesgos que requerirían ser rápidamente mitigados (ver Figura 1).

Figura 1: mapa de riesgos ó "Heat map"

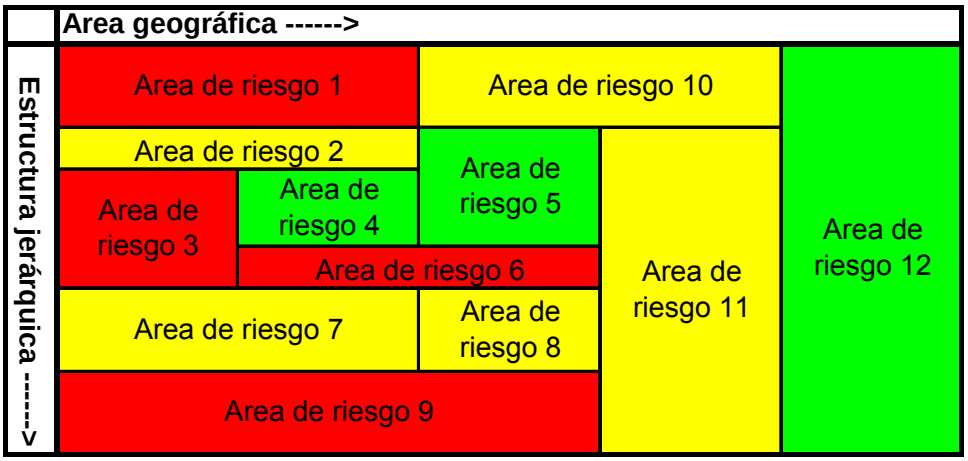


3.1. Asignación de riesgos a áreas de riesgo

Una metodología alternativa consiste en asociar los riesgos identificados y evaluados en función de su probabilidad de ocurrencia e impacto a ciertas áreas de riesgo, las que pueden comprender una o varias unidades de negocio, de manera tal que el resultado puede brindar una imagen del perfil de riesgos de la entidad. Por definición la suma de todas las áreas de riesgo debería englobar todos los procesos y funciones de negocio de la entidad. El principal objetivo de esta desagregación es reflejar claramente la estructura de la entidad e identificar áreas de RO que necesiten ser gestionadas en forma conjunta.

Como primer paso, se requiere definir lo que se entiende por *área de riesgo*. Un punto de partida podría ser el sector del banco sobre el cual pueda establecerse una responsabilidad jerárquica; desde ese punto de vista se podrían considerar las áreas que se puedan asociar a un gerente de línea. Pero también pueden agregarse otras dimensiones, como la jerarquía organizacional y la dispersión geográfica. De esta manera se podría obtener un mapa como el exhibido a continuación

Figura 2: ejemplo de un mapa de riesgos



3.2. Asignación de riesgos a procesos

Scandizzo[11] propone en cambio asignar los riesgos a los procesos de negocio, para lo cual debe definirse claramente el concepto de *proceso de negocio* (por ejemplo como el conjunto de actividades destinadas a crear un producto a partir de ciertos insumos[12]). Como primer paso, requiere identificar los procesos claves de la organización para luego, identificar los generadores de riesgo (o *"risk drivers"*), tales como las personas, los sistemas y la infraestructura. Dependiendo del área analizada y de la naturaleza de las tareas realizadas estos generadores de riesgo darán origen a diversos factores de riesgo (*"risk factors"*). Por ejemplo, la precisión será un factor de riesgo clave para las tareas de un cajero, mientras que la capacidad puede serlo para un programador. El siguiente paso será intentar responder cómo estos factores de riesgo podrían materializarse y, en tal caso, estimar las pérdidas que sen generarían.

Para realizar la asignación de riesgos, en general se recaban todos los procesos de la entidad, de tal manera que puedan ser catalogados en un formato estructurado. Para ello se requiere:

- Identificar al personal experto para evaluar los procesos.
- Agregar los reportes de evaluación por producto, localidad, unidad de negocio u otra forma.
- Comparar las auto-evaluaciones de RO con las pérdidas observadas, para luego definir KRI adecuados que permitan estimar los RO.

El diseño de la herramienta para la asignación de riesgos requiere una metodología para identificar y cubrir los riesgos relevantes en los diversos pasos de un proceso (p.ej. la auto-evaluación), seleccionando los KRI mas apropiados, y diseñando las actividades de control adecuadas. Ello permite analizar las causas de los eventos operacionales, como así también vincular las pérdidas financieras con el área de la organización en donde se originó el problema. Este, a su vez, es un paso clave para un proceso de medición y reporte transparente de la exposición al RO, como así también para la mitigación de los riesgos no deseados.

[11] Scandizzo (2005).
[12] Anders & Sandstedt (2003).

Se podría describir el proceso de asignación de riesgos como un mecanismo sistemático para extraer información sobre las maneras en que puede fallar un proceso, es decir, se trata de descubrir "qué es lo que puede salir mal". Para su respuesta, es preciso hacer un análisis minucioso de cada proceso de negocios específico. Este análisis genera dos resultados complementarios. En primer lugar provee una comprensión de las causas y consecuencias de eventos específicos:

- qué recurso en particular genero la falla (persona, proceso o sistema),
- en qué parte de la entidad se generó la falla,
- cuál es el impacto de la falla y qué áreas fueron afectadas.

En segundo lugar, genera una base de datos cuantitativa -o al menos cuantificable- que puede ser usada para modelar el perfil de riesgo de la organización, como así también para guiar a la entidad en cuanto a medidas correctivas. Ello conlleva:

- la medición directa a través de técnicas estadísticas (estimándose la probabilidad y severidad de cada riesgo),
- el diseño de actividades críticas de control, y la correspondiente asignación de recursos, de acuerdo a la importancia relativa de cada exposición,
- la identificación y cómputo de KRIs como una manera de anticipar cambios en las exposiciones al riesgo y poder anticipar problemas.

3.3. Asignación simultánea de riesgos a áreas de riesgo, procesos y productos

Una propuesta de la empresa global de servicios de administración del RO *RiskBusiness*[13], describe el uso de las siguientes dimensiones:

- Grupos de productos y servicios: las líneas de negocio propuestas por Basilea II fueron expandidas a 40 grupos de productos y servicios, que pueden ser considerados en forma separada o agregados como líneas de negocio.
- 45 funciones de negocio (procesos de alto nivel) que permiten englobar en la práctica cada proceso usado para la entrega de un producto o servicio en la industria bancaria.
- 15 categorías de riesgo, elegidas entre las categorías de RO a nivel 2 definidas por Basilea.

La *KRI Library and Services*[14] también está promoviendo este nivel de detalle (ver más adelante en sección 4.3.). Ello permitiría en principio identificar más de 10.000 puntos de riesgo en un cubo tridimensional a los que podrían asociarse los riesgos en una etapa de la provisión de un producto o servicio financiero (los ejes del cubo serían la función de negocio, líneas de negocio, y las categorías de riesgo). Cada punto necesita ser administrado en forma individual y pueden ser usados a efectos de definir indicadores de riesgos (o KRI) y establecer prioridades en cuanto al análisis de ciertos puntos de riesgo críticos. Este procedimiento ayuda a identificar las partes de los procesos que deberían ser modificadas con el fin de cambiar el perfil de riesgos de la entidad.

[13] Taylor & Davies (2003)
[14] KRIeX.

Una vez identificados los puntos de riesgo, puede construirse un "*heat map*" en base a la estimación del riesgo de cada punto numerado por ejemplo, de 1 (menor riesgo) a 9 (máximo riesgo) y con un código de color. Un ejemplo del perfil de riesgo resultante se exhibe en el Anexo IV. El mapa de riesgo resultante provee un mecanismo efectivo para priorizar riesgos y en el caso de ser usado por un conjunto de entidades con los mismos criterios, facilitaría un proceso de "*benchmarking*". Además, en la práctica permitiría crear un perfil de riesgos para cada área de la organización y una imagen de las categorías de riesgo por función de negocio en cada área de riesgo específica.

4. Indicadores de riesgo (KRI)

4.1 Definición

Los *indicadores de riesgo clave* (KRI) son variables de carácter financiero u operacional que ofrecen una base razonable para estimar la probabilidad y severidad de uno o más eventos de RO[15]. Se suelen utilizar parámetros como el número de operaciones fallidas, la tasa de rotación de asalariados, el porcentaje de transacciones que requieren ser ingresadas manualmente, la frecuencia y / o gravedad de los errores u omisiones, etc. En el Anexo V se exponen algunos KRI frecuentemente utilizados, segregados según la categoría de riesgo correspondiente.

Los KRI pueden ser de carácter cualitativo o cuantitativo, aunque estos últimos suelen ser más objetivos a efectos de ser incorporados a las técnicas de estimación del RO. Pueden ser expresados en porcentajes, cantidades o montos de dinero, pero fundamentalmente deben tener un vínculo con la causa raíz que genera los eventos de pérdida por RO. Los KRI también se pueden segregar según su naturaleza, ya que pueden ser de carácter anticipado, histórico, corriente, o bien una combinación de los tres. Entre los atributos deseables de los KRI[16] se pueden citar:

- permiten establecer niveles de riesgo actuales, a través de medidas precisas del estado de un riesgo identificado y la efectividad para su control,
- son útiles para el control del RO, permitiendo acciones preventivas o que minimicen pérdidas materiales al posibilitar una acción temprana,
- posibilitan detectar tendencias y cambios en el nivel de riesgo,
- ofrecen señales de alerta temprana al hacer resaltar los cambios en el entorno, eficiencia de los controles y exposición a riesgos potenciales antes que se materialicen.

Los KRI pueden contribuir a la toma de decisiones a través del establecimiento de umbrales mínimos y rangos de tolerancia para los diversos riesgos, los que deberían ser definidos por las máximas autoridades. Estos umbrales se pueden ajustar posteriormente para ser alineados con la dinámica del entorno de negocios. Una práctica habitual consiste en establecer rangos de valores para cada indicador que permitan asociar un riesgo identificado con las diversas zonas de un mapa de riesgos (ver sección 3). En particular se pueden diseñar acciones de mitigación específicas cuando los valores de los KRI vayan ingresando en zonas de mayor riesgo.

[15] Scandizzo (2003).
[16] Lloyd's (2007).

4.2 Aplicación de los KRI

Los indicadores se suelen clasificar en tres grandes clases: como medidas de riesgo (KRI), medidas de desempeño ("*Key performance indicator*" o KPI) y medidas de control ("*Key control indicator*" o KCI). Se define a los KCI como indicadores que miden la efectividad (p.ej diseño y performance) de un control especifico, de tal manera que un deterioro en un KCI puede indicar un incremento en la probabilidad o impacto de un riesgo residual[17]. A su vez los KPI son medidas que permiten cuantificar objetivos vinculados al desempeño estratégico de una organización. Sin embargo existe cierta dificultad en clasificar unívocamente cada indicador, pues un mismo indicador podría ser adjudicado a distintas clases según el usuario que lo utilice[18]. Obviamente los más relevantes a efectos de la administración del RO son los KRI.

A efectos de realizar un seguimiento del nivel de riesgos, deben revisarse los KRI en forma periódica y sistemática para alertar cambios que puedan indicar problemas. Asimismo deben revisarse periódicamente los umbrales y rangos establecidos para asegurar que permanezcan alineados con el cambiante entorno de negocios y los riesgos significativos asumidos por la entidad en cualquier punto del tiempo. Según la "*KRI Library and Services"*[19] eventos como ciertos fraudes corporativos bien conocidos (ENRON, Worldcom, etc.) y la implementación de Sarbanes-Oxley pudieron haber generado una mayor sensibilización respecto a determinados riesgos.

Es muy frecuente combinar distintos KRI como componentes ponderados de un "*scorecard"* (ver sección 5) para evaluar un proceso o línea de negocio, con la ayuda de una opinión experta, a pesar de que esto último agregue un elemento subjetivo. En algunos casos debe tenerse en cuenta que los indicadores sólo serán útiles en conjunción con otros KRI, y que la relevancia de ciertos KRI puede cambiar a través del tiempo. Por ejemplo Scandizzo ofrece un ejemplo de aplicación de KRIs tal como puede observarse en siguiente cuadro.

Cuadro 4: Uso de KRIs para evaluar la actividad de desembolso de préstamos[20]

Indicadores de riesgo	Unidad	Valor	Tendencia (%)	Límite inf.	Limite sup.	Score	Pond.
Backlog	%	7.4	1.5	5	10	2	1
Tasa errores	%	4.9	3.4	3	5	2	1
Pérdidas financieras	EUR	200.000	5.6	100.000	1.000.000	1	3
Errores de reconciliación	%	9.8	15.3	1	5	3	2
Operaciones aprobadas vs. total operaciones	%	93	5	95	85	2	1
Existencia de alternativas (p.ej. backups)	Si / No	Si	0	–	–	1	2
Puntaje de auditoría	1– 4	3	0	3	2	2	2
Retrasos de procesamiento	Hrs	25	45	8	16	3	2
Tiempo de sistema caído	Hrs	3.4	7	2	5	2	3
Resultados de la evaluación regulatoria	1– 4	4	0	3	2	1	2
Monitoreo performance de los proovedores	Si / No	Si	0	–	–	1	1
Costos de oportunidad	EUR	5,000.000	35	1.000.000	3.000.000	3	3
Puntaje ponderado de la actividad						**1,96**	

[17] *KRIex.*

[18] Considérese p.ej. una operación de "Trading and Sales" ejecutada por un operador la que es reconfirmada con la contraparte a través de un tercero, y que además involucra una tercera función que liquida las correspondientes obligaciones. Un indicador que registra el número de transacciones aún no confirmadas podría ser interpretada como un KPI para el operador (pues mide la frecuencia de errores), un KCI para el tercero independiente (pues representa el número de transacciones no confirmadas lo que implicaría la necesidad de mejoras), y un KRI para la función que cierra la operación (pues este tipo de operaciones puede resultar en errores o en impagos). Fuente: "*KRI Library and Services", KRIex.*

[19] KRIex.

[20] Scandizzo (2003).

Las fuentes de información que permiten identificar riesgos significativos y contribuyen en el diseño de KRI son las bases de datos de pérdida por RO, los resultados de los procesos de auto-evaluación del RO, los informes de auditoría interna y externa y de los órganos de supervisión, como así también la información obtenida a través de conversaciones con las diversas líneas de negocio.

Los KRIs tienen una serie de aplicaciones, entre las cuales se puede mencionar[21]:

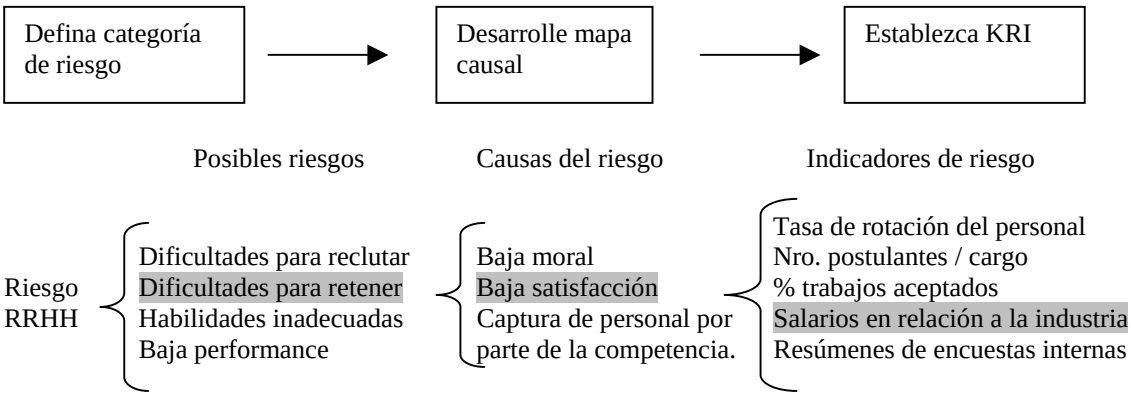
- Potencial para identificar zonas de alto riesgo, lo cual permite anticiparse y minimizar pérdidas.
- Capacidad para identificar procesos y/o debilidades en los controles, lo que permite fortalecer los mismos y resolver problemas.
- Establecer objetivos en términos de los KRI, a través de los cuales puede condicionarse la conducta del personal para lograr los resultados deseados.
- Alcanzar los niveles de apetito por riesgo de la entidad, estableciendo niveles de tolerancia para los diversos KRI.
- Cumplimiento regulatorio: la identificación y administración de los KRI puede ser objeto del control del ente regulador.
- Asignación de capital económico a las diversas líneas.

Es importante conocer los aspectos prácticos vinculados a la implementación de los KRI. Se suelen crear grupos de trabajo en las líneas de negocio a efectos de identificar indicadores importantes en sus procesos, colaborando con asesores expertos y/o niveles gerenciales superiores. Se establecen responsabilidades específicas y recursos informáticos para cargar los KRI, integrarlos, y difundirlos a través de reportes a los usuarios interesados y a la gerencia senior. Se puede solicitar colaboración técnica a otras áreas para garantizar que los KRI estén focalizados en áreas críticas y que sean implementados en forma robusta, de tal manera que apoyen efectivamente la toma de decisiones y el control de riesgos. El número de KRI adecuado variará dependiendo de la escala, sofisticación, características yb recursos de la entidad que los implementará.

A continuación se exhibe un ejemplo muy sencillo de cómo identificar un KRI, en el caso particular de observarse dificultades para retener al personal (ver Cuadro 5). Como consecuencia de observar una mayor tasa de deserción del personal en relación a la industria, el sector de RRHH de un banco crea un grupo de trabajo para identificar los posibles riesgos vinculados con su área, e identifica cuatro riesgos principales. A continuación realiza una serie de encuestas internas de las cuales surge que existen cuatro causas, entre las cuales se destaca un bajo nivel de satisfacción entre el personal. Como consecuencia de ello se solicita a una función interna o consultor externo especializado, que identifique una serie de indicadores internos asociados a dicho factor. Posteriormente, a través de un análisis estadístico, se detecta una fuerte relación entre uno de los KRI (salarios) y la dificultad para retener personal, concluyéndose que es el KRI adecuado para controlar el problema.

[21] Lloyds (2007)

Cuadro 5: Ejemplo de identificación de un KRI



La forma más práctica para hallar KRIs adecuados consiste en concentrarse en los RO significativos y sus causas y considerar indicadores históricos y / o "*forward-looking*" cuya evolución pueda estar vinculada a ellas. Algunas empresas incluso aplican técnicas estadísticas como análisis de componentes principales, análisis discriminatorio y control estadístico de los procesos, para explorar la relación entre los KRI y las pérdidas operativas, como así también para hallar la importancia relativa de un indicador dentro de un conjunto amplio de KRI[22]. Algunos autores proponen aplicar las técnicas de control estadístico de la calidad al análisis de estos indicadores (ver Cuadro 6).

Cuadro 6: El control estadístico de la calidad en los procesos de las entidades financieras

Cuando se habla de procedimientos cuantitativos en el marco de la administración del RO, usualmente se hace referencia al análisis de las pérdidas históricas y no tanto al proceso de definir medidas útiles para la administración diaria del RO. En tal sentido es útil el desarrollo de medidas estadísticamente robustas, comparables y consistentes para medir la calidad de los procesos.

Shepheard-Walwyn (2004) propone aplicar las técnicas cuantitativas existentes por ejemplo en la industria manufacturera, a la administración y el control de la calidad de los procesos en la industria financiera. A tal fin propone la aplicación del control estadístico de la calidad ("*statistical process control*" o SPC), ampliamente difundido en la industria manufacturera, que implica básicamente mejorar la media de un proceso y la reducción de la variabilidad del mismo. Los procesos vinculados a los servicios financieros (ya sea apertura de cuentas, realización de pagos, etc.) pueden ser estimados, de tal manera que pueden establecerse métricas (aplicadas a KRIs) adecuadas para su medición[23]. El SPC propone medidas puntuales de alerta temprana para dichas métricas, como la obtención de un resultado a más o menos desvíos estándar de la media; una corrida de X resultados seguidos por encima o debajo de la media, etc. Señales como estas, que son definidas usando estrictas técnicas estadísticas, proveen una forma consistente de caracterizar problemas de calidad en procesos claves de las entidades financieras.

La media y varianza de un proceso son "*proxies*" atractivas por su contribución al riesgo, siempre y cuando se pueda establecer una relación lineal entre pérdidas y riesgo. Incluso sin esa relación lineal podría usarse la varianza de ciertos KRI (apertura de cuentas, ausentismo, manejo de las quejas) para comparar el desempeño – y tal vez el riesgo relativo – entre distintas líneas de negocio. Además abriría la posibilidad de definir umbrales y rangos de valores a través de medidas del tipo VaR.

La madurez de la administración del RO será alcanzada cuando pueda establecerse un lenguaje común, desarrollar un enfoque estadístico para la administración de los procesos y establecer vínculos entre las métricas de los procesos y las pérdidas por RO. En tal sentido el análisis de un conjunto de KRI mediante el uso consistente de métodos SPC proveen una herramienta fundamental.

[22] Sungard Bancware Erisk (2007)
[23] Corregidas por el ciclo económico y de negocio.

4.3. El proyecto de la "KRI – Library and Services"

La "*KRI Library and Services*" es una iniciativa orientada a las compañías de servicios financieros interesadas en mejorar su administración del RO. Este proyecto se inició a través de un estudio de dos años de los KRI en la industria bancaria y es liderado por un grupo conformado por representantes de bancos internacionales[24]. En la actualidad es administrada por la *Risk Management Association* y *RiskBusiness International*. La participación está abierta a cualquier entidad financiera incluyendo bancos, comisionistas, administradores de fondos y de activos, aseguradoras y bancos centrales.

Esta biblioteca consiste en un consorcio que reúne información referida a KRI de las entidades participantes[25] y ya tienen registrados más de 1800 indicadores consistentes en cuanto a la definición y a su forma de medición. Los mismos se asignan a puntos específicos de riesgo en un cubo de riesgos, cuyas dimensiones fueron definidas según 15 categorías de riesgo[26], 50 productos y servicios (y que cubren múltiples líneas de negocio)[27], y 47 funciones corporativas y de procesos específicos. En dicho cubo el usuario puede identificar los KRI más apropiados en función a sus necesidades específicas. Típicamente los KRI aparecen en más de un nodo de riesgo, y 74 de ellos aparecen en todos, por lo cual fueron designados como indicadores comunes.

Este esquema puede ser usado para establecer perfiles de riesgo para cada producto o grupo de servicios, como así también de toda la organización. A cada nodo se le asigna un puntaje en función del riesgo residual asociado al mismo. Este mapa permite priorizar y focalizar los esfuerzos en determinadas áreas y facilita la comparación y en algunos casos el *"benchmarking"* contra una mapa promedio (resultante de la agregación de los datos de todos los contribuyentes).

La biblioteca inicialmente se ha concentrado en aquellos nodos que fueron identificados por los actuales usuarios como de mayor riesgo. Cada uno de los KRI viene acompañado por definiciones y especificaciones detalladas y esto es acompañado por una guía sobre cómo aplicarlo para lograr los mejores resultados. A su vez se los clasifica según su grado de compatibilidad interna y externa, la facilidad para recolectar la información y la efectividad del KRI para identificar un riesgo determinado en un punto especifico del cubo de riesgos.

El proyecto también incluye un servicio de "*benchmarking*", donde las entidades pueden comparar sus valores para un KRI determinado, contra las estadísticas de la industria o un grupo de pares. Esto permitirá a los miembros desarrollar criterios para establecer umbrales o para tomar medidas correctivas cuando los KRI se salen de rangos preestablecidos. Esta información, combinada con los datos de pérdida por eventos operativos recolectada por consorcios de datos (p.ej. ORX), contribuye a la industria a entender la manera en que los KRI ayudan a estimar el riesgo y predecir pérdidas futuras.

[24] ABSA, Citigroup, Commonwealth Bank of Australia, Dresdner, Erste Bank, Investec, Kleinwort, KeyCorp, Royal Bank of Canada, State Street y Wachovia

[25] En la actualidad son 65, principalmente bancos.

[26] Para asegurar consistencia con Basilea II se usaron 15 de las líneas de nivel 2 de eventos de pérdida operativa allí propuestas.

[27] Las líneas de negocio propuestas por Basilea II fueron expandidas a 40 distintos productos y grupos de servicios.

5. Scorecards / RDCA

La técnica de *tarjetas de puntaje* ("*scorecards*")[28] se refiere a un conjunto de sistemas expertos para la medición del RO que tienen en común la evaluación de los generadores de riesgo ("*risk drivers"*), como así también, la evaluación de la amplitud y calidad del ambiente interno de controles de riesgos, todo ello a través del uso de cuestionarios. La metodología de tarjetas de puntaje también suele ser conocida como "R*isk Drivers and Control Approaches"* (RDCA).

Estos cuestionarios consisten en una serie de preguntas ponderadas y basadas en el nivel de riesgo de la línea de negocio consultada, que permiten trasladar evaluaciones cualitativas a una métrica cuantitativa. El cuestionario está diseñado de tal manera de reflejar el perfil de riesgos único de la entidad, lo que se logra a través del diseño de preguntas específicas para la organización, la calibración de las respuestas, y la aplicación de ponderadores y puntajes alineados con la importancia relativa del riesgo para la entidad. Las tarjetas son usualmente completadas por personal de línea a intervalos regulares y sujetas a revisión por una función centralizada de control de riesgos. Un ejemplo de cuestionario referido al fraude interno para ser contestado a nivel de unidad de negocio se puede ver en el Anexo VI.

Esta técnica transforma evaluaciones de carácter cualitativo en medidas cuantitativas que permiten clasificar de forma relativa los diferentes tipos de exposiciones al RO. Al involucrar a las líneas de negocio en el desarrollo y diseño del marco del RDCA, las responsabiliza por los resultados informados. Asimismo su participación potencia el desarrollo colectivo del conocimiento del RO al involucrar también a los especialistas de los riesgos clave. Además suele ser muy útil en cuanto motiva a cada unidad de negocios a pensar en los RO a los que se ven expuestas.

Un aspecto importante del RDCA es que evalúa el RO al momento de detectarse las debilidades y vulnerabilidades es decir, cuando la probabilidad de ocurrencia es alta, resultando en consecuencia en una herramienta de carácter *"forward looking"*. Ello contrasta con la estimación del RO obtenida exclusivamente a partir de datos de pérdida históricas en cuyo caso, debido a las acciones correctivas posteriores, la probabilidad de pérdidas se ve afectada.

Las evaluaciones de riesgo hechas a través de esta técnica son explícitas y transparentes, especialmente para los gerentes de línea y suelen estar sujetas a un escrutinio regular por parte de la gerencia, la auditoria y los supervisores. Por otra parte, el RDCA responde rápidamente a cambios en el entorno de negocios, o a la aparición de nuevos ROs, permitiendo acomodar los nuevos riesgos a medida que van surgiendo, agregando preguntas o cambiando otras, sin necesidad de esperar a que se materialicen las pérdidas. Por su diseño, las metodologías RDCA están totalmente alineadas con el marco de gestión del RO de la entidad, vinculando en consecuencia la medición con el seguimiento de dicho riesgo.

Asimismo, las entidades podrían utilizar esta técnica para asignar el nivel de capital económico que corresponde a cada línea de negocio dependiendo de los resultados de la gestión y control de diversos aspectos del RO (ver cuadro 7). La directa vinculación entre el capital económico y el desempeño de las gerencias ofrece fuertes incentivos para realizar

[28] RMG (2003)

mejoras en la gestión del RO, al centrar los esfuerzos de las unidades de negocio en mitigar el riesgo y mejorar los controles internos.

Cuadro 7: Ejemplo de proceso para determinar el capital económico con RDCA[29]

1er paso: Hacer una primera estimación del requisito de capital por RO, basada en una serie de técnicas, que incluyen:

- Un "benchmarking" respecto a una fracción del capital total, respecto a entidades financieras similares, o respecto al capital determinado a través del método estandarizado propuesto por Basilea II.
- Un análisis de las distribuciones de pérdida (LDA).
- Un análisis a través del uso de escenarios (SBA).

2do paso: Uso de un cuestionario consistente de preguntas ponderadas basadas en riesgo orientadas a estimar los principales generadores de riesgo (*risk-drivers*) y controles establecidos para todo el rango de categorías de RO determinadas en la entidad[30]. El cuestionario deberá:

- Ser completado por las unidades de negocio.
- Recabar información respecto el nivel de los generadores de riesgo (risk-drivers) y la calidad de los controles establecidos para cada categoría de riesgo.

3er paso: Asignar un requisito inicial de capital a cada una de las categorías de riesgo, como por ejemplo "fraude interno". Esta asignación también tendrá en cuenta:

- Datos internos y externos sobre riesgo operativo.
- Información cualitativa recabada en los cuestionarios.

4to paso: Distribución del capital asignado para cada categoría de riesgo entre las diversas líneas de negocio, basada en el perfil de riesgos y escala determinada a través del cuestionario.

Un aspecto fundamental es la validación del RDCA con el objetivo de verificar que los resultados que arroje el modelo sean razonables. Para ello habrá que tener en cuenta que será muy difícil en el corto plazo implementar una validación puramente estadística y en cambio cobrará mucha importancia un "*test de uso*" del modelo como parte de la gestión día a día del proceso. Algunos componentes de la validación del modelo son:

- Evaluación de la sensibilidad de los parámetros (puntaje y ponderador de cada pregunta, hipótesis de las distribuciones, etc.).
- Comparación de las respuestas a los cuestionarios con datos de pérdidas interna / externa debidos al RO y considerar el uso de los escenarios de estrés, utilizando también la opinión de expertos.

Alguna de las lecciones aprendidas en la implementación de un RDCA incluyen[31]:

- Asegurar el compromiso del máximo órgano de conducción de la entidad para asignar el capital por RO a cada línea de negocio.

[29] Elaborado en base a FSI Connect: "Basel II – Operational Risk – AMA" (2007).
[30] Estas categorías de riesgo podrían ser las definidas en Basilea II, o las determinadas por cada banco.
[31] SWG (2003).

- Involucrar a las líneas de negocio desde un principio.
- Hacer una experiencia piloto con algunas líneas de negocio a efectos de incorporar comentarios.
- Diseñar las preguntas de tal manera que puedan ser validadas en forma independiente.

Scandizzo[32] asocia las tarjetas de puntaje (las que denomina "*balanced scorecards"*) de RO a una presentación organizada de los KRI's, identificados para cada factor de riesgo, de tal manera de cubrir todos los procesos de la entidad. Según este autor, la tarjeta de puntaje debe estar organizada en función de los generadores de riesgo (tamaño y complejidad de las operaciones, personas, procesos, sistemas y eventos externos) y contener KRI's, pérdidas operacionales e información cualitativa referida a los cambios en el perfil de riesgo y en la estructura de controles internos de la entidad. Esta información cualitativa debería reflejar mejoras en el ambiente de control del riesgo que alterarán la frecuencia y severidad de futuras fallas debidas al RO.

Las tarjetas de puntaje también pueden ser utilizadas como una herramienta de seguimiento del RO, facilitando una serie de controles al combinar KRIs en la evaluación y reporte de impacto de nuevos controles y otros cambios en el ambiente operativo de la entidad. En el Anexo VII se muestra un ejemplo de una tarjeta de puntaje de RO, reproducido de Scandizzo. A efectos de su agregación, los KRI deben ser normalizados, esto es expresados sobre una base común[33]. Asimismo deberá ponderárselos, basándose entre otros aspectos, en opinión experta, datos de pérdidas pasadas, evidencia empírica e información gerencial. También podrá hacerse la ponderación en base a los objetivos estratégicos de la entidad, a efectos de incentivar las conductas buscadas.

6. Análisis de escenarios (SBA)

El análisis de escenarios (en inglés "*Scenario based approach"* o SBA) consiste en la modificación conjunta de un rango de parámetros que afectan la posición de la entidad financiera en una forma coherente y simultánea[34]. Los escenarios constituyen eventos hipotéticos que podrían ocurrir y deben ser representativos para cada entidad, teniendo en cuenta todos los factores de riesgo relevantes. Los escenarios pueden involucrar la ocurrencia de eventos catastróficos de carácter financiero u operacional, pero también pueden involucrar cambios en los planes de negocio, cambios en los ciclos económicos y daños a la reputación de la entidad debidos a fraudes o escándalos financieros. Los escenarios pueden ser generados de varias maneras, por ejemplo a partir de modelos estadísticos basados en las distribuciones de frecuencia y la severidad de los eventos de RO, el análisis o repetición de eventos históricos, o eventos hipotéticos.

Una variante de los análisis de escenarios son los *tests de sensibilidad*, que involucran la modificación de los valores de un solo parámetro de tal manera que afecte la posición de la entidad financiera en forma extrema, con el fin de determinar el impacto sobre su salud financiera de la entidad.

[32] Scandizzo (2005).
[33] Por ej. podrían tomarse como [Indicador / máx. (Indicador)], de tal manera que resulte un valor entre 0 y 1.
[34] Lloyds (2007).

Para implementar el análisis de escenarios, como primer paso, se categorizan los factores de riesgo. A su vez, se puede desagregar la entidad en áreas organizacionales en las cuales pueda evaluarse el RO en forma independiente. A continuación se identifica un conjunto razonable de eventos realistas que reflejen la dinámica del negocio, basados en el marco de la administración de riesgos, el registro de riesgos, las opiniones de la línea gerencial además de las opiniones de expertos en el tema. Los eventos que deben ser considerados y cuantificados a través del uso de esta técnica son los que generan pérdidas esperadas (las que deberían ser previsionadas), pérdidas inesperadas (se les asigna capital económico) y pérdidas extremas[35].

Con esta información se procede a generar clases de escenarios que tengan[36]:

- Consistencia: cada área de la entidad considera al menos un conjunto común de clases de escenarios, para lo cual una serie de *workshops* facilitados por una función centralizada de gestión del RO puede ser efectiva. A efectos de una mayor consistencia también puede contribuir una revisión por parte de la auditoría interna.
- Relevancia: cada área de la entidad determina si los escenarios son relevantes para su actividad.
- Los escenarios determinados deben maximizar la cobertura de los riesgos previstos. Esto se puede lograr a través de una discusión con todas las áreas para garantizar que se cubran cada uno de sus riesgos específicos.

Cada área organizacional deberá evaluar el impacto de los escenarios, para lo cual suelen usarse:

- Cuestionarios
- "Workshops" guiados
- Matrices de recursos críticos vs. estado de los riesgos
- La propia experiencia de la alta gerencia.

Un ejemplo de este análisis se representa en el Anexo VIII. Allí se incluyen efectos directos e indirectos, como así también los impactos debidos a fallas en los controles[37], a la vez que se considera la calidad del ambiente de control de la entidad y se complementa el análisis con el uso de KRI's y pérdidas históricas.

Para validar las evaluaciones de los escenarios se suelen aplicar auditorias internas al proceso de evaluación y a la calidad resultante, y se comparan las pérdidas estimadas contra las esperadas por los expertos.

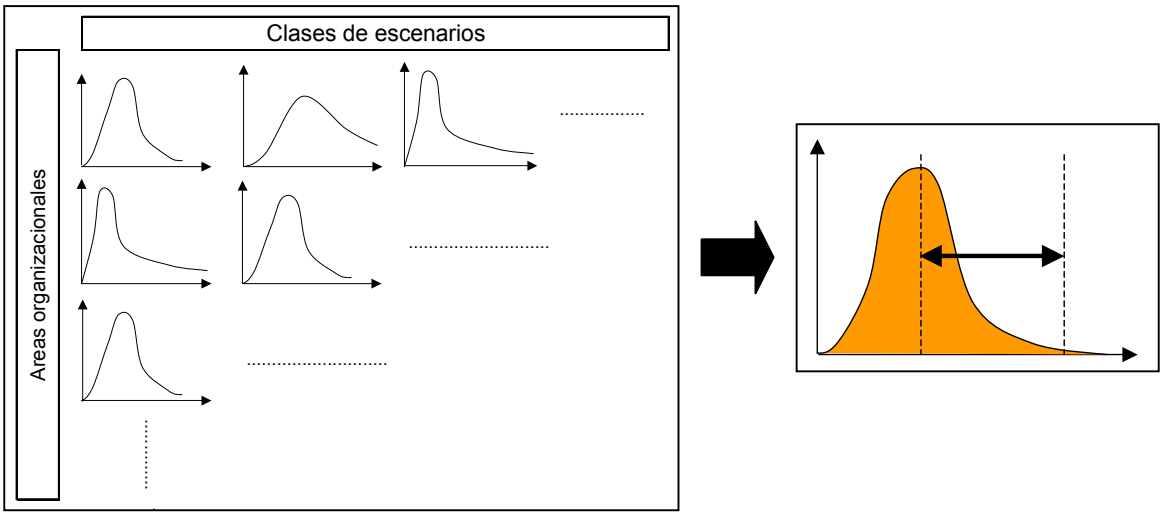
Una vez evaluados los escenarios en cada área organizacional se los emplea para modelar estadísticamente las distribuciones de pérdida. A través de los datos de pérdida que surgen de aplicar los escenarios, se estiman los parámetros del modelo estadístico elegido para la frecuencia y la severidad de los eventos[38]. Determinados estos parámetros puede calcularse la

[35] Las pruebas de estrés y el análisis de escenarios se concentran en la medición y cuantificación de pérdidas inesperadas y el daño reputacional asociado a ellas.
[36] SBA(2003).
[37] Es importante considerar los efectos colaterales al cuantificar los efectos de cada escenario. Por ej. un evento que involucra grandes pérdidas puede tener como consecuencia "defaults" de compañías reaseguradoras de ese tipo de eventos.
[38] Algunas de las distribuciones de pérdida usadas para la severidad son la Lognormal y Normal Gamma, y para la frecuencia la Binomial negativa y la Poisson.

distribución de pérdida resultante mediante el uso de la técnica de simulación de Monte-Carlo.

Un paso posterior consiste en agregar los resultados del análisis de escenarios para todo el grupo, en cuyo caso puede ser apropiado considerar los efectos de la correlación entre escenarios. Como resultado de este proceso se obtiene primero una matriz de distribuciones de pérdida por RO para cada área de la entidad, y para cada clase de escenario. Finalmente puede estimarse una distribución de pérdidas por RO para toda la entidad tal como esquematiza la siguiente figura.

Figura 3: distribución de pérdidas operativas



La importancia de implementar estas técnicas reside en que:

- Son *forward-looking*, se vinculan directamente con el proceso de gestión y promueven una sana administración del riesgo.
- El proceso de evaluación y análisis de los factores de riesgo permite una mayor comprensión de los RO y proveen información importante para mejorar la gestión.
- Capturan de manera rápida, cambios en el perfil de riesgos de la entidad y / o en la estructura organizacional.
- Establecen lazos entre los riesgos y sus controles.
- Ayudan a evaluar el impacto financiero y no-financiero de eventos extremos con grandes pérdidas inesperadas.
- Ayudan a determinar el perfil global de riesgos de la entidad y a establecer el apetito por riesgo dada su capacidad de asumirlo.
- A partir de la razonabilidad de los resultados, permiten validar modelos y los análisis estocásticos realizados, como así también la calibración de las hipótesis del modelo.
- Proveen información para la determinación del capital económico[39] y son por ello un elemento integral del marco de administración de riesgos de la entidad.

[39] Ver Cuadro 8

Cuadro 8: Ejemplo de proceso para determinar el capital económico con SBA [40]

Los pasos involucrados en un proceso SBA son los siguientes:

1er paso: Generación de escenarios. Los factores de riesgo que reflejan el perfil de RO de la entidad se identifican y categorizar en clases de escenarios. Estas clases de escenarios pueden ser luego aplicadas a las líneas de negocio que pueden verse impactadas por esos factores de riesgo.

2do paso: Se evalúan los escenarios generados. Esto puede hacerse según varios criterios, que pueden incluir el uso de datos históricos de pérdida, el uso de KRIs, coberturas obtenidas a través de pólizas de seguro, la calidad de los factores de riesgo relevantes, y el ambiente de control.

3er paso: Se validan las estimaciones. Este proceso verifica la razonabilidad de los resultados de la evaluación a través de escenarios en el contexto del perfil de riesgos operacionales de la entidad. Las técnicas usadas pueden incluir evaluaciones de la auditoria interna, comparaciones de las pérdidas estimadas respecto a lo esperado por personas expertas en el tema, y revisiones de los gerentes de riesgo.

4to paso: Desarrollo de un modelo estadístico basado en las distribuciones de frecuencia y severidad para estimar las pérdidas futuras, que podrá incluir simulaciones de Monte-Carlo.

5to paso: Derivación del requisito de capital a partir del agregado de todas las distribuciones de pérdida, para un determinado nivel de confianza y el horizonte temporal elegido.

7. Conclusiones

Los requerimientos regulatorios respecto de la aplicación de sanas buenas prácticas en la administración del RO, en conjunto con un interés creciente de las entidades en gestionar este riesgo, han colaborado, entre otros factores, al desarrollo de diversas técnicas cualitativas para la gestión del RO. Esas metodologías permiten realizar una evaluación presente y *"forward-looking"* de los factores de riesgo de negocios subyacentes y del ambiente de controles internos de la entidad financiera y resultan complementarias al uso de datos internos y externos en la evaluación del RO.

Debido a que las entidades financieras tienen particularidades que las diferencian entre sí, no existe una única técnica o metodología universalmente aplicada con idénticas características, sino que la implementación práctica depende en gran medida de las características específicas, negocios, procesos y controles internos de cada entidad.

En este trabajo se expusieron algunas de esas metodologías de gestión del RO, tales como la auto-evaluación del RO, los indicadores de riesgo (KRIs), los procesos de asignación del riesgo, las tarjetas de puntaje (scorecards), y el análisis de escenarios. Estas técnicas resultan un complemento necesario a los datos internos y externos y a la evaluación que pueda hacerse en base a ellos.

Desde el ámbito regulatorio, el uso de estas técnicas comenzó siendo impulsado por el BCBS en sus estándares de sanas prácticas de gestión del RO del año 2003, en los cuales se señala que además de la recolección de datos históricos de pérdidas operativas, también se deben identificar y evaluar los RO a través del uso de indicadores de riesgo (KRIs), las auto-evaluaciones del RO, la asignación o "mapeo" de riesgos, etc.

[40] Basado en FSI Connect: "Basel II – Operational Risk – AMA" (2007).

Por otro lado, las técnicas cualitativas para la gestión del RO permiten identificar los factores básicos del entorno de negocio y del control interno que pueden modificar el perfil de RO de las entidades financieras. El uso de estos factores hace que las evaluaciones del riesgo que realice la entidad estén más orientadas hacia el futuro; reflejen de forma más directa la calidad de los entornos operativos y de control de la institución; contribuyan a alinear las evaluaciones de capital con los objetivos de la gestión de riesgos y reconozcan de una manera más inmediata tanto la mejora como el deterioro de los perfiles de RO. Por último, y como se puntualizó a lo largo del trabajo, muchas veces las técnicas se hallan interrelacionadas, ya que pueden emplearse en conjunto, o bien porque una de ellas incluye el uso de otra.

Referencias bibliográficas

- Anders & Sandstedt (2003) *"An operational risk scorecard approach"*, revista RISK, Enero 2003.

- BCBS (2003) Basel Committee on Banking Supervision: *"Sound practices for the management and supervision of operational risk"* y versión en español: *"Buenas prácticas para la gestión y supervisión del riesgo operativo"*, Febrero 2003.

- BCBS (2004) Basel Committee on Banking Supervision: *"International Convergence of Capital Measurement and Capital Standards. A revised framework"*, Junio 2006.

- BCRA (2008) COM. "A" 4793: *"Lineamientos para la gestión del riesgo operacional en las entidades financieras. Texto ordenado"*, Abril 2008.

- Fitch Rating (2004): *Financial institutions special report: "The Oldest Tale but the Newest Story: Operational Risk and the Evolution of its Measurement under Basel II"*.

- Financial Stability Authority (2007): *"Operational Risk Appetite"*, Operational Risk Appetite Expert Group, Abril 2007.

- Huebner, R. (2001): *"The qualitative analysis of operational risk"*, CFS Forum, Diciembre 2001.

- KRIex - http://www.kriex.org (es una iniciativa de las empresas "RiskBusiness" y de "The risk management association").

- Lloyd's (2007) - http://www.lloyds.com (Risk management toolkit).

- RMG (2003): "Risk drivers and controls approaches: linking operational risk measurement and management", Risk management group's Conference on Leading issues in operational risk measurement – Presentation by Scorecard Working Group, Federal Reserve Bank of New York, May 2003.

- SBA (2003) "Scenario-based AMA" Presentation for RMG- Conference, 5/ 2003.

- Scandizzo (2003) "Risk mapping and key risk indicators in operational risk management", Economic Notes by Banca Monte dei Paschi di Siena SpA, vol.34, nr. 2-2005, pp.231-256.

- Scorecard Working Group (2003): "Risk drivers and controls approaches: linking operational risk measurement and management". Risk management group's conference on leading edge issues in operational risk measurement. Federal Reserve Bank of New York , Mayo 2003.

- Seivold (2008): *"Business Environment & Internal Control Factors (BEICFs)"* presentado en el seminario sobre tópicos de Basilea II en el Banco Central de Argentina, Mayo 2008.

- Shepheard-Walwyn (2004) “KRI VaR: lessons from manufacturing for the financial services industry”, Risk Management Association (RMA) Journal, Mayo 2004.

- Sungard Bancware Erisk (2007): http://www.erisk.com/Learning/JigSaw/OperationalRisk.asp

- Taylor & Davies (2003): “Getting traction with KRIs: laying the groundwork”, The RMA Journal, November

Anexo I: Registro de riesgos operacionales (ejemplo 1)[41]

Evento de riesgo 1.1: Gestión ineficiente de la información ó de la tecnología informática

Propietario del riesgo: XXX **Impacto / probabilidad inherente:** B1

Componentes del riesgo:
Rupturas de confidencialidad de la información como ser filtraciones de información sensible a precios ó aspectos comerciales
Gestión de información inadecuada, con retrasos, o de baja calidad que afecta la efectiva toma de decisiones ó generación de reportes.
Rupturas de la legislación asociada a la protección de los datos.
Fallas para mantener una estrategia de IT.

Control	Procedimiento	Propietario del control	Descripción del control	Tipo	Frecuencia	Diseño	Desempeño
Establecer estrategia IT	xx	xx	Estrategia para provisión de IT y desarrollo de programas	Preventivo	Anual	V	V
Procedimiento de protección de datos	xx	xx	Procesos de registración, requiere conexión y avisar al "staff"	Preventivo	sobre la marcha	V	V
Terminos de los contratos de empleo	xx	xx	Todos los contratos de empleo contienen declaraciones de adhesión a las regulaciones relativas a información sensible y temas vinculados a laseguridad	Preventivo	sobre la marcha	A	V
Comité de IT	xx	xx	El comité de IT hace reuniones de actualización mensuales	Preventivo	Mensual	V	V

Evaluación:
Nivel elevado de controles preventivos, departamento interno de IT con amplia experiencia.
Los registros históricos no sugieren implicancias materiales.

Impacto / probabilidad residual: A1
Impacto / probabilidad objetivo: A1

Fecha de revisión de la evaluación: xx yy zz

Evento de riesgo 1.2: Fallas ó pérdida de una infraestructura clave

Propietario del riesgo: XXX **Impacto / probabilidad inherente:** B1

Componentes del riesgo:
Actos maliciosos o terrorismo dirigidos a la entidad.
Accidentes o daños no intencionales incluyendo daños por incendios e inundaciones.
Actos generalizados (fallos para el acceso p.ej. dificultades con el transporte).
Fallas tecnicas (incluyendo fallas del software y caída de redes informáticas).
Fallas de servicios criticos u otros servicio provisto por terceros.
Fallos con los datos, incluyendo los resultantes de ataques por hackers o virus.
Fallas de los sistemas de procesamiento centrales.

Control	Procedimiento	Propietario del control	Descripción del control	Tipo	Frecuencia	Diseño	Desempeño
Plan de continuidad del negocio (recuperación en caso de desastres)	xx	xx	Plan de continuidad del negocio (documentado como procedimiento y parte del manual del personal) atendiendo todos los temas de infraestructura, incluyendo IT, datos y reemplazo de personal. Será revisado regularmente y puesto a prueba (incluyendo proveedores externos).	Preventivo	Anual	A	V
Controles de seguridad para IT	xx	xx	Controles apropiados de IT para preservar su seguridad de los sistemas e integridad de los datos, incluyendo facilidades de back-up que son regularlmente testeadas.	Preventivo	sobre la marcha	A	V
Seguridad física disponible	xx	xx	Medidas de seguridad apropiadas para prevenir acceso no autorizado a la infrastructura, asi como códigos de acceso y sistemas de alarma que son regularmente comprobados. Existencia de sistemas contra incendios.	Preventivo	sobre la marcha	A	V
Existencia de pólizas de seguro	xx	xx	Políticas apropiada de cobertura con pólizas como ser responsabilidad civil, accidentes personales, son revisados regularmente.	Preventivo	Anual	A	V

Evaluación:
Nivel elevado de controles preventivos.

Impacto / probabilidad residual: A1
Impacto / probabilidad objetivo: A1

Fecha de revisión de la evaluación: xx yy zz

[41] Lloyds (2007): "Self-assesment tool 6.10"

Anexo I: Registro de riesgos operacionales (ejemplo 2)

CATEGORIA DE EVENTOS 1 – FRAUDE INTERNO

Pérdidas debidas a actos de algún tipo con la intención de defraudar, malversar bienes o incumplir regulaciones, la ley ó las políticas de la empresa (excluyendo eventos vinculados con la diversidad / discriminación), que involucren al menos a un empleado de la entidad.

Categorías de eventos de 2do nivel son:

1.1 Robo y extorsión
1.2 Fraude
1.3 Infracción a los códigos profesionales e internos
1.4 Violación de los sistemas de seguridad

……

1.2 – Fraude

Descripción del riesgo	**Causas**
FRAUDE INTERNO	**Categoría de causas 1: Organización** 1. Estructura organizacional inadecuada 2. Insuficiente segregación de tareas **Categoría de causas 2: IT** 3. **Categoría de causas 3: Información** 4. **Categoría de causas 4: Recursos humanos** 5. Procedimientos de captación de personal inadecuados **Categoría de causas 5: Procesamiento** 6. Procesos de control inefectivos 7. Uso creativo de regulaciones / procedimientos 8. No adhesión a regulaciones / procedimientos 9. Colusión entre personas **Categoría de causas 6: Disrupción externa** 10.
Definición del riesgo Es el riesgo de que (nombre gerencia) sea incapaz de prevenir o detectar fraudes internos y / o que los procedimientos existentes no apoyen la prevención o detección de fraudes. Resultando en: - Pérdida financiera sustancial - Daño a la reputación - Responsabilidad criminal - Posibilidad de evitar o dificultar procedimientos	

……

1.4 – Violación de los sistemas de seguridad

Eventos que involucren el ingreso no autorizado a archivos de datos electrónicos para beneficio personal debido o con la asistencia de empleados.

Descripción del riesgo	**Causas**
SISTEMAS DE SEGURIDAD **Definición del riesgo** El riesgo de que las medidas de seguridad de (nombre gerencia) no garanticen que: - personas no autorizadas tengan acceso a datos / información crítica (confidencialidad) - Sistemas / información este disponible - Datos / información sea confiable resultando en: - ruptura de confidencialidad - acceso no autorizado (o uso) de aplicaciones / información - daño reputacional - difusión no autorizada de un negocio - pérdida de negocios - suspensión de la actividad de la empresa	**Categoría de causas 1: Organización** 1. Asignación de un número mayor de accesos que los necesarios para la tarea **Categoría de causas 2: IT** 2. Inadecuación de sistemas, lo que lleva a l uso de sistemas secundarios (p.ej. hojas Excel) 3. Encriptación insuficiente de información confidencial almacenada en ambientes inseguros o enviados vía e-mail a través de canales inseguros. **Categoría de causas 3: Información** 4. Documentación dirigida a otra impresora 5. Negligencia con el uso de información confidencial 6. Impresiones sensibles no son destruidas después de usarse 7. Control de auditoría inadecuado o inexistente 8. Uso de contraseñas débiles (que pueden ser inferidas fácilmente) 9. Difusión de contraseñas 10. Validación de perfiles de acceso y de asignación de usuarios irregular / inadecuadas 11. Falta de requisitos de autorización **Categoría de causas 4: Recursos Humanos** 12. Disciplina Insuficiente del personal (p.ej. para apagar PC, limpiar escritorios) 13. Insuficiente motivación / disciplina del personal 14. Dejar PC's portátiles y medios de almacenamiento masivo (diskettes, etc.) sobre el escritorio luego del horario laboral 15. Insuficiente conciencia del personal respecto a medidas de seguridad **Categoría de causas 5: Procesamiento** 16. No adherencia a procedimientos / guías 17. demasiada gente involucrada en operaciones altamente sensibles 18. Precauciones Insuficientes / inadecuadas para prevenir fugas de información confidencial (en soporte físico o magnético) a personas no autorizadas dentro y fuera de la entidad 19. Ausencia de reporte a la gerencia de línea de posibles rupturas de seguridad informática 20. Procesos de control inefectivos **Categoría de causas 6: Disrupción externa** 21.

Anexo II: Ejemplo de *Workshop* para la identificación de RO

1. Registro de los participantes

Participantes	**Área**	**Reunión inicial**	**Entrevistas previas**	**Reunión de validación**	***Workshop***
		Fecha	Fecha	Fecha	Fecha
Nombres					
.....					

2. Priorización de los riesgos (A,B,C, ...)

	Riesgos evaluados durante la realización del workshop (ordenados según prioridad)	**Evaluación de la exposición al riesgo**	**Tendencia**
F	*Violación de los sistemas de seguridad*	*Moderada. .....*	↑
A			
B			
...			

3. Análisis del riesgo (por ejemplo el riesgo A)

Riesgo A	**Causas potenciales**
Describa el riesgo acá **Definición:** El riesgo es que el área ..... (riesgo) y puede resultar en: • Reclamos financieros y pérdidas. • Reelaboración manual. • Quejas de clientes. • Pérdida de clientes. • Daño a la reputación del banco**.**	1. *Compartir en forma insuficiente experiencias / conocimientos* 2. *Tiempo Insuficiente para completar la tarea* 3. *Falta de RRHH* 4. *Sistemas inadecuados / no disponibles* 5. *Entrenamiento insuficiente.* 6.

4. Como resultado del *"workshop"* se define:

- **Controles adecuados a implementar.**
- **Impacto / Probabilidad del riesgo.**
- **Planes de acción para su mitigación.**
- **Dueño del riesgo.**
- **Posición a tomar respecto al riesgo**

(p.ej. la exposición respecto a este riesgo no es aceptable y requiere desarrollar un plan de acción para su reducción).

Anexo III: Plantilla para evaluar un riesgo operacional y sus controles[42]

Riesgo numero:	**26**	**Operacional**

Evento riesgoso:	**Falla de una función de procesamiento clave**
Descripción del riesgo:	Pérdida financiera, ineficiencia, daño a la imagen corporativa / pérdida reputacional debida a fallas en funciones de procesamiento claves en los niveles de servicio requeridos

Evaluación estimada inherente:	**C**	**3**

La escala y magnitud de los procesos implican que el impacto es alto.

El desarrollo durante un período de tiempo de varios de esto procesos, sugieren que la ocurrencia de fallas en los próximos 12 meses es poco probable.

Componentes del riesgo

Fallas en el sistema de suscripción
Fallas en los sistemas contables y sus vinculos con el procesamiento contable general
Fallas en los procesos de planificación
Fallas para adaptar los procesos a los requerimientos generados por un entorno de negocios cambiante
Fallas para modernizar procesos críticos
Procesos de reportes ineficiente
Mala administración de los procesos de negocio
Administración no-satisfactoria de fondos en custodia

Control	Responsable	Descripción del control	Tipo	Frecuencia	Diseño	Performance	Nuevo
Internal control failure reporting (R26)	N.A.	Reporte mensual al ejecutivo de operaciones sobre fallas observadas en los controles	Detección	Mensual	Ambar	Amarillo	No
Revisiones de auditoría interna (R26)	N.A.	Función independiente que reporta al comité de auditoria y revisa la conveniencia y efectividad de los sistemas y controles internos de la organización a través de un *approach* basado en riesgos.	Detección / Prevención	Según requerimiento	Verde	Verde	No
Reporte de notificación mensual (R26)	N.A.	Sistema de reporte mensual de fallas de control internas	Detección	Mensual	Amarillo	Amarillo	No
Manual de Compliance efectivo (R26)	N.A.						
Revisión interna de Compliance (R26)	N.A.						

Evaluación estimada residual:	**C**	**2**

El impacto de las falla no puede realmente ser controlado.
Los controles establecidos reducen aún más la ya baja probabilid de ocurrencia.
El Directorio no ha definido los recursos necesarios para desarrollar la acción descripta más abajo; en consecuencia la evaluación del riesgo no se reducirá en el corto plazo.

Acción	Responsable	Descripción de la acción	Fecha	Estatus
Administración del RO por la entidad	N.A.	Desarrollar la gestión del RO dentro de la entidad	31/12/2005	Iniciado
Marco de gestión del riesgo	N.A.	Desarrollo continuo del marco de control y gestión de los riesgos por parte de la	31/12/2005	Iniciado

Evaluación estimada objetivo:	**B**	**1**

El objetivo es reducir el impacto y probabilidad, pero ello require un marco de medición / monitoreo efectivo. El objetivo del proyecto es establecer un marco de monitoreo eficaz a partir del cual pueda reducirse el riesgo.

[42] Lloyds (2007): "Self-assesment tool 6.7"

Anexo IV: Proceso de asignación[43] (extracto)

Marco de gestión de KRI: Asignación de funciones de negocios a categorías de riesgos			Originación					Ejecución		Operaciones y procesamiento							.....
			Desarrollo de productos y servicios	Gestión de las relaciones comerciales	Aprobación y revisión de créditos	Modelos y metodologías	Investigación	Servicios de consultoría	Determinación de precios	Captura comisiones de transacciones	Colateral / Margenes / Neteo	Administración de transacciones	Contabilidad de transacciones	Valuación interna	Custodia de valores	Administración de caja	.....
Riesgo de procesos	Gestión de ejecución, entrega y procesamiento	Errores de procesamiento manual	3	4	4	3	2	3	5	9	8	9	6	5	7	6	.....
		Gestión de datos	6	7	9	9	6	6	8	8	8	7	4	7	6	7	.....
		Reportes y publicidad	3	8	3	3	2	2	2	3	3	3	2	2	3	3	.....
	Disrupción de negocios	Infraestructura y sistemas	3	4	4	3	2	3	8	8	6	7	3	4	4	7	.....
Riesgos conductuales	Clientes, productos y practicas de negocio	Fiduciario	5	5	3	2	3	8	5	4	5	4	2	1	5	2	.....
		Prácticas impropias	6	9	9	2	5	9	8	7	8	7	6	6	7	6	.....
	Fraude interno y robos	Actividad de mercado no autorizadas	0	0	0	0	0	0	7	8	0	6	0	0	0	0	.....
		Fraude interno y robo	5	9	9	5	5	3	7	8	7	5	4	5	6	4	.....
	Prácticas de empleo y seguridad en el ambiente laboral	Diverisdad y discriminación	0	0	0	0	0	0	0	0	0	0	0	0	0	0	.....
		Relaciones con empleados	0	0	0	0	0	0	0	0	0	0	0	0	0	0	.....
		Seguridad en el ambiente laboral	1	3	2	1	2	2	2	2	2	2	2	1	2	2	.....
Riesgos externos	Daños a activos físicos	Desastres naturales y accidentes	1	3	2	2	1	1	2	3	4	3	2	2	6	2	.....
		Daños intencionales	1	3	2	2	1	2	2	3	3	3	2	2	4	2	.....
	Fraude externo	Fraude externo y robo	2	4	2	2	2	2	3	2	2	2	2	2	2	2	.....
		Disrupciones intencionales	2	9	9	2	4	4	2	3	9	3	2	2	5	2	.....

[43] KRIex.

Anexo V: Ejemplos de KRI's vinculados al riesgo operacional por categoría de riesgo

Personas
Tasa de rotación del personal
% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses
Costos reales de entrenamiento vs. los proyectados
Cantidad de horas extras pagadas.
Ausentismo de personal / tasa de enfermedades.
% de evaluación de personal por debajo de "satisfactorio".
% de personal permanente / temporario.
Ratio de número días de personal enfermo sobre número total de días

Procesos
Número y naturaleza de superación de límites establecidos.
Cambio porcentual en el número de transacciones.
Número de observaciones / cargos debidos a incumplimientos regulatorios.
Volumen de transacciones a procesar proyectadas sobre capacidad disponible.
Número de cuentas no conciliadas.

Sistemas
Número y tipo de violaciones a seguridad.
Número de incidentes con virus informáticos.
Tiempo de sistema caído.
Porcentaje de disponibilidad de servidores.
Número de cambios de sistema.
Número y severidad de incidentes con sistemas.

Fraudes externos
Número de fraudes de origen externo exitosos.
Número de ataques informáticos.

Fraudes internos
Cantidad de eventos de alarma de robo detectados por el personal de seguridad.
Cantidad de violaciones a la confidencialidad de los clientes.

Prácticas de negocios, productos y clientes
Discrepancias en el número de confirmaciones de operaciones
Número de quejas de los clientes.
Variabilidad de ingresos por producto.
Cuota de mercado por producto.
Número / porcentaje de cuentas de clientes con documentación incompleta.
Número de nuevos productos.

Anexo VI: Ejemplo de cuestionario para la elaboración de una tarjeta de puntuación[44]

Cuestionario sobre fraude Interno (muestra)

Objetivos de control: Deberían existir medidas de seguridad física para prevenir la destrucción / robo de activos (p.ej. instrumentos negociables, PCs u otro equipamiento, documentos valiosos, información de clientes / propia, etc.), como resultado de acceso inapropiado por individuos no autorizados.

Mejores Practicas: Estas deberían restringir y monitorear el acceso a las instalaciones y áreas estratégicas (p.ej. centros de almacenamiento de datos, workstations, cajas de seguridad, áreas de almacenamiento de información sobre clientes, etc.).

Incluyen:

• Mecanismos de identificación sofisticados (p.ej. identificadores biométricos, tarjetas inteligentes, etc.).

• Control de accesos generales (p.ej. tarjetas de seguridad, cuartos de vigilancia con monitores de video, cámaras, claves de seguridad, tarjetas de identificación, etc.) como un segundo nivel de restricción.

• El otorgamiento de acceso, los cambios y los reportes de violación a la seguridad deberían ser formalmente aprobados y controlados por la gerencia.

Preguntas de mitigación

Para su línea de negocio como logra cumplir con los objetivos arriba mencionados para asegurar que existen las adecuadas medidas de seguridad?

	Valor	Pond.	Score
• Las medidas de seguridad física para restringir el acceso a las instalaciones y áreas sensibles incluyen todos los atributos arriba mencionados. El proceso es sujeto a una revisión independiente en base anual y existe un proceso formal de monitoreo con los correspondientes planes de acción.	1	0,15	0,15
• Las medidas de seguridad física para restringir el acceso a las instalaciones y áreas sensibles incluyen algunos de los atributos mencionados. La gerencia aprueba formalmente y controla la mayoría de los accesos otorgados. Los cambios y los reportes de violación a la seguridad son formalmente aprobados y controlados por la gerencia en base diaria. El proceso es sujeto a una revisión independiente en base anual y existe un proceso formal de monitoreo con los correspondientes planes de acción.	2	0,15	
• Existen sofisticados mecanismos de identificación y de controles de acceso generales que restringen el acceso a las instalaciones y áreas sensibles. La gerencia aprueba formalmente y controla la mayoría de los accesos otorgados. Los cambios y los reportes de violación a la seguridad son formalmente aprobados y controlados por la gerencia sobre una base diaria. El proceso es sujeto a una revisión independiente en base anual y existe un proceso informal de monitoreo con los correspondientes planes de acción.	3	0,15	
• Todos los accesos a las instalaciones y áreas sensibles son restringidos a través del uso de algún control de accesos general. La gerencia aprueba y controla informalmente alguno de los accesos otorgados. Los cambios y los reportes de violación a la seguridad son formalmente aprobados y controlados por la gerencia sobre una base menor a la diaria. El proceso es sujeto a una revisión independiente en base mayor a la anual y existe un proceso informal de monitoreo con los correspondientes planes de acción.	5	0,15	
• Todos los accesos a las instalaciones y áreas sensibles son restringidos a través del uso de algún control de accesos general. La gerencia aprueba y controla informalmente alguno de los accesos otorgados. El proceso es sujeto a revisión sobre una base ad-hoc.	8	0,15	

[44] SWG (2003).

Anexo VII: Ejemplo de tarjeta de puntaje (*Scorecard*) para riesgo operacional[45]

Categoría de riesgo	**Finanzas corportivas**			**Negociación y ventas**			**Banca minorista**			**Banca comercial**			**Pagos y liquidación**			**Servicios de agencia y custodia**			**Administración de activos**			**Administración minorista**		
Generador de riesgo	KRI	Unid.	Pond.	KRI	Unid.	Pond.	KRI	Unid.	Pond.	KRI	Unid.	Pond.	KRI	Unid.	Pond.	KRI	Unid.	Pond.	KRI	Unid.	Pond.	KRI	Unid.	Pond.
Actividad																								
Complejidad																								
Personas																								
Procesos																								
Sistemas																								
Indicador agregado																								
Pérdidas realizadas																								
Enviado a pérdida Pérdida de recursos Restituciones Responsabilidad legal Regulación e impuestos Pérdida / Daños a activos																								
Pérdidas totales																								

Acciones correctivas																								
Nuevos procedimientos Sistemas de información RRHH y capacitación	N.		Pond.	N.		Pond.	N.		Pond.	N.		Pond.	N.		Pond.	N.		Pond.	N.		Pond.	N.		Pond.
Total (ponderado)																								

Indicador agregado (luego de acciones correctivas)						

Notas:

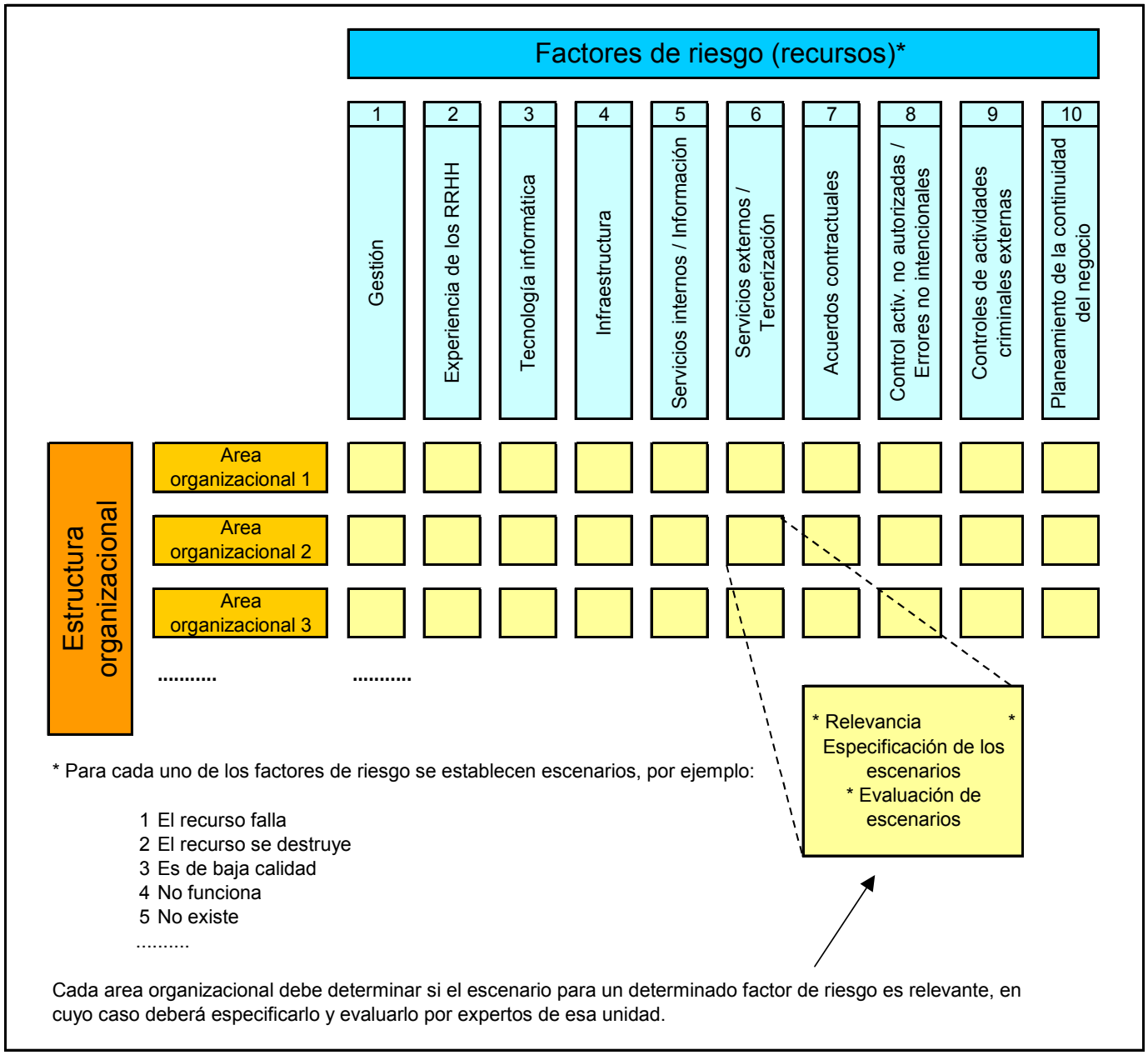
Unid. representa la unidad de medida ($, cantidad, Si / No, etc.)

Pond. representa la ponderación asignada al indicador.

N. Corresponde a la ennumeración de los procedimientos.

[45] Scandizzo (2003).

Anexo VIII: Modelo SBA usado por el Dresdner Bank[46]



[46] SBA (2003).