UNIVERSIDAD NACIONAL DE CÓRDOBA

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE GRADUADOS EN CIENCIAS ECONÓMICAS

MAESTRÍA EN DIRECCIÓN DE NEGOCIOS

TRABAJO FINAL DE APLICACIÓN

"Integración de riesgos tecnológicos y operacionales"

Autor: Cra. Florencia Torcivia

Tutor: MBA José Luis Reynero

Córdoba

2016


Integración de riesgos tecnológicos y operacionales” by Florencia Torcivia is licensed under a Creative Commons Reconocimiento-CompartirIgual 4.0 Internacional License.

Agradecimientos

A la Escuela de Graduados, por su invitación para iniciar la Maestría en Dirección de Empresas que a la vez me abrió las puertas para realizar un intercambio estudiantil con ESSEC de Francia, una de las experiencias más fantásticas de mi vida.

A mi tutor, José Luis Reynero, por ser de guía durante este proceso de aprendizaje.

A mis compañeros de la maestría por las amistades, las experiencias y los conocimientos compartidos.

A mi círculo íntimo de amistades, por acompañarme durante una etapa más de mi crecimiento.

A mi familia, en especial a Adriana y Ángel por su apoyo incondicional y por inculcarme siempre los valores de la honestidad, esfuerzo y dedicación.

A Nicolás por la paciencia.

I. Índice de contenido

II. Índice de tablas

II. Índice de ilustraciones

I. PRESENTACIÓN DEL PROYECTO

A. RESUMEN

Dado el paradigma de la globalización, el contagio de las crisis del sector financiero al real de la economía, los actores financieros deben comprometerse con una administración de riesgos eficiente, aprobada por los organismos de contralor relevantes.

Como trabajo final de aplicación, se plantea la oportunidad de mejorar la gestión de riesgos operacionales, integrándolos a los tecnológicos, buscando agregar valor más allá del mero cumplimiento normativo.

La propuesta final incluye no solo la integración de riesgos, sino la mejora integral del proceso de su gestión, desarrollando las recomendaciones más significativas para la actualización del mismo.

B. PROBLEMA

1. Contexto

El presente trabajo final tiene como marco organizacional a una entidad financiera de la provincia de Córdoba. La misma está conformada por una casa matriz y 144 sucursales. La estructura organizacional se puede resumir a través del siguiente esquema: un directorio, una gerencia general, seis subgerencias generales y diversas gerencias de primera dependientes de la gerencia general. En vista de otorgarles soluciones integrales a las principales problemáticas del banco, con frecuencia predefinida se ponen en funcionamientos los comités interdisciplinarios, teniendo así una mayor flexibilidad en la organización.

El sector financiero en el que se encuentra inmerso el Banco S.A., presenta un comportamiento dinámico influido principalmente por las nuevas fronteras de posibilidades comerciales gracias a la innovación tecnológica y al mismo tiempo por la implementación de nuevas regulaciones.

La historia reciente muestra que desde la crisis financiera internacional de 2008, el sistema financiero nacional e internacional ha experimentado presiones crecientes para

instaurar mecanismos de control interno y reducir el impacto de los riesgos financieros y operativos (Bank for International Settlements, 2010). Este fue el marco en el que el Comité de Supervisión Bancaria de Basilea, emitió el acuerdo denominado Basilea III (Bank for International Settlements, 2010), con la finalidad de mejorar la capacidad del sistema bancario de absorber las pérdidas en situaciones de estrés financiero o económico, reduciendo así el contagio desde el sector financiero al real.

Previo al acuerdo de Basilea III, el mismo comité ya se había pronunciado respecto de las normas de supervisión bancaria, resumidas en los documentos Basilea I y Basilea II.

Una de las mejores prácticas de Basilea I (Bank for International Settlements, 2001)se puede resumir en la implementación de un sistema de medida de capital de bancos y otras entidades financieras. A partir de 1992, este capital ascendía al 8% del total de los activos riesgosos de su propiedad. Al mismo tiempo se establecieron lineamientos para el control y regulación marcados como objetivos del acuerdo. Las acciones concretas se concentran en torno de:

- Gobierno corporativo
- Manejo del riesgo de crédito
- Manejo del riesgo operativo
- Definición del marco de los sistemas de control interno

En el acuerdo de Basilea II (Bank for International Settlemet, 2006), la complejidad del sistema financiero internacional se evidenció en las mayores exigencias que se impusieron. Se establecieron tres pilares, que a forma de resumen se exponen:

- Requerimiento mínimo de capital: con un objetivo de un adecuado manejo de riesgos por parte de los bancos, para lo cual se fomenta el desarrollo de modelos de gestión de riesgos propietarios.
- Proceso de examen supervisor: para aumentar el control por parte de los Bancos Centrales y al mismo tiempo hacer más profesional la administración bancaria.

- Disciplina de mercado: busca generar información de gestión en forma uniforme asegurando su corrección y transparencia.

Las regulaciones internacionales, han sido adoptadas por los organismos de contralor de cada país, siendo en Argentina el Banco Central de la República Argentina (BCRA) el responsable por emitir las comunicaciones a fines de alinear los objetivos de política financiera con las buenas prácticas de Basilea. Las presiones para una mayor fiscalización sobre las entidades del sector si bien representan mejoras en los sistemas, tienen como contracara un aumento en los costos.

En este contexto, el Banco S.A. tiene la responsabilidad de cumplir con las normativas nuevas en los otorgados plazos. Particularmente, se debe dar respuesta a la integración en el relevamiento y administración de los riesgos operacionales y tecnológicos presentados formalmente en los acuerdos de Basilea. Al mismo tiempo, como dato a destacar, el Banco S.A. transita un período de normalización de los principales ratios económicos, financieros y de gestión a niveles aceptables por parte del BCRA. Esta premisa, se puede traducir como una limitante en los esfuerzos económicos a afrontar para el cumplimiento normativo.

Los actores principales dentro del proyecto de integración de riesgos son la Gerencia de Protección de Activos de la Información y la Gerencia de Gestión Integral de Riesgo.

2. Definición de la oportunidad

El marco temporal y espacial descripto en el punto anterior permite vislumbrar una oportunidad de mejora continua y de eficiencia de recursos. Puntualmente se plantea la oportunidad de dar cumplimiento normativo referido a la integración de riesgos operacionales y tecnológicos agregando valor al banco a través de una administración integral y eficiente de los riesgos. De esta manera, la base de riesgos utilizada para el cálculo de capital económico (capital mínimo) va a tener un mayor grado de desagregación permitiendo más posibilidades de gestión de riesgos (alocación de capital económico de acuerdo a los riesgos de los productos ofrecidos por el banco).

3. Objetivos del trabajo

El objetivo principal de este trabajo final de aplicación es:

- Mejorar el sistema de gestión de riesgos operacionales que incluya los riesgos tecnológicos. La aplicación final se mostrará sobre el producto de Plazo Fijo. De esta manera, se busca a partir del marco teórico a elaborar sobre la temática, desarrollar un proceso secuencial e integral en donde los actores intervinientes agreguen valor a la organización mediante la identificación, registración, medición y seguimiento de los riesgos señalados.

Como objetivos secundarios se plantean:

- Definir mapas de procesos y sistemas homogéneos. Este objetivo permitirá visualizar y comprender los procesos de negocio y de soporte en los cuales se identifican los riesgos y amenazas.

- Estandarizar la identificación y evaluación de riesgos para mejorar la calidad de los outputs, con principal reflejo en la matriz de riesgo para capital económico.

Desde una perspectiva personal, el presente trabajo se elabora con la finalidad de culminar la Maestría en Dirección de Empresas en la Escuela de Graduados de la Facultad de Ciencias Económicas de la Universidad Nacional de Córdoba.

4. Límites o Alcance del trabajo

Los límites de este trabajo se circunscriben a la mejora del sistema de gestión de riesgos operaciones (puntualmente sobre los subprocesos de identificación y evaluación de riesgos) que contemple además los riesgos tecnológicos, con aplicación en el proceso de negocio de plazo fijo dentro del Banco SA. Para esto, será necesario también analizar los procesos de soporte, sin embargo se hará hincapié en los subprocesos directamente relacionados a los depósitos a plazo.

Luego del trabajo de campo sobre el mencionado proceso de negocio, se analizará la factibilidad de extrapolar los conocimientos adquiridos y los sistemas desarrollados a los demás procesos de negocio y soporte que ejecuta el banco.

5. Organización del trabajo

El presente trabajo se estructura de la siguiente manera:

II. DESARROLLO DEL PROYECTO

A. MARCO TEÓRICO

El marco teórico constituye una de las secciones más importantes del trabajo de aplicación final, ya que contiene las teorías en la que se sustenta el proyecto planteado.

Se estructura en dos capítulos, estando el primero direccionado a la mejora de procesos siguiendo al autor James Harrington y el segundo a los riesgos operacionales y tecnológicos siguiendo los lineamientos del Banco Central de la República Argentina.

Capítulo 1: Mejora de Procesos

El presente trabajo se encuentra encuadrado dentro de la disciplina de Mejora de Procesos (o BPI por sus siglas en inglés Business Process Improvement), ya que supone la mejora del proceso de gestión de riesgos operacionales incluyendo también los riesgos tecnológicos. Siguiendo al autor James Harrington en su libro Business Process Improvement[1], 1991, Ed.McGraw-Hill, un proceso puede ser definido como cualquier "*actividad o grupo de actividades que utiliza recursos de entrada, agrega valor a estos y genera recursos de salida para un cliente interno o externo. Los procesos usan los recursos de una organización para generar determinados resultados"* (Harrington, 1991).

La importancia de enfocarse en los procesos radica en la posibilidad de pensar más allá de las estructuras verticalistas de las organizaciones contemporáneas. La mayoría de los procesos fluyen en forma horizontal, permitiendo tener una visión global y acabada de los esfuerzos y acciones necesarias para obtener una salida. La visualización de los procesos desde un principio hasta el final, posibilita su mejora (Dumas, 2013).

La mejora de procesos entendida como una estrategia dentro del negocio, debe tener los siguientes objetivos:

- Obtener procesos efectivos, generando los resultados esperados.
- Obtener procesos eficientes, minimizando los recursos utilizados.

[1] Business Process Improvement: Mejoramiento en los procesos en la empresa en su versión en español, Edición de 1993.

- Obtener procesos flexibles a las necesidades cambiantes del entorno.

Para darle un mayor respaldo a la gestión a través de procesos de negocios, resulta de ayuda desmentir falsas creencias en la gerencia que pueden obstaculizar con los objetivos principales de la empresa, como por ejemplo las siguientes:

a) Los procesos ineficaces no cuestan mucho dinero a la organización: los procesos ineficaces de la empresa le cuestan a las organizaciones miles de millones de dólares todos los años. Entre un 40% y un 70% de los esfuerzos de los empleados de oficina no agregan valor alguno. Eliminar los errores de los empleados y la burocracia puede reducir los costos indirectos hasta en un 50% (Harrington, 1991). Estos números son relevantes y sensibles, modificar los procesos haciéndolos eficaces tiene un impacto directo en el cuadro de resultados de la empresa, y lo que es igual de importante, un impacto directo sobre la percepción en los clientes (internos y externos).

b) Es poco lo que pueden las organizaciones ganar mediante el mejoramiento de los procesos de la empresa: el mejoramiento de los procesos de la empresa puede tener alto impacto sobre la cultura de las organizaciones (Harrington, 1991). Una vez iniciada la mejora en los procesos, se observan transformaciones desde el plano de los colaboradores (pasando de una visión individualista a una grupal) hasta Cycle-Time[2] que disminuye teniendo un impacto sobre los clientes.

c) Los procesos de la empresa no pueden controlarse: no sólo es posible sino que deben controlarse estos procesos (Harrington, 1991). Es preciso controlar y auditar los procesos de la empresa de la misma manera que los procesos de manufactura. De esta forma se obtiene una alta calidad en toda la empresa.

d) Los procesos de la empresa carecen de importancia en comparación con los procesos de producción: los clientes son 5 veces más susceptibles a alejarse de las organizaciones debido a procesos mediocres de la empresa que a causa de

2 Cycle Time: referido al tiempo entre el comienzo y el final del proceso

productos deficientes. Sin una buena interacción entre las organizaciones y los clientes, aun el mejor de los productos dejará de atraerlos (Harrington, 1991).

Al implementar la mejora de procesos de como disciplina y marco teórico, los procesos eficaces, eficientes y flexibles presentan una serie de características:

- Tienen definido un dueño responsable
- Tienen documentados las tareas y las responsabilidad
- Son medibles y tienen definidos puntos de control
- Tienen definidos los tiempos de ejecución y finalización
- Tienen documentados y formalizados los cambios en los procedimientos

La mejora de procesos de negocios, supone diversas etapas de aplicación, luego de la selección del proceso. La selección del proceso es un determinante clave para el éxito en la implementación de la estrategia. Como condición inicial debe seleccionarse un proceso sobre el cual no se tienen satisfechas las expectativas sobre el output del mismo. El enfoque total, en el cuál se desea trabajar con todos los procesos de la compañía, solo es recomendable en empresas de una envergadura limitada. El enfoque de mejora selectiva ofrece ventajas en grandes estructuras para tener el apoyo en sucesivos planes de mejora al ver los resultados en los primeros procesos seleccionados.

Las etapas a desarrollar en la mejora de proceso, son las siguientes:

I. Organización previa para el mejoramiento de los procesos

En esta instancia se tiene como principal objetivo asegurar la reforma exitosa de los procesos a través de un compromiso del equipo de trabajo y la figura de un líder que esté al frente de la mejora. Para estas acciones, se realiza un diagnóstico interno del proceso de negocio a mejorar.

Las principales actividades involucradas en esta etapa son:

a. Estudio de la estructura de la organización. La estructura organizacional puede definirse como la división de todas las actividades de una empresa que se agrupan para formar gerencias, departamentos o áreas, estableciendo autoridades, que a través de la organización y coordinación buscan alcanzar objetivos. Pueden diferenciarse dos partes: la estructura organizativa formal y la informal. La estructura organizativa formal es aquella que se basa en el conjunto de relaciones explicitadas por la dirección, son relaciones deliberadas. La estructura organizativa informal son el conjunto de relaciones que no han sido definidas explícitamente y responden básicamente a las necesidades que entran en contacto con el trabajo. Puede definirse una tercera estructura, que es la real y se basa en el conjunto de relaciones formales e informales.

   La relevancia en el estudio de la estructura radica en que la misma debe ser la adecuada para la ejecución de las actividades de todos los procesos de la organización. Al plantearse la mejora de los procesos, se debe analizar la correspondencia mencionada.

b. Diagnóstico del comportamiento y liderazgo directivo. El liderazgo en las organizaciones actuales es un aspecto de primordial importancia para el trabajo y desarrollo de los equipos y las organizaciones. No debe tener únicamente como aspecto guía la concreción de los objetivos planificados, sino también el desarrollo integral y la satisfacción laboral que aspiran a alcanzar los colaboradores, que les permita una flexibilidad para afrontar cambios en el entorno y un mejoramiento continuo de los procesos y de los resultados obtenidos.

   Un comportamiento y liderazgo directivo comprometido, facilita la planificación de mejoras y permite el cumplimiento de los plazos pactados para las mismas por el apoyo que reciben los agentes de cambios en las distintas etapas del proceso.

c. Detalle de canales de comunicación interna. La comunicación interna dentro de una empresa es una de las herramientas organizacionales más eficaces para mejorar la productividad de las mismas. En esta expresión recae la importancia de analizar los canales usados entre los colaboradores antes una mejora de procesos. Dentro de la organización existen canales de comunicación informales y formales, y estos últimos a su vez pueden ser ascendentes, descendentes o transversales. Tener conocimiento sobre los canales de comunicación permite plantear una estrategia para la implementación de las mejoras, de acuerdo a la cultura de la organización, los usos y costumbres, aumentando las probabilidades de éxito.

d. Reuniones participativas de colaboradores. A través de las reuniones de trabajo es posible entender cómo se están realizando las actividades y si se están consiguiendo los objetivos de la organización. El trabajo en equipo es fundamental para la consolidación y el éxito de un proyecto como una mejora de procesos.

   Para que las reuniones sean fructíferas se proponen distintas medidas, a saber:

   - Planificar los objetivos de la reunión (obtener información, resolver un problema, acordar una conclusión) y qué asistentes deben estar presentes.

   - Elaborar con anticipación la agenda de contenidos de la temática a exponer y entregar documentos o reportes a las personas que vayan a asistir para que estos sepan de qué se va a hablar.

   - Respetar el orden de los temas que se van a abordar y procurar que no se produzcan comentarios fuera del tema que se está debatiendo.

- Dejar registro en un documento de todas las ideas expresadas y de las conclusiones a los que se haya llegado. Esto evita que en futuras reuniones se traten los mismos temas además se puede hacer un seguimiento de todo lo tratado.

e. Selección del proceso a mejorar. Como se mencionó ut supra el proceso sobre el que se decida trabajar, debe ser aquél sobre el cual no se tienen satisfechas las expectativas sobre el output del mismo.

   Es posible identificar los indicios que señalan que los procesos no están cumpliendo sus objetivos adecuadamente. Estas señales pueden surgir tanto del exterior como del interior de la organización. Del exterior se pueden identificar:

   - Fuertes quejas de clientes
   - Costos de garantía que aumentan
   - Alta rotación de clientes fuera del benchmark de la industria
   - Disminución de participación de mercado
   - Falta de Información sobre los productos
   - Descontento de los canales de distribución por la forma de atención.

   Del interior se pueden observar los siguientes síntomas:

   - Muchos errores y consiguientes reprocesos
   - Comunicaciones deficientes
   - Alta rotación de empleados
   - Bajo compromiso de los colaboradores
   - No cumplir con todos los requerimientos
   - Conflictos entre departamentos ó áreas

II. Evaluación y entendimiento del proceso actual

Se busca tener un conocimiento acabado del proceso como se encuentra actualmente y sus interacciones con la estructura organizacional.

Las principales actividades involucradas en esta etapa son:

a. Establecer alcance y objetivos del proceso. El alcance se refiere al área cubierta por el proceso y predefine los límites dentro de los cuales se realiza el trabajo de mejora. Por otro lado, los objetivos puntualmente debe cumplir con las siguientes características:

   - Ser específicos, deben que estar claramente definidos sin ambigüedades.
   - Ser medibles, debe ser posible definir unos parámetros cuantificables que permitan evaluar el avance y la consecución de los objetivos.
   - Ser realistas, tiene que ser factible su consecución con los recursos y plazo disponibles.
   - Tener un tiempo definido, es decir una duración determinada.

b. Definir límites del proceso. Cada proceso posee unos límites claros y conocidos (el primer y último paso del mismo), comenzando con una necesidad concreta de un cliente (puede ser interno o externo), y finalizando una vez que la necesidad ha sido satisfecha. El inicio se define como la primera tarea del proceso que marca el hito de inicio temporal del mismo. El fin es la última tarea del proceso que marca el hito de finalización del mismo.

c. Obtener la visión general del proceso. Esta visión general permite la identificación de los elementos básicos del proceso (alcance, objetivos, límites, requerimientos, clientes, entradas y salidas, actividades, recursos e indicadores), teniendo en cuenta su interrelación. La visión general ayuda a

no enfocarse en detalles y a su comprensión acabada que permite analizar si la correlación entre los imputs actividades y outputs es la correcta.

d. Definir los clientes. Son los que utilizan la salida del proceso. Pueden ser internos (otra gerencia, departamento o sector dentro de la misma empresa) o externos (cliente final). La mejora de procesos implica la aplicación de métodos y prácticas pero también significa implementar una coordinación de personas e intereses para lograr un objetivo en común y poder ensamblar un proceso general, llamado a veces sistema de gestión de calidad y que tiene relación directa con la propuesta de valor a los clientes (nuevamente, internos o externos).

e. Establecer los indicadores y límites para medir la efectividad, eficiencia y adaptabilidad. "*Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre*" Lord Kelvin.

   Medir es una parte fundamental de la mejora continua, permite corregir a futuro situaciones pasadas no conformes. Sin embargo la medición por sí sola no es capaz de conseguir las mejoras deseadas. Pero sólo a través de la medición es posible identificar y cuantificar las oportunidades de mejora que pueden implementarse a través de un plan de acción. La evolución de estos mismos indicadores evidencia si la mejora adoptada está resultando o no efectiva.

   Para el establecimiento de indicadores es necesario definir:

   - Proceso, y de corresponder subproceso, al cual pertenece
   - Objetivo del indicador
   - Unidad de medida
   - Fórmula de cálculo

- Fuente de datos
- Periodicidad de cálculo
- Estándar o valor meta

Existen distintos tipos de indicadores, entre los cuales se pueden citar:

Indicadores de cumplimiento: el cumplimiento tiene que ver con la conclusión de una tarea. Estos indicadores están relacionados con las razones que indican el grado de completamiento de tareas, trabajos, proyectos.

Indicadores de eficiencia: estos indicadores de eficiencia están relacionados con las razones que indican los recursos utilizados en una tarea. Típico indicador de eficiencia es la productividad (cociente entre output e imput).

Indicadores de eficacia: miden el logro de los resultados propuestos. Muestra si se realizaron las tareas que se debían hacer, los aspectos correctos del proceso. Los indicadores de eficacia tienen su foco en el qué se debe hacer, por esto es fundamental conocer y definir los requerimientos del cliente del proceso para comparar lo que entrega el proceso contra lo que él espera. De no hacerlo, se puede estar logrando una gran eficiencia en aspectos no relevantes para el cliente.

f. Dibujar el diagrama de flujo del proceso actual. Un diagrama de flujo, es una herramienta de gran valor para entender el funcionamiento interno y las relaciones entre los procesos de la empresa. La misma permite construir una imagen del proceso etapa por etapa para su análisis, discusión o con propósitos de comunicación al mismo tiempo que permite definir, estandarizar o encontrar áreas de un proceso susceptibles de ser mejoradas.

g. Reunir los datos de costo, tiempo y valor. La mejora de procesos debe resultar en una mayor eficacia, eficiencia y adaptabilidad de los mismos. El tiempo es un recurso consumido durante la ejecución de las tareas del proceso, y en las

organizaciones modernas el tiempo empleado en las mismas tiene su contracara de erogación monetaria, costo. Al tener los datos de los costos, tiempo y el valor que agrega el proceso actual, se podrá analizar los resultados de la mejora y si los mismos están de acuerdo a las expectativas planteadas.

h. Documentar el proceso. La finalidad de la documentación es mantener controles internos que van a permitir una mejor gestión y desempeño por parte del colaboradores en cada área. Los documentos deben tener su codificación y deben estar disponibles para toda la organización (con limitaciones de tratarse de procesos con información confidencial o secreta).

III. Modificación del proceso

En esta instancia se trabaja sobre el proceso actual para transformarlo en el deseado, mejorando la eficiencia, efectividad y adaptabilidad del proceso de la empresa.

Las principales actividades involucradas en esta etapa son:

a. Identificar oportunidades para la intervención, como por ejemplo:

   - Errores y retrabajos
   - Demoras prolongadas
   - Mala calidad

b. Eliminar la burocracia. Muchas de las tareas y actividades que forman la burocracia poco o nada tienen que ver con la satisfacción del cliente, sino más bien con necesidades que la propia Organización ha creado, con lo cuál pierden su razón de ser.

c. Eliminar actividades que no agreguen valor. El cliente del proceso busca una satisfacción de una necesidad con el output del proceso. En este output, la percepción del cliente identifica solo las actividades que son funcionales a su

necesidad, por lo que toda actividad que no genere valor (para un cliente directo o indirecto) debe eliminarse del proceso.

d. Reducir el tiempo de proceso. Se puede definir como flow-time al tiempo empleado por una orden tipo en un proceso. Mientras que el cycle-time es el tiempo promedio entre unidades producidas (la razón entre uno y la capacidad del proceso). Estas medidas de los procesos deben ser reducidas en la mejora del proceso o mantenerlas si la calidad del output aumenta. La reducción de tiempos, conlleva a una disminución de costos.

e. Eliminar los errores del proceso. El diagnóstico del proceso, permite identificar en qué actividades se presentan errores. En la racionalización del proceso estos errores deben ser corregidos, y teniendo una mirada más amplia, en etapas subsiguientes, con el proceso ya mejorado es posible que se den errores. Estos puntos críticos exigen el desarrollo de un sistema de control interno, para la mitigación de los errores y los impactos que puedan tener los mismos en el output del proceso.

f. Estandarización. El fin de esta actividad es que los procesos sean ejecutados de manera previamente establecida, es decir utilizando un modo o método prefijado, aceptado y normalmente seguido para realizar determinado tipo de actividades o funciones. Un estándar es aquello que debe ser seguido en caso de recurrir a algunos tipos de acción. Dentro de la mejora de procesos, la estandarización contribuye a reducir tiempos de respuestas ante situaciones reiterativas, identificar excepciones que deben ser tratadas como tal, y en definitiva a una gestión más eficiente de los procesos.

   La estandarización juega un rol tan importante en la economía, negocios y en los consumidores, que desde 1946 la Organización Internacional de Estandarización (ISO) ha emitido más de 21 mil normas de estandarización. Estos estándares internacionales son herramientas estratégicas que permiten a las organizaciones responder a los cambios permanentes de contexto.

Las normas ISO ayudan a las empresas de las siguientes maneras (International Organization for Standardization, s.f.):

- Reducción de Costos a través de mejora de sistemas y procesos
- Aumento en la satisfacción de clientes a través de la mejora en la calidad y seguridad de los procesos
- Acceso a nuevos mercados, a través del aseguramiento de compatibilidad de productos y servicios ofrecidos
- Reducción del impacto ambiental.

g. Documentar el proceso. Si el proceso previo a la mejora no se encontraba documentado, es menester que se lo documente. Si estaba documentado, las modificaciones deben quedar registradas para mantener el historial y trazabilidad de las distintas versiones que se generan. También es recomendable documentar el proceso de mejora, guardar el registro del diagnóstico que sirva como base para comparar los avances logrados con la mejora del proceso.

h. Otorgar capacitación y entrenamiento a los colaboradores. "*Si cree usted que la educación es cara, pruebe con la ignorancia*." Derek Curtis Bok, ex-Presidente de la Universidad de Harvard.

   La capacitación en el proceso de mejora cumple un rol fundamental, y debe ser vista como una inversión del mismo proceso. La capacidad y la capacitación de los colaboradores son los factores que diferencian a las organizaciones e influencian su capacidad de supervivencia. De poco sirve mejorar los procesos, si en la práctica quienes lo ejecutan no están formados para advertir los resultados de la mejora e identificar nuevas oportunidades de acción.

   En este punto es importante destacar que la gestión del conocimiento debe garantizar que ante una rotación de los recursos humanos, el conocimiento no

se escape de la organización, sino que quede disponible para el aprendizaje de futuros colaboradores.

i. Estudiar y aplicar herramientas de automatización. La tecnología es un aliado a la hora de planificar, desarrollar e implementar la mejora de proceso, ya que permite la automatización disminuyendo el riesgo de errores en las tareas manuales. Sin embargo, para una correcta implementación de estas tecnologías es fundamental el estudio de las mismas, antes de adquirirlas o desarrollarlas, para asegurarse que la inversión en estas sea redituable por los ahorros en tiempo y aumento en ratios de eficiencia y eficacia.

IV. Mediciones y controles

En esta etapa se debe implementar un sistema de control interno para el monitoreo del proceso y permitir la mejora continua del mismo.

Las principales actividades involucradas en esta etapa son:

a. Identificar los puntos en el proceso donde los errores pueden ocurrir y explicar cómo se pueden evitar. Esta actividad permite ahorrar tiempo, mitigar la frecuencia de ocurrencia de los errores y su impacto en resultados.

b. Crear herramientas para asistir a las personas que deben llevar adelante el proceso. Las herramientas pueden ser formularios que guíen las actividades a desarrollar, tableros de indicadores que concentren información clave para detectar desvíos.

c. Desarrollar métricas para conocer cómo está funcionando el proceso y si está funcionando de acuerdo a lo planeado.

V. Implementación de la mejora

Como instancia final se pone en marcha la mejora a través de la ejecución del proceso por parte de los usuarios

Las principales actividades involucradas en esta etapa son:

a. Presentación de la mejora a nivel departamental/gerencia de acuerdo a la estructura de la organización. Se debe tener en cuenta siempre los canales de comunicación que se utilizarán de acuerdo a los destinatarios de la presentación.

b. Capacitación de los usuarios.

c. Implementar el nuevo proceso mejorado

Gráficamente, las etapas de la mejora de proceso pueden representarse con el siguiente esquema:

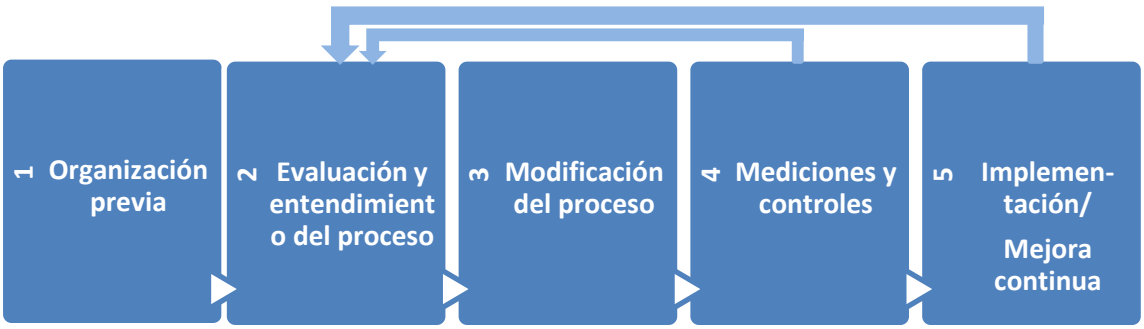


Ilustración 1 - Las cinco etapas de BPI. Fuente: Harrington, J. (1991). Business Process Improvement. McGraw Hill

Capítulo 2: Riesgo operacional - Riesgo tecnológico

Es necesario, para comprender el alcance del presente trabajo de aplicación final, acercar un marco teórico específico en materia de riesgo operacional y tecnológico. En tal sentido, el BCRA ha establecido a través de numerosas normas, los lineamientos para la gestión de riesgos en las entidades bancarias (BCRA, 2013). En estos lineamientos, se hace obligatoria la existencia de un proceso integral para la gestión de riesgos, en donde se involucre la alta gerencia para identificar, evaluar, controlar, mitigar y reportar todos

los riesgos significativos. La gestión y el esfuerzo que demande debe estar acorde al tamaño y al peso relativo de la entidad, teniendo en cuenta también la diversidad de operaciones y su complejidad. Por todo esto se concluye que el proceso integral para la gestión de riesgos deberá ser adecuado, comprobado, documentado y revisado periódicamente en función de los cambios que se produzcan en el perfil de riesgo de la entidad y en el mercado.

La existencia de riesgos genera la obligación por parte de las entidades a constituir un capital económico. El mismo se requiere para cubrir, las pérdidas inesperadas originadas por los riesgos crediticio, operacional y de mercado, y también las que de otros riesgos a los que puede estar expuesta la entidad financiera.

Como se mencionó anteriormente, uno de los riesgos a los cuales se encuentran expuestas las entidades es el riesgo operacional. El mismo puede ser definido como el riesgo de pérdidas motivadas por de la falta de adecuación o fallas en los procesos internos, de la actuación del personal o de los sistemas o bien aquellas que sean producto de eventos externos. Este concepto incluye al riesgo legal, y excluye al riesgo reputacional y estratégico.

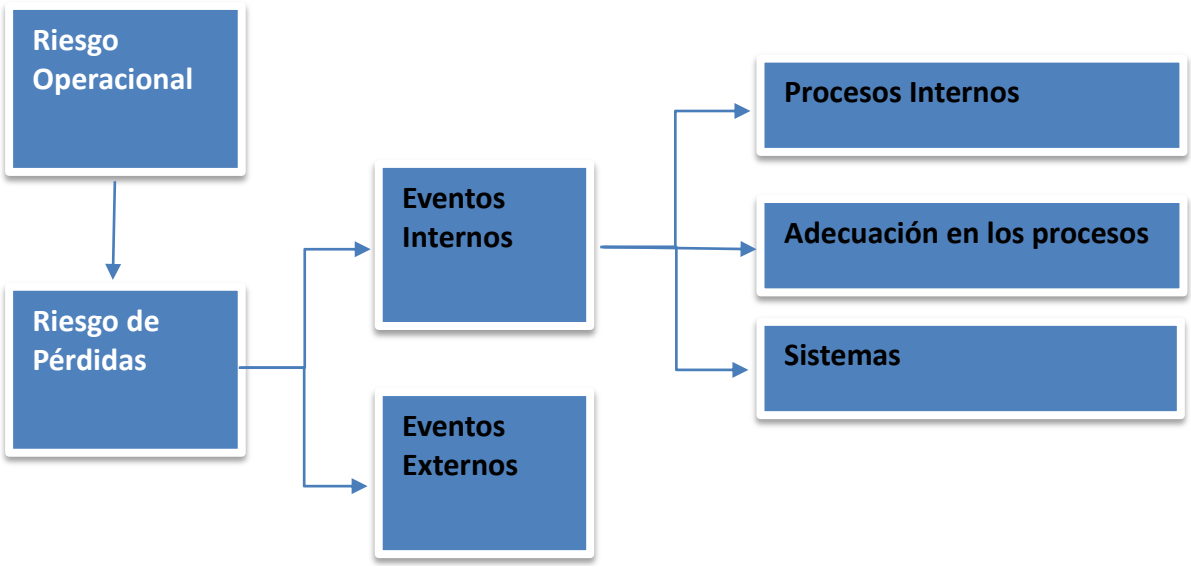


Ilustración 2 - Concepto de RO. Fuente: elaboración propia.

El riesgo operacional, debe ser gestionado a través de un proceso con las siguientes etapas: la identificación, evaluación, seguimiento, control, mitigación y reporte.

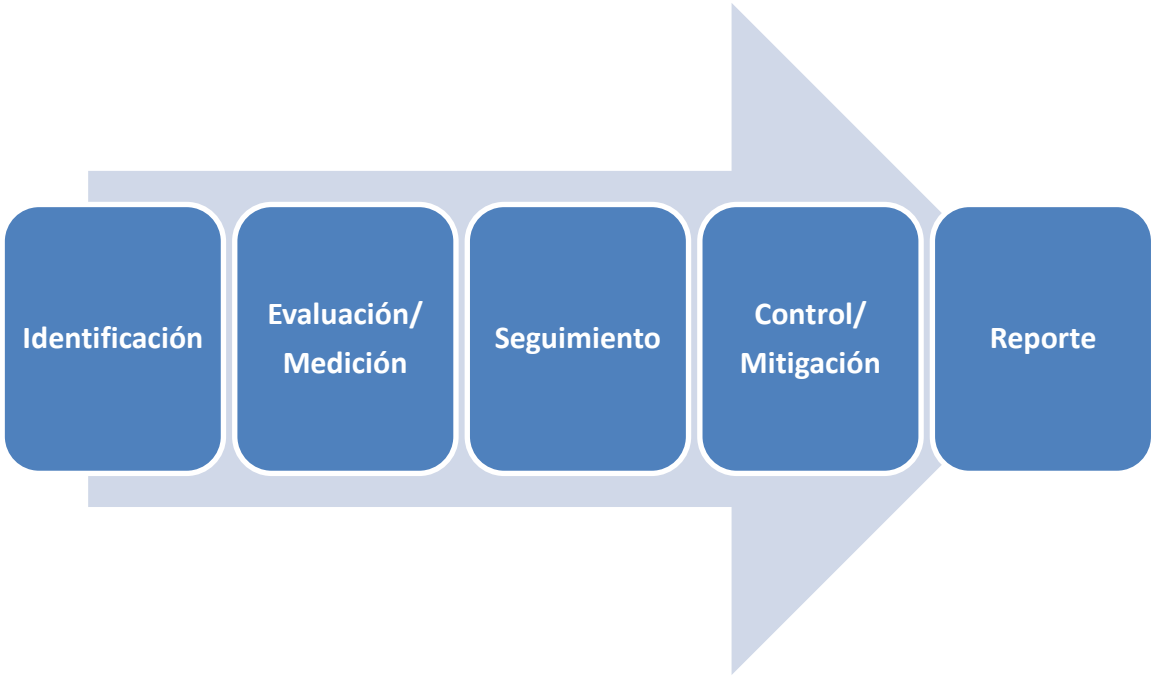


Ilustración 3 - Sistema de gestión de RO. Fuente: elaboración propia.

Para la identificación del riesgo pertinente, se deben tener en cuenta factores internos (como por ejemplo la estructura de la entidad financiera y la naturaleza de sus actividades) y externos (incluyendo cambios en el sector y avances tecnológicos), con la capacidad de tener un impacto en los procesos e influir negativamente en las proyecciones realizadas conforme a las estrategias de negocios predefinidas. Las entidades financieras utilizarán datos internos, en cuál pueda registrarse y consignarse en forma sistemática la frecuencia, severidad, categorías y otra información importante de los eventos de pérdida por riesgo operacional. La finalidad de tener un seguimiento a través de la registración de esos eventos es disminuir la frecuencia y el impacto de dichos incidentes, también puede plantearse como objetivo mejorar la calidad de los servicios y de los productos. Para aumentar el éxito en el proceso de recolección de datos se deberá desarrollar una política de incentivos que ayude a su registración, promoviendo una cultura organizacional para el reporte de tales datos y de controles que contribuyan a la verificación de su consistencia e integridad.

Estos eventos registrados deben ser clasificados, según las categorías que el BCRA explicita (BCRA, 2009):

1. Fraude interno: información falsa sobre posiciones -propias o de clientes-, robos por parte de empleados, utilización de información confidencial de la entidad financiera en beneficio del empleado, etc.

2. Fraude externo: robo, falsificación, daños por intromisión en los sistemas informáticos, etc.

3. Relaciones laborales y seguridad en el puesto de trabajo: reclamos de indemnizaciones por parte de los empleados, infracciones a las normas laborales de seguridad, de higiene, de discriminación, responsabilidades generales, etc.

4. Prácticas con los clientes, productos y negocios: abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas de la entidad financiera, lavado de dinero, venta de productos no autorizados, etc.

5. Daños a activos físicos derivados de: actos de terrorismo y vandalismo, terremotos, incendios, inundaciones, etc.

6. Alteraciones en la actividad y fallas tecnológicas: fallas del "hardware" o del "software", problemas en las telecomunicaciones, interrupción en la prestación de servicios públicos, etc.

7. Ejecución, gestión y cumplimiento del plazo de los procesos: errores en la introducción de datos, fallas en la administración de garantías, documentación jurídica incompleta, concesión de acceso no autorizado a las cuentas de los clientes, litigios con proveedores.

Además de las clasificaciones propuestas por el organismo de contralor que son útiles para analizar la información de riesgo, existen ciertas herramientas que las entidades deben utilizar para identificar y evaluar sus riesgos operacionales entre las cuales se destacan:

- Autoevaluación del riesgo operacional: a través de un proceso interno utilizando listas de control o de grupos de trabajo se identifican fortalezas y debilidades del entorno de riesgo operacional;

- Mapeo de riesgos: una vez identificados los riesgos, se los puede agrupar de acuerdo a las líneas de negocios, funciones organizativas, procesos y subprocesos;

- Indicadores de riesgo: se refieren a parámetros definidos y medidos con una periodicidad preestablecida por las entidades financieras. Estos indicadores deben ser útiles para reflejar las fuentes potenciales del riesgo operacional, tales como, una expansión acelerada, el lanzamiento de nuevos productos, la rotación del personal, interrupciones en las operaciones o en los sistemas, etc. Se pueden mencionar como ejemplo de indicadores el número de operaciones fallidas o con errores, las tasas de rotación del personal y la frecuencia y/o gravedad de los errores-

Las entidades financieras deben contar con un proceso de seguimiento eficaz de forma tal que sea posible una detección y corrección a tiempo de las posibles deficiencias que se produzcan en sus políticas, procesos y procedimientos de gestión del riesgo operacional. Este proceso debe insertarse como uno más dentro de las actividades habituales de la entidad financiera. Además del seguimiento de los eventos de pérdidas, las entidades deben monitorear el comportamiento de los indicadores para ir evaluándolos y adaptándolos de acuerdo a la naturaleza de los eventos de pérdida producidos. La unidad organizativa responsable encargada de la gestión del riesgo operacional tiene la obligación de emitir informes específicos sobre la misma a la alta gerencia. Como contenido de dichos entregables, se puede mencionar a los resultados del seguimiento realizado, las pertinentes propuestas de corrección en los procesos y procedimientos, avances de la gestión entre otros. La finalidad de estos informes también debe incluir poner en conocimiento a los niveles gerenciales correspondientes y las áreas de la entidad financiera que pudieran verse afectadas, a fin de que adopten esas medidas correctivas para asegurar una gestión eficaz del riesgo operacional.

En cuanto al control y mitigación, los bancos deben establecer procesos y procedimientos administrativos de control y al mismo tiempo generar un marco que facilite y asegure el cumplimiento de las políticas internas reexaminando con una frecuencia mínima anual las estrategias de control y reducción de riesgos operacionales. Para disminuir la vulnerabilidad ante los riesgos operacionales más significativos, se disponen de herramientas tales como pólizas de seguros, sin embargo estas deben ser entendidas como complementos a la gestión del riesgo operacional. La alta gerencia y las unidades organizacionales involucradas directamente con la gestión del riesgo deben mostrar fehacientemente un elevado grado de compromiso para fortalecer los mecanismos de control interno. Las entidades financieras deben contar con planes de contingencia y de continuidad de la actividad, de acuerdo a las características particulares de cada una, para hacer uso pleno de su capacidad operativa y la reducción de las pérdidas en caso de interrupción de la actividad. Para ello, deberán identificar sus procesos más críticos -incluidos aquellos dependientes de terceras partes- y mecanismos alternativos, a los efectos de reanudar el servicio en caso de su interrupción. Las entidades periódicamente deben comprobar la eficacia de sus planes de recuperación y de continuidad del negocio mediante su puesta a prueba, verificando que sean acordes con las operaciones y estrategias de negocio. En relación con los aspectos vinculados a la tecnología informática, además de ser aplicable la normativa pertinente, deben incluirse dentro de los riesgos operaciones de acuerdo a la probabilidad de generar pérdidas.

El organismo de contralor, también se ha expedido específicamente sobre la gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información (BCRA, 2006).

En relación a este tema, el Directorio es el responsable del establecimiento y la existencia de un área que gestione la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas para todos los canales electrónicos utilizado para la comercialización y operatoria habitual de los productos y servicios ofrecidos. Esta unidad organizativa debe evidenciar clara separación funcional con relación a los sectores usuarios de la misma. Del mismo modo, debe ser responsable de las políticas generales y

planes estratégicos (de corto y mediano plazo), y de la asignación de los recursos necesarios. Debe estar involucrado con los aspectos generales que gobiernen la tecnología de la información y sus actividades relacionadas, los riesgos que conllevan, y evidenciar mediante documentación formal la toma de decisiones, el seguimiento y el control de lo establecido.

Los procedimientos que deben llevarse a cabo para el desarrollo de la tarea y control de las áreas de sistemas de información, los cuales involucran al Directorio, Gerencia General, Gerencia de Sistemas de Información (SI) y personal de la entidad, deben estar diseñados para proveer un grado razonable de seguridad en relación con el logro de los objetivos y los recursos aplicados en los siguientes aspectos:

- Eficacia. La información y sus procesos relacionados, debe ser relevante y pertinente para el desarrollo de la actividad. Debe presentarse en forma correcta, coherente, completa y que pueda ser utilizada en forma oportuna.

- Eficiencia. El proceso de la información debe realizarse mediante una óptima utilización de los recursos.

- Confidencialidad. La información crítica o sensible debe ser protegida a fin de evitar su uso no autorizado.

- Integridad. Se refiere a la exactitud que la información debe tener, así como su validez acorde con las pautas fijadas por la entidad y regulaciones externas.

- Disponibilidad. Los recursos y la información, ante su requerimiento, deben estar disponibles en tiempo y forma.

- Cumplimiento. Se refiere al cumplimiento de las normas internas y de todas las leyes y reglamentaciones a las que están sujetas las entidades financieras.

- Confiabilidad. Los sistemas deben brindar información correcta para ser utilizada en la operatoria de la entidad, en la presentación de informes financieros a los usuarios internos y en su entrega al BCRA y demás organismos reguladores.

Todos estos aspectos deben estar presentes en recursos intervinientes en los procesos de tecnología informática, ya sean datos, sistemas de aplicación, tecnología, instalaciones y personas.

En lo referido puntualmente a los riesgos de tecnología, se especifica que el directorio es el responsable de la existencia de mecanismos de control del grado de exposición a potenciales riesgos inherentes a los sistemas de información, de la tecnología informática y sus recursos asociados. Al mismo tiempo, se exige que exista evidencia formal sobre la existencia de análisis de riesgos formalmente realizados y documentados sobre los sistemas de información, la tecnología informática y sus recursos asociados. El seguimiento y los resultados de los análisis mencionados y sus actualizaciones deben incluirse en un informe a presentar ante el Directorio con una periodicidad adecuada. La finalidad de estos reportes repetitivos es que se gestionen que las debilidades que expongan a la entidad a niveles de riesgo alto o inaceptable sean corregidas a niveles aceptables.

B. METOLODOGÍA

El desarrollo del presente trabajo se organizará bajo el siguiente proceso, tal como fue descripto en el marco teórico de Mejora de Proceso siguiendo al autor James Harrington:

I. Organización previa para el mejoramiento de los procesos. Se hará hincapié en la estructura organizativa interviniente en la mejora, los canales de comunicación existentes, y el nivel de compromiso de los colaboradores.

II. Evaluación y entendimiento del proceso actual. Se estudiará el proceso elegido para la mejora, cómo se encuentra actualmente delimitado, identificar los clientes, principales indicadores de efectividad eficiencia y adaptabilidad, obtener la documentación del proceso.

III. Modificación del proceso. En base a un entendimiento acabado de los procesos a mejorar e integrar, se identificará las oportunidades para aumentar la eficacia, eficiencia y adaptabilidad y generar un nuevo proceso

integrado, eliminando errores, retrabajos, burocracia, demoras y baja calidad de las salidas esperadas.

IV. Mediciones y controles. Diseñar e implementar un sistema de control interno para el monitoreo del proceso y permitir la mejora continua del mismo. Se incluye la definición de nuevas métricas del proceso y los umbrales aceptables.

V. Implementación de la mejora. Poner a disposición de los usuarios el nuevo proceso integrado, eligiendo los canales de comunicación adecuados, con la capacitación y los manuales de procedimientos para su utilización

C. TRABAJO DE CAMPO

Capítulo 1: Ámbito de aplicación

En la presente sección se describe la organización sobre la cual se trabaja en la mejora de proceso. Se mencionan los niveles de operaciones, así como también la estructura y las unidades organizativas fundamentales en el proceso.

La institución financiera en donde se aplicará la metodología descripta en los puntos anteriores, desarrolla su actividad de servicios en la provincia de Córdoba, Santa Fe y Capital Federal.

Para dimensionar la magnitud de la entidad financiera, la misma pertenece al grupo de los diez bancos más importantes del país.

En lo que respecta a las operaciones de plazo fijo, presenta una evolución de depósitos que se puede apreciar en la siguiente tabla:

Tabla 1 Evolución de Operaciones de plazos fijos por cartera

	dic-13	dic-14	dic-15	mar-16	jun-16
Cant. de operaciones a plazo fijo Individuos	51.221	58.275	75.976	92.561	100.29

Cant. de operaciones a plazo fijo Empresas	2.813	2.931	3.276	2.389	2.416

Fuente: (BCRA, s.f.)

Estas operaciones pasivas, representan a junio de 2016 más de $11.214.203.000 (BCRA, s.f.).

El banco tiene como principal accionista al gobierno de la provincia de Córdoba. Este hecho marca fuertemente la misión, visión y valores que a continuación se describen:

Misión

Proveer servicios y productos financieros de calidad, eficientes y competitivos, propiciando el desarrollo de la región y de nuestros recursos humanos; logrando ser referentes de una gestión sustentable en nuestra comunidad. Cumplir lo antes posible en el tiempo con el plan de Saneamiento, lo cual requiere fundamentalmente capitalización por utilidades e incrementar sustancialmente el volumen de negocios.

Visión

Ser un banco de desarrollo regional líder, reconocido por su solidez, eficiencia y competitividad, por su excelencia operativa y calidad de atención, así como por su fuerte compromiso con el progreso del sector productivo de la Provincia, la región y la comunidad en general.

Valores

Orientación al Cliente

Sustentabilidad

Compromiso Social

Evolución

Trabajo en equipo

Profesionalismo

Dada la naturaleza de la entidad financiera, se indica que como rasgo distintivo que la banca minorista prevalece sobre la banca comercial, y que el banco opera como socio facilitador en las acciones de gobierno de la provincia, siempre bajo estricta vigilancia de los organismos de contralor pertinentes.

En la ilustración 4 se encuentra plasmada la estructura organizativa sobre la cual se trabaja constantemente para su adecuación a los nuevos procesos de negocios y de soporte y así poder optimizarlos, evitar superposición de responsabilidades, mantener fluidez en la operatoria diaria y dar la flexibilidad suficiente para el trabajo matricial en el caso de proyectos nuevos y de situaciones que así lo ameriten

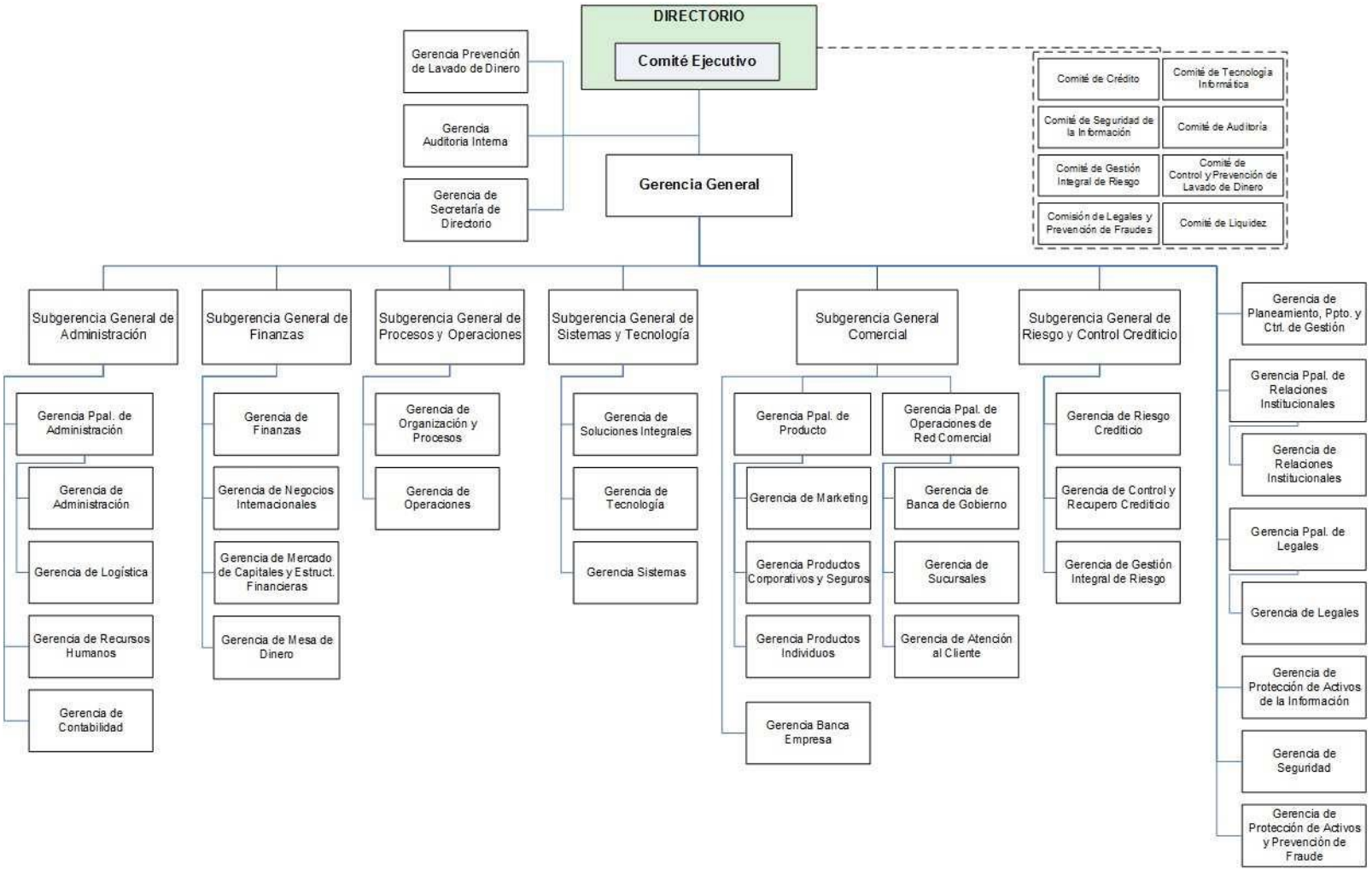


Ilustración 4 Estructura organizacional Banco SA

Una de las unidades organizativas que se identifican en el Banco, es la Gerencia de Gestión Integral de Riesgo (desde ahora en adelante GGIR), que está estructurada de acuerdo se visualiza en la Ilustración 5. La mencionada gerencia tiene como misión controlar los procedimientos vinculados a la gestión integral de riesgos, verificando el cumplimiento de las políticas establecidas en la materia.

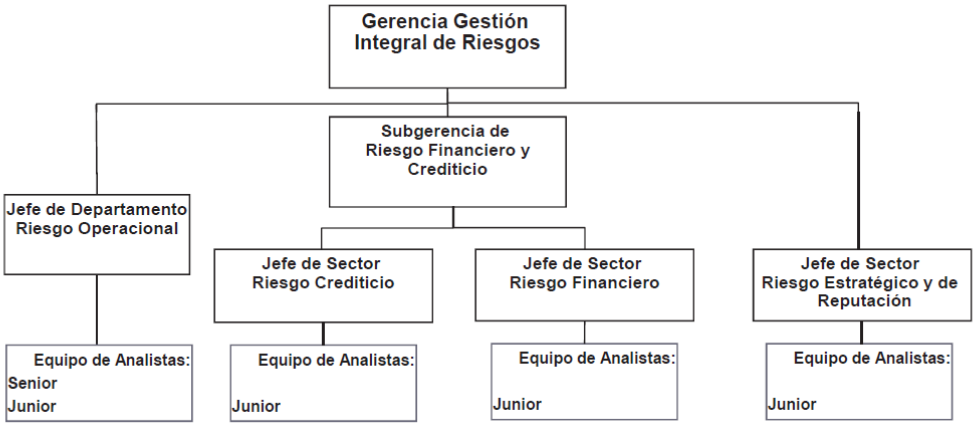


Ilustración 5 Organigrama GGIR

En lo que respecta a la gestión de riesgo, puntualmente el operacional, la misma debe incluir la identificación, evaluación o medición, seguimiento, mitigación y/o control, y reporte de los riesgos operacionales incluyendo los que derivan de amenazas tecnológicas.

En este contexto, es que toma relevancia también la Gerencia de Protección de Activos de la Información (desde ahora en adelante GPAI), que tiene como misión definir los mecanismos apropiados para la administración y el control de la seguridad sobre el acceso lógico y físico a los distintos ambientes tecnológicos y recursos de información que posee y gestiona el Banco. La estructura de la misma se puede visualizar en la Ilustración 6.

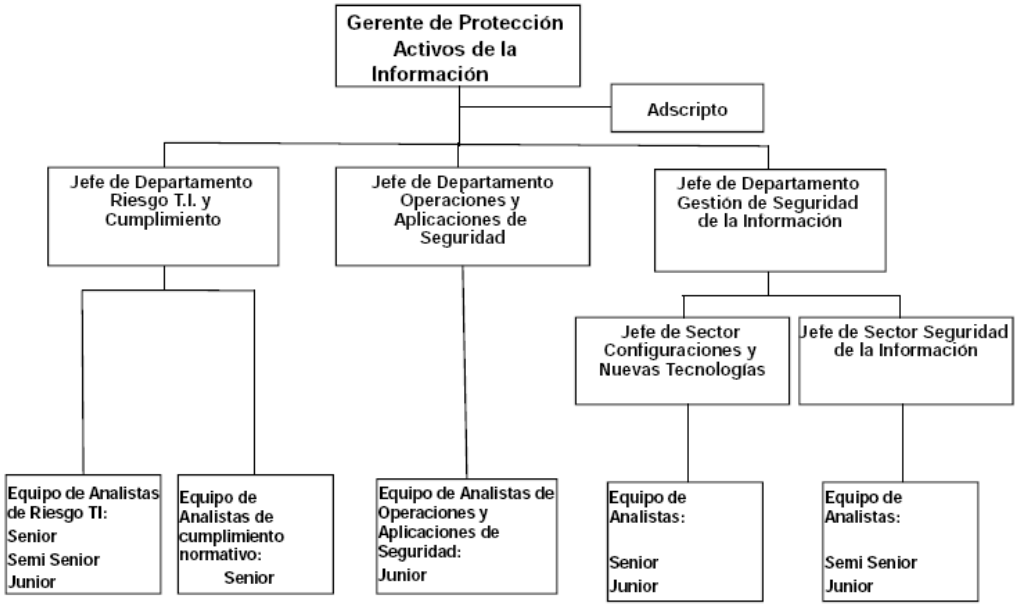


Ilustración 6 Organigrama GPAI

Las dos mencionadas unidades organizativas son relevantes en lo que respecta a la mejora de proceso de gestión de riesgos operacionales. La GGIR es quién tiene como responsabilidad la gestión de los mencionados riesgos, mientras que la GPAI es quién realiza el análisis de riesgos tecnológicos. La interacción entre ambas es fundamental para entender el proceso actual, identificar las potenciales mejoras y plasmar un nuevo proceso integrativo cumpliendo con las exigencias del BCRA.

Capítulo 2: Aplicación de la metodología general

En el capítulo que comienza, se desarrollan los subprocesos para la mejora de la gestión de riesgos operacionales, que se enumeran a continuación:

- Organización previa para el mejoramiento de los procesos
- Evaluación y entendimiento del proceso actual
- Modificación del proceso
- Mediciones y Controles

- Implementación

En lo referido a la modificación del proceso, se presentan en forma integral las tres líneas de trabajo más importantes que dan respuesta a las necesidades de mejora más relevantes identificadas en la evaluación y entendimiento del proceso actual.

2.1. Organización previa para el mejoramiento de los procesos

Con la finalidad de tener un entendimiento acabado del ambiente sobre el cuál se va a trabajar es que se estudiaron los siguientes puntos:

a) Estudio de la estructura de la organización. Tal como se indicó en el apartado anterior, el banco cuenta con una amplia estructura plasmada en la Ilustración 4. Las unidades organizativas relevantes son:

1. Comité de Gestión Integral de Riesgo. tiene como misión, asegurar la administración de los riesgos y supervisar su encuadramiento dentro de los límites de riesgo establecidos por Directorio Se reúne con una periodicidad mínima trimestral. Entre sus atribuciones, se destaca la de supervisar las funciones de control interno implementadas para monitorear el cumplimiento de las reglas del Código de Gobierno Societario, realizar el seguimiento de las actividades relacionadas con la admisión y administración de los distintos riesgos, verificando que los mismos no excedan los niveles definidos por Directorio.

2. Gerencia de Gestión Integral de Riesgo. Dependiente de la Subgerencia General de Riesgo, tiene atribuciones para controlar los procedimientos vinculados a la gestión integral de riesgos, verificando el cumplimiento de las políticas establecidas en la materia. Entre las principales funciones se puede mencionar: coordinar con los responsables de procesos la evaluación, seguimiento, control y mitigación del riesgo operacional en sus aspectos cualitativos y cuantitativos; elaborar propuestas de procedimientos relacionados con la gestión de riesgos operacionales asegurándose que estén en

línea con las políticas y prácticas aprobadas por el Directorio; participar con otras áreas del Banco en la gestión del riesgo operacional inherente a los productos, actividades, procesos y sistemas relevantes; participar activamente en el diseño y reformulación de los indicadores de riesgo operacional cuando lo considere necesario; y finalmente proponer adecuación de los indicadores previstos para la gestión del riesgo operacional cuando lo considere necesario

3. Gerencia de Protección de Activos de la información Dependiente de la Gerencia General, tiene atribuciones en lo referido a gestionar los riesgos asociados a TI identificando controles y medidas tendientes a minimizarlos de forma eficiente y dando cumplimiento a las normas establecidas por los organismos de supervisión. Dentro de las funciones más importantes se destacan: mantener informado a la gerencia con respecto del grado de exposición a potenciales riesgos inherentes a los sistemas de información, de tecnología informática y sus recursos asociados; elaborar reportes y registrar las acciones realizadas para atenuar los riesgos devenidos de la tecnología de la información; elaborar reportes de control de la implementación de políticas de clasificación y valoración de activos de la información; efectuar el seguimiento de aplicación del mapa de riesgos; elaborar reportes de control de implementación de políticas de clasificación y valoración de Activos de la información; y finalmente implementar mecanismos de control para la detección, registro, análisis, comunicación, corrección, clasificación y cuantificación de los incidentes asociados al área.

Como se puede apreciar, las principales unidades organizativas no dependen de las mismas autoridades inmediatas, con lo que será fundamental lograr el compromiso de todos los colaboradores para con el proyecto. Así mismo se destaca la necesidad

de compromiso de los responsables de las gerencias para que ayuden a la asignación ordenada de tareas y se administren las horas de trabajo con una prioridad de temas similar.

b) Diagnóstico del comportamiento y liderazgo directivo. La alta gerencia se encuentra comprometida con la ejecución del proceso de gestión de riesgos. La dirección de la entidad financiera también muestra compromiso, a través de la valoración de los temas más relevantes de la gestión que son elevados y tratados en comité. El soporte de la dirección y la alta gerencia es un factor clave para comenzar con la mejora del proceso. La complejidad y las tareas diarias de la gestión, pueden desviar el foco de atención en la mejora a realizar, sin embargo cuando existe un firme liderazgo directivo que fija el rumbo de la estrategia de cambio, el proyecto aumenta sus probabilidades de éxito.

c) Detalle de canales de comunicación interna. Dentro de la organización existen canales de comunicación informales y formales. La comunicación informal está marcada principalmente por el uso del correo electrónico interno, llamadas telefónicas y reuniones de trabajo a demanda de acuerdo a la importancia de la interacción entre las partes involucradas. Los canales formales, que a su vez tienen validez documental, se los pueden clasificar como:

    1. Comunicación descendente: en este caso se incluye la información de intranet donde se formalizan las políticas de Gestión Integral de Riesgo planteadas por el directorio de la organización.

    2. Comunicación ascendente: se puede citar actas del Comité de Gestión Integral de Riesgo, Informe Semestral de Riesgo Operacional, Informe trimestral de pérdidas por Riesgo Operacional, Informe trimestral de control de límites; Informe Semestral de Riesgo Tecnológico y cumplimiento.

3. Comunicación Transversal: por ejemplo Minutas de Reunión donde quedan plasmadas las principales convenciones sobre un proyecto o tarea en particular.

d) Reuniones participativas de colaboradores: Se utilizarán los canales informales de comunicación para las informar acerca del proyecto que involucra la mejora del proceso de gestión de riesgos operacionales. Los colaboradores a convocar a las reuniones son:

1. Miembros del Departamento de Riesgo Operacional de la GGIR.
2. Miembros del Departamento de Riesgo de TI y Cumplimiento de GPAI.
3. Staff de consultoras involucradas en el proceso.

La finalidad de estas reuniones previas es poner a todos los participantes en conocimiento y lograr un compromiso hacia el proyecto en todas sus etapas.

Para dejar registro de la hablado y acordado en las reuniones previas a la mejora de procesos, se propone utilizar un formulario de minuta de reunión tabulado, tal como se muestra en el ANEXO I.

e) Selección del proceso a mejorar: El proceso a mejorar dado lo descripto en los puntos anteriores es la gestión de riesgos operacionales. No se plantea como proceso a mejorar la gestión de riesgos tecnológicos ya que esta cumple con los requisitos mínimos impuestos por el BCRA, y porque la salida de este proceso es un imput para el proceso de gestión de riesgo operacional.

Para el relevamiento detallado del proceso seleccionado para la mejora, se utilizarán entrevistas a los colaboradores y responsables involucrados en el proyecto, teniendo en cuenta la jerarquía que ocupan en la organización. Los modelos de entrevistas están disponibles en el ANEXO II. Por otra parte se llevará a cabo el análisis de la documentación interna de la empresa. Organigramas, políticas de riesgo, manuales de riesgo e instructivos.

2.2. Evaluación y entendimiento del proceso actual

Se busca tener un conocimiento acabado del proceso seleccionado para mejorar. Tal como se mencionó en el apartado anterior, las principales fuentes de información al abordar esta etapa son los manuales de procedimientos administrativos y las encuestas a los integrantes de la Gerencia de Gestión Integral de Riesgo.

La información obtenida se muestra en forma esquematizada de acuerdo a enfoque metodológico seleccionado.

a) Alcance y objetivos del proceso.

El proceso de gestión de Riesgo Operacional, según se desprende de los manuales de procedimientos administrativos se limita a la identificación, evaluación, control y seguimiento de los riesgos operacionales. El objetivo del proceso es trasladar, mitigar o mantener los riesgos de acuerdo a la estrategia previamente fijada y en base a la identificación y cuantificación previa de los mismos.

En la práctica, según surgen de las entrevistas con los referentes de la Gerencia de Gestión Integral de Riesgos, los riesgos que específicamente se tratan son los riesgos operacionales cuya naturaleza están relacionada a los procesos (ejecución, gestión y finalización de procesos; clientes, productos y prácticas empresariales), personas (relaciones laborales y seguridad en el puesto de trabajo y fraude interno), y a factores externos (fraude externo y daños a activos materiales). No se tratan aquellos riesgos de naturaleza tecnológica, así como tampoco los riesgos vinculados a la continuidad del negocio (catástrofes y similares).

b) Límites del proceso.

De las entrevistas que se realizaron a los colaboradores de la Gerencia de Gestión Integral de Riesgo, se identifica que los límites no se encuentran definidos claramente. Sin embargo, del relato de la práctica se pudieron establecer los siguientes límites:

- Límite inicial: Envío de mail a la unidad organizativa a mapear (identificación de procesos, subprocesos y subprocesos de una determinada Gerencia o Sub Gerencia). Se observa que no existe un orden

para trabajar con las áreas organizativas, a excepción de que se detecten eventos de pérdida por riesgo operacional de la contabilidad formal del Banco. En este caso, se inicia el mapeo del área que reportó la pérdida.

- Límite final: Carga de los cuestionaros de autoevaluación en el Sistema SARO. El seguimiento y los reportes de gestión no se encuentran integrados ni forman parte de la visión global del proceso.

c) Visión general del proceso.

La gestión de riesgo operacional es abordada como un proceso dentro de Banco SA, y se puede describir mediante los siguientes subprocesos:

- **Identificación de riesgos**: Los imputs de esta etapa constituye la información recabada por los colaboradores de riesgo operacional a través de talleres reuniones participativas con todas las áreas del Banco SA para analizar los procesos, subprocesos. En los talleres se pone de manifiesto conceptos claves para esta etapa de la gestión, como son los procesos y qué se entienden por riesgo operacional[3]. Se observa que no existe un material estandarizado para explicar estos conceptos.

  También se toma como imput las partidas de pérdidas y recuperos que figuran en determinadas cuentas contables en las cuáles se registran eventos de riesgo operacional. Ante la detección de una imputación inusual se consulta a las áreas intervinientes sobre las causas de la misma, para determinar si se corresponde a un nuevo riesgo operacional.

  El output de esta etapa son los riesgos operacionales de cada unidad analizada, su descripción, identificación de sus causas y relaciones con otras áreas.

3 La definición se explicita de acuerdo a la Com “A” 5398 del BCRA.

Ilustración 7 Subproceso Identificación. Fuente: elaboración propia.

- **Evaluación**: Sobre los riesgos identificados en la etapa anterior, se realiza una evaluación de su impacto medio y máximo, y su frecuencia para así poder determinar la peligrosidad de los riesgos. Se entiende por impacto a la cuantificación de en términos monetarios de la pérdida que resulte de la concreción del riesgo, calculando a juicio experto la pérdida media y la pérdida máxima; la frecuencia es definida como la cantidad de veces que se puede concretar el riesgo en el período de un año. Al definir el impacto máximos en pesos y la frecuencia en cantidad de veces, a través de las tablas de conversión se asigna un valor del 1 al 5 al impacto y frecuencia. De la relación de estos valores, se define la peligrosidad (también en la escala del 1 al 5, significando 1 el riesgo inherente más bajo y 5 el más alto). También se valora la efectividad de los controles que se ejecutan sobre los procesos con riesgos identificados, otorgándole una puntuación del 1 al 5, en donde 1 es el mitigante más efectivo y 5 el mitigante menos efectivo. De la interacción entre la peligrosidad y la efectividad del mitigante, se obtiene una valoración de riesgo inherente, pudiendo ser Alto (rojo), Medio (amarillo) y Bajo (verde). Estos riesgos son alocados en las líneas de negocio correspondientes y sirve para su seguimiento. La información recolectada se plasma en el Sistema de Administración de Riesgos Operacionales (SARO).

Tabla 2. Escalas de Impacto Máximo por riesgo.

	Impacto Máximo Anual	
Impacto	Desde	Hasta
1	$ 0	$ 119,999

2	$ 120,000	$ 499,999
3	$ 500,000	$ 999,999
4	$ 1,000,000	$ 9,999,999
5	$ 10,000,000	

Tabla 3. Escala de Frecuencia por riesgo.

	Frecuencia Anual	
Frecuencia	Desde	Hasta
1	0.01	0.99
2	1	23.99
3	24	47.99
4	48	119.99
5	120	

En forma resumida los inputs son los procesos, la frecuencia, impactos y efectividad de mitigantes. Los outputs son las valoraciones de riesgos inherentes y residuales.

Ilustración 8. Subproceso Evaluación. Fuente: elaboración propia.

La información recolectada en los subprocesos de identificación y evaluación se plasma en los formularios de "Mapa de Riesgo Operacional" y "Autoevaluación de Riesgo Operacional" que se incluyen en el ANEXO III y ANEXO IV respectivamente.

En este punto se observa, al analizar la base de riesgos cuantificada, que no se ha aplicado un criterio uniforme en su cuantificación y que gestionar por la matriz de riesgo residual calculada como está en la actualidad no coincide con

la gestión que surge de la asignación de capital luego del cálculo de capital económico.

- **Seguimiento**: De la información recolectada se construye la matriz de riesgo del Banco, lo posibilita la fácil identificación del perfil de riesgo de la entidad. Al mismo tiempo, desde la GGIR se elaboran indicadores para monitorear la evolución de los principales riesgos declarados. El seguimiento también se realiza a través de la herramienta SARO con un sistema de alertas y vencimientos de mapeos de riesgos por unidad organizativa.

  En forma resumida los inputs son los riesgos cuantificación y valoración, y el output son las matrices de riesgo inherente y residual.

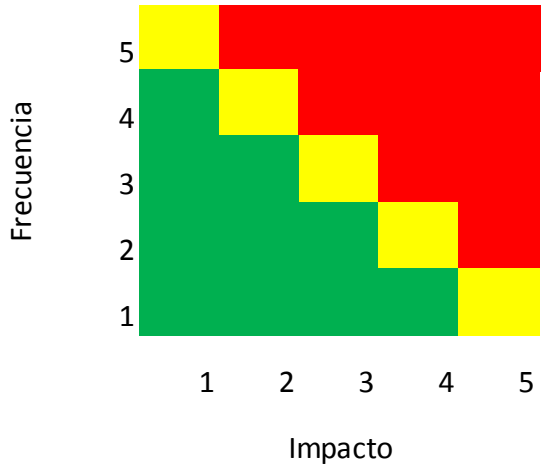


Ilustración 9 Matriz de Riesgo Inherente

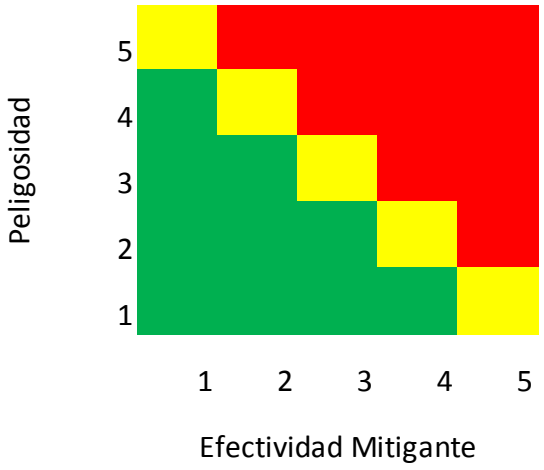


Ilustración 10 Matriz de Riesgo Residual

- **Control y mitigación**: En esta etapa se involucran tanto los colaboradores del Departamento de Riesgo Operacional así como también colaboradores designados como referentes dentro de toda la organización. Ante la detección de riesgos clasificados como altos (por poseer un riesgo residual en rojo) se debe desarrollar un plan de mitigación donde se identifican los siguientes elementos: proceso, subproceso, riesgo, acciones para mejorar la calificación de riesgo (tendiente a disminuir impacto o frecuencia del mismo), responsables de la implementación de las mejoras y finalmente fechas de revisión y/o avance.

  El plan de mitigación queda plasmado en un formulario como se muestra en el ANEXO V.

- **Reporte**. La información disponible en SARO y en los formularios utilizados durante el proceso de gestión de riesgo operacional es utilizado para los siguientes informes:

  - Informe Semestral de Riesgo Operacional: de índole cualitativa, hace un seguimiento sobre las unidades organizativas mapeadas, se resaltan los riesgos críticos de las mismas, se menciona el seguimiento de los principales riesgos operacionales de toda la entidad y se utiliza como vía para informar sobre cambios relevantes a nivel de gestión de riesgo operacional. Cliente interno: Comité de Gestión Integral de Riesgo.

  - Informe trimestral de pérdidas por Riesgo Operacional: a los riesgos cargados en SARO, se les asignan imputaciones de pérdidas y recuperos asociadas (tomando como fuente principal la contabilidad de gestión de la entidad). Trimestralmente se elabora dicho informe de forma tal de presentar todos los eventos de manera agregada lo que permite mejorar la acciones de mitigación sobre aquellos riesgos con mayor pérdida. Cliente Externo: BCRA. Cliente Interno: Comité de Gestión Integral de Riesgo.

- Informe trimestral de control de límites: Para los riesgos operacionales críticos, se elaboran indicadores que representan la evolución de dicho riesgo en la entidad. El informe también contiene indicadores de otros tipos de riesgos (riesgo de mercado, riesgo estructural de balance, riesgo de crédito, riesgo de concentración y riesgo de liquidez). Cliente Interno: Comité de Gestión Integral de Riesgo.

- Base de información para Cálculo de Capital Económico por riesgo operacional. El Banco SA tiene la obligación de elaborar el Informe Anual de Autoevaluación de Capital, en donde se hace referencia al Cálculo de Capital Económico por Riesgo Operacional. Para su determinación se usa como imput el mapa general de riesgos de la entidad, obtenida de SARO en donde se toman los datos de riesgos, impacto máximo, impacto promedio y frecuencia. También se incluye como imput la base de eventos de pérdida por riesgo operacional obtenida de SARO y su asignación a riesgos. Ambas bases son procesadas por un motor de cálculo de acuerdo a distintos modelos de simulación estadísticas que permitan estimar el Capital Económico por Riesgo Operacional.

  La situación actual, es que a Diciembre de 2015 el valor del Capital Económico por Riesgo Operacional representa un 16% del Capital Regulatorio (siendo el promedio de las entidades financieras de igual magnitud del Banco SA el 20%). Esta situación se debe, en parte, a la variabilidad de los criterios de evaluación de los riesgos (pasando de un criterio experto a uno de valoración a través de factores cuantificables).

d) Clientes.

Los principales clientes del proceso son internos de la entidad. Agrupando los subprocesos se definen los siguientes clientes.

Identificación, evaluación y control y mitigación: los clientes son las propias unidades organizacionales del banco. En la gestión de riesgo operacional, el conocimiento de los riesgos que se identifican y su control depende de las áreas intervinientes, es por esto que el la devolución de la información procesada por la GGIR, es de utilidad para sector, departamento, subgerencia y subgerencia para la toma de decisiones y la asignación de recursos de manera más eficiente.

Seguimiento: el principal cliente interno es el Comité de GIR, ya que la definición del perfil de riesgo de la entidad y su seguimiento es un asunto de la alta dirección. Este perfil de riesgo debe estar acorde a las demás políticas del banco (ante mayor riesgo asumido, más agresiva la estrategia comercial y viceversa).

Reporte: Los clientes son de dos categorías, internos y externos, esto depende de qué tipo de reporte se trate. En el caso del Informe Semestral de Riesgo Operacional, el principal cliente es el Comité de GIR, en el caso del Informe Trimestral de Pérdidas por Riesgo operacional, el principal cliente es el BCRA, como secundario el Comité de GIR, el informe de Control de Límites tiene cliente también al Comité de GIR y finalmente la Base para cálculo de Capital Económico tiene como principal cliente la misma GGIR.

e) Indicadores y límites para medir la efectividad, eficiencia y adaptabilidad.

En la actualidad, los únicos indicadores que existen, son los que se pueden relevar en el informe de Control de Límites. Estos son cocientes que dimensionan la evolución de los dos riesgos más significativos de la entidad. Sin embargo estos indicadores, no son los más adecuados para medir la efectividad eficiencia y adaptabilidad de la Gestión de Riesgo Operacional.

De acuerdo se desprende de la presentación de Capital Económico por Riesgo Operacional a Diciembre de 2015, el mismo representaba un 16% del Capital Regulatorio por Riesgo Operacional. Este porcentaje está por debajo del promedio de otras entidades de igual magnitud en el país, reflejando en parte, una escasez de riesgos identificados y evaluados que alimentan la base de cálculo para Capital Económico.

f) Diagrama de flujo del proceso actual.

De acuerdo a los manuales de procedimiento, el proceso no cuenta con un diagrama de flujo.

g) Costo, tiempo y valor.

El costo del proceso es directamente proporcional a los recursos empleados y al tiempo que se consume para terminar el proceso por cada unidad organizacional y a los reportes elaborados.

Actualmente, se sabe que los colaboradores de la GIR que trabajan en relación al Riesgo Operacional son tres: un analista junior, un analista senior y un jefe de departamento.

Quienes realizan la tarea de identificación, evaluación y seguimiento en forma conjunta con las unidades organizaciones son los analistas. Los sueldos mensuales con cargas sociales son las siguientes[4]:

Tabla 4 Costo Salarial

	Conceptos				
	REMUNERATIVOS	NO REMUNERA.	CONTRIB.	SAC	**COSTO TOTAL**
AN. JUNIOR	$ 19.530,92	$ 1.075,32	$ 6.249,89	$ 2.148,40	**$ 29.004,54**
AN. SENIOR	$ 35.386,44	$ 2.782,11	$ 11.323,66	$ 3.892,51	**$ 53.384,72**

Se estima que para la identificación y evaluación de riesgos en una unidad se utilizan 75 horas de trabajo completas de ambos analistas (no existe un registro formal de inicio y fin de mapeo de riesgos). La dedicación horaria varía en función a la complejidad de los procesos a evaluación, y a la cantidad de procesos llevados a cabo por la unidad organizativa tratada.

4 Los valores referenciados están de acuerdo a la escala salarial del convenio colectivo de trabajo de empleados bancarios (nº 18/75), sin tener en cuenta costos indirectos como por ejemplo las licencias.

En cuanto al seguimiento que incluye el monitoreo a través de alertas y la elaboración de presentaciones para Comité de GIR se emplea por mes 7.5 hs de analista jr (en promedio, ya que los comités están programados trimestralmente) en el caso del analista sr 7.5 hs cada dos meses.

Control y mitigación, es una de los subprocesos en donde los protagonistas son los referentes de las unidades organizativas y los colaboradores de ellos. Estos recursos son los que están presentes en las actividades en forma diaria, con la oportunidad de solicitar e implementar mitigantes. Por este motivo las horas de los colaboradores del Dpto. de Riesgo operacional tiene una participación en términos relativos despreciable, por lo que no se incluye en el cálculo de costos.

Al mismo tiempo para la elaboración de los informes se utilizan las siguientes horas en el momento de elaboración de cada informe:

1. Informe semestral de Riesgo Operacional: analista jr. 37.5 hs. Frecuencia de preparación anual: dos veces por año.

2. Informe trimestral por pérdidas de Riesgo Operacional: analista jr. 30 hs. Frecuencia de preparación anual: cuatro veces por año.

3. Informe de Control de Límites: analista jr. 15 hs. Frecuencia de preparación anual: cuatro veces por año.

4. Base para cálculo de Capital Económico: analista jr. 7.5 hs. Frecuencia de preparación anual: una vez al año.

Cabe aclarar que los informes son preparados sin distinción de las unidades organizativas o procesos evaluados y sus riesgos.

Tabla 5 Tiempo y costos de subprocesos

Subproceso	Detalle	Hs. An. Junior	Costo	Hs. An. Senior	Costo	Costo Total
Identificación Evaluación		75	$ 14,502.27	75	$ 26,692.36	$ 41,194.63
Subtotal		75	$ 14,502.27	75	$ 26,692.36	$ 41,194.63

Mapeo						
Seguimiento		90	$ 17,402.72	45	$ 16,015.42	$ 17,402.72
Subtotal Seguim.		90	$ 17,402.72	45	$ 16,015.42	$ 17,402.72
Reporte	Informe Semestral RO	75	$ 14,502.27	-	-	$ 14,502.27
	Informe Trimestral RO	120	$ 23,203.62	-	-	$ 23,203.62
	Informe Control de Límites	60	$ 11,601.81	-	-	$ 11,601.81
	Base para Capital económico	7.5	$ 1,450.23	-	-	$ 1,450.23
Subtotal Reporte		262.5	$ 50,757.93	-	-	$ 50,757.93
Costo total						**$ 109,355.27**

Con la información relevada, se puede determinar que el costo por mapeo de riesgo (incluye identificación, evaluación) es de $41,194.63 por unidad organizativa, el costo del seguimiento es de $ 17,402.72 al año y el de elaboración de reporte es de $109,355.27 por año.

h) Documentar el proceso.

El proceso en su situación actual se encuentra documentado en el Manual de Procedimiento de Riesgo Operacional.

2.3. Modificación del proceso

En base a la información recopilada, el análisis del proceso actual y la detección de las mejoras, se plantean en forma metodológica las mejoras y modificaciones que pueden aplicarse en el proceso de gestión del Riesgo Operacional, particularmente sobre los subprocesos de Identificación y Evaluación de riesgos.

Las principales actividades involucradas en esta etapa son:

a) Oportunidades para la intervención.

Los puntos más críticos a mejorar dentro del proceso de gestión de riesgo operacional son:

- No se incluyen los riesgos tecnológicos: la principal falencia del proceso radica en la exclusión de los riesgos relacionados a los activos de información[5] y a los activos informáticos[6]. Se propone, luego de las entrevistas con los colaboradores de la Gerencia de PAI, identificar las amenazas de TI que coinciden con Riesgos Operacionales (es necesario trabajar con las taxonomías de riesgos propuestas por el BCRA), incorporar al mapeo estas amenazas bajo riesgos ya existentes o nuevos, respetando la frecuencia de ocurrencia de TI, y asignándole un valor de impacto en el negocio (no tecnológico ya que la tecnología se encuentra garantizada en los contratos con los proveedores o por redundancia de equipos).

- Demoras prolongadas: el proceso (especialmente los subprocesos de identificación y evaluación) demoran más de lo deseado. Esta apreciación se basa en la entrevista realizada a la responsable de la GIR, ya que no existe medición de los tiempos empleados en el proceso. La valoración de su juicio experto se basa en las actividades que se dejan de lado para atender el mapeo de procesos y riesgo. Este último ítem es otro aspecto a mejorar.

  Las causas de demora en el proceso obedecen a los siguientes factores:

5 Activos de información: denominación que se le otorga a los datos que son utilizados en un proceso de negocio o de soporte, que pueden ser agrupados por su similar origen o utilización.

6 Activos informáticos: cada uno de los componentes de las capas informáticas, por ejemplo dentro de la capa: “Software de aplicaciones”: Sistema SAP, Sistema QView, etc.

- Si bien el proceso de gestión se encuentra descripto en el manual de procedimientos administrativos, esta descripción es genérica, no existe un manual de usuario o guía de check list con los pasos necesarios a ejecutar que guíen el accionar de los colaboradores de Riesgo Operacional. Se recomienda desarrollar un manual de usuarios o un check list que incluya: revisión de Manual Orgánico Funcional de la entidad, revisión de observaciones de auditoría interna, revisión de mapeos anteriores, revisión de mapeos residuales (se trata de riesgos cuyos dueños no se encuentran identificados), actualización de impactos por inflación, entre otros aspectos relevantes.

- Escasa capacitación de las unidades organizativas. Si bien, previo a cada mapeo de procesos y riesgos de realiza un taller en donde se ponen de manifiesto conceptos claves para esta etapa de la gestión, como son los procesos y qué se entienden por riesgo operacional, no existe un material estandarizado para explicar estos conceptos. Se propone realizar una capacitación general para todos los miembros del Banco SA a través de la plataforma de e-learning. Al mismo tiempo se recomienda armar un contenido de capacitación específica para los referentes de riesgo operacional en cada una de las unidades organizativas, en donde se refuercen los conceptos más relevantes y se facilite la identificación y medición de riesgos.

- No existe una fluida comunicación entre el Dpto de Riesgo Operacional y las unidades organizativas sobre las cuales se analizan los procesos y riesgos. El contacto es por mail, no está sistematizado y no se respetan los tiempos de entrega de información pactados. La propuesta recae en armar un circuito automatizado para comenzar el mapeo con un requerimiento por

parte de la GGIR al responsable de la unidad organizativa, dejando registrado el tiempo que se demora en la asignación y contestación de la solicitud. El circuito puede funcionar sobre el sistema de SAP ERM, que ya posee la entidad.

- Los criterios para la evaluación de riesgos no son uniformes en todos los riesgos relevados. La elaboración de informes y de reportes se ven influenciados por esta falencia, ya que no permite la comparabilidad de los mismos, afectando al mismo tiempo la base de cálculo par Capital Económico por Riesgo Operacional. Se propone una nueva forma de cuantificar los riesgos, ya no basado en juicio experto, sino con variables que sean medibles, enfocándose en el impacto residual de los riesgos.

b. Eliminar la burocracia

En el proceso actual, la burocracia está representada por las numerosas interacciones por mail, ya sea por solicitud de información para el mapeo procesos y riesgos o motivos de imputaciones de movimientos. Con la automatización en un circuito vía ERM, esta burocracia que implica una pérdida de tiempo en el proceso se verá reducida a una secuencia definida de pasos concretos y con destinatarios prefijados.

Con la inclusión de los riesgos tecnológicos dentro de la órbita de los riesgos operacionales se puede producir un exceso de burocracia para solicitar información e integrar los riesgos. Para evitar esta situación, se plantea incluir en el manual de procedimiento las relaciones entre las Gerencias de PAI y GIR e instancias de validación para evitar re trabajos en instancias avanzadas en el proceso de gestión de riesgos operacionales.

c. Eliminar actividades que no agreguen valor

En el presente trabajo de aplicación, al estudiar el proceso no se identifican actividades que no agreguen valor. La ejecución de los subprocesos es significativa ya que el organismo de contralor de la actividad financiera exige su cumplimiento. De esta manera, si se eliminaran actividades se generaría un costo adicional por la imposición

de multas, empeoramiento de la calificación CAMELBIG[7] y hasta un impacto reputacional.

e. Reducir el tiempo de proceso

La mejora en el proceso se plantea como tiene como consecuencia esperada disminuir el tiempo de proceso. Puntualmente en los siguientes subprocesos:

Tabla 6 Reducción de tiempos por subproceso

Subproceso	Detalle	Hs. Proceso Actual		Hs. Proceso Mejorado		Reducción en %
		An. Jr.	An. Sr.	An. Jr.	An. Sr.	
Identificación		75	75	55	55	27%
Evaluación						
Subtotal Mapeo		75	75	55	55	27%
Seguimiento		90	45	60	30	33%
Subtotal Seguim.		90	45	60	30	33%
Reporte	Informe Semestral RO	75	0	60	0	20%
	Informe Trimestral RO	120	0	100	0	17%
	Informe Control de Límites	60	0	30	0	50%

[7] Superintendencia de Entidades Financieras y Cambiarias de Argentina califica a cada entidad financiera con una nota de 1 a 5, siendo 1 la mejor nota y 5 la peor. Dicha calificación surge de una evaluación compuesta sobre distintos componentes de la entidad financiera, tanto cualitativos como cuantitativos, a saber C Capital, A Activos, M Mercado, E Ganancias, L Liquidez, B Negocio, I Controles internos y G Gerencia. La calificación obtenida podrá ser limitante para ciertas operaciones (Ej.: fraccionamiento del riesgo crediticio en call money, exigencia de capital por riesgo de crédito, cesión de cartera de créditos, apertura de sucursales, participación en ciertas empresas de servicios complementarios de la actividad financiera, aporte al Seguro de Depósitos, entre otros).

	Base para Capital económico	7.5	0	7.5	0	0%
Subtotal Reporte		262.5	0	197.5	0	25%
Total de horas		**547.5**		**397.5**		**27%**

La reducción en los tiempos de los subprocesos de Identificación y evaluación obedecerían a las siguientes causas:

1. Mejora en la preparación previa de los mapeos de las unidades organizativas por la elaboración de check list con actividades tales como revisión de Manual Orgánico Funcional de la entidad, revisión de observaciones de auditoría interna, revisión de mapeos anteriores, revisión de mapeos residuales (se trata de riesgos cuyos dueños no se encuentran identificados), actualización de impactos por inflación.

2. Mejora en los talleres/autoevaluaciones luego de capacitación con contenido específico para los referentes de riesgo operacional en cada una de las unidades organizativas, en donde se refuercen los conceptos más relevantes y se facilite la identificación y medición de riesgos. Este contenido debe ser uniforme y actualizado para todos los mapeos.

3. Modificación de formularios, que incluyan origen de datos para la evaluación reiterativa, utilización de lenguaje unificado (a nivel de taxonomías de riesgos de BCRA y amenazas de riesgo tecnológico). Los formularios deben estar acorde a los nuevos criterios de cuantificación.

4. Aplicación del circuito de ERM para el inicio, seguimiento y finalización de los mapeos.

La reducción en los tiempos de los subprocesos de seguimiento y reporte se plantean como una consecuencia en la mejora de los outputs del mapeo de procesos y riesgos. Al tener información completa (incluyendo riesgos tecnológicos), homogénea y en

tiempo y forma, el seguimiento y los reportes de interés deben consumir menos tiempo por recurso (aumenta la eficiencia).

f. Estandarización

La estandarización en el proceso de puede apreciar en las siguientes mejoras descriptas previamente:

1. Circuito de ERM.
2. Capacitación con material uniforme y actualizado.
3. Utilización de formularios únicos con información homogénea.

g. Documentar el proceso

Dado el hecho de que el proceso actual se encuentra documentado, se propone la actualización de manual de procedimiento administrativo con las mejoras enunciadas en los puntos anteriores.

En el manual debe incluirse también el diagrama de flujo del proceso para ayudar al entendimiento del mismo, su fácil transmisión a otros colaboradores,

También se propone modificar el Manual Funcional Orgánico para incluir las siguientes funciones (dándole mayor jerarquía al proceso de gestión de riesgo operacional):

- A la Gerencia de Gestión Integral de riesgo: la función de administrar los riesgos tecnológicos considerando los impactos en el negocio de los mismos, en consonancia a lo evaluado por la Gerencia de Protección de Activos de la Información.
- A la Gerencia de Protección de Activos de la Información: la función de informar sobre lo actuado respecto a riesgos tecnológicos a la GGIR y prestar colaboración para la incorporación de los mismos a su gestión de riesgos.

- A todas las Gerencias de la entidad financiera: la función de identificar, evaluar, controlar y mitigar los riesgos operacionales de los procesos que se ejecuten en colaboración con la GGIR.

h. Otorgar capacitación y entrenamiento a los colaboradores

Se ha mencionado de manera reiterativa la necesidad de otorgar capacitación tanto global a través de una plataforma de e-learning como también una capacitación focalizada en los referentes de riesgo operacional de las unidades organizativas.

Por otro lado, los colaboradores de riesgo operacional también deben instruirse respecto al nuevo proceso con las modificaciones finales, además de perfeccionarse de manera continua con cursos sobre operatoria bancaria y congresos y jornadas relacionadas a riesgo operacional, prevención de fraude interno y externo, auditoría y otros temas afines.

i. Estudiar y aplicar herramientas de automatización

La herramienta que hoy soporta la gestión de riesgo operacional es SARO. Esta aplicación de negocio, tiene como ventaja que ha sido desarrollada en la propia entidad financiera, con lo cual su modificación y testeo de resultados esperados se pueden realizar sin costos significativos.

Las principales modificaciones a aplicar son:

- Incorporación de campos adicionales relevados en forma homogénea con la nueva metodología de mapeo que incluya los riesgos tecnológicos tales como:
    - Fecha de mapeo
    - Taxonomía de riesgo según Comunicación “A” 4904 del BCRA
    - Frecuencia de Ocurrencia Máxima
    - Pérdida Esperada Media

- Pérdida Esperada Máxima
- Mapea con amenaza de TI?
- Amenaza de TI relacionada
- Amenaza de TI dependiente
- Interno de Riesgo-Amenaza dependiente

- Modificación de campos existentes: dado el nuevo criterio para cuantificar, se deben cambiar las denominaciones y fórmulas de los campos “Riesgo Inherente” y “Riesgo Residual” por “Riesgo Medio” y “Riesgo Máximo”.
- Modificación de funciones existentes: los reportes disponibles en el sistema (Riesgos por procesos y matrices analíticas) deben contemplar los nuevos campos y la modificación de los existentes. En el caso de matrices de “Riesgo Inherente” y “Riesgo Residual” serán reemplazadas por las matrices de “Riesgo Medio” y “Riesgo Máximo”.

En forma integral se desarrollan las siguientes mejoras:

a) Integración de riesgos operaciones y tecnológicos.

La integración de riesgos supone el trabajo en conjunto de las gerencias involucradas de manera tal que como resultado final se obtenga la matriz de riesgos completa. En la misma debe incluirse el registro de los riesgos, sus frecuencias e impactos, con la opción de realizar el análisis por producto o proceso de negocio.

Se tiene como información que la gestión de riesgos operacionales se estructura de la siguiente manera (soportado por el sistema SARO):

I .Líneas de Negocio: Se trata de una clasificación del BCRA que incluye los procesos de negocios y pueden definirse en forma adicional Líneas de Soporte que auxilia la operatoria comercial. Ejemplo: Banca Minorista

1. Productos: Se incluyen los principales productos comercializados por la entidad financiera. También se incluyen los productos de soporte. Ejemplo: Depósitos a plazo.

    a. Procesos: actividad o grupo de actividades que utiliza recursos de entrada, agrega valor a estos y genera recursos de salida para un cliente interno o externo. Los procesos usan los recursos de una organización para generar determinados resultados (Harrington, 1991). Ejemplo: Alta, Baja y Modificación de Plazos Fijos.

        i. Subprocesos: cada grupo de actividades que conforman parte de un proceso. Ejemplo: Alta de Plazo Fijo por Back Office.

            1. RIESGO: Taxonomía de riesgo operacional, con indicación de factores y cuantificación.

Respecto a la gestión de riesgos tecnológicos, se vislumbra el siguiente esquema (soportado en planillas de Excel):

1. Procesos de Negocio: Están relacionados a la conglomeración de subprocesos llevados a cabo para generar productos y servicio. Ejemplo: Depósitos a Plazo.

    a. Procesos de Soporte: Son aquellos procesos que coordinan el desarrollo y el ciclo de vida de las actividades contenidas en los procesos principales.

        i. Activos de la información: Se refiere a la clasificación de la información que se genera, que se comunica y se mantiene de los procesos antes mencionados. Depósitos a Plazo.

            1. Activos tecnológicos: Se refiere a cada una de las aplicaciones de negocios, aplicaciones de software base,

hardware que dispone el banco y son clasificadas por cada una de estas capas antes mencionadas.

a. Amenazas: riesgos tecnológicos que son evaluados en cuanto a la probabilidad de ocurrencia y e impacto (no monetario).

Ilustración 11 Integración de Riesgos. Fuente: elaboración propia.

En base a la información disponible, y para evitar la duplicación de riesgos, se decide la integración a nivel de Riesgo Operacional – Amenaza de TI.

A continuación se describe la integración, de acuerdo a la participación de cada una de las gerencias involucradas (Gerencia de Gestión Integral de Riesgos y Gerencia de Protección de Activos de la Información) y las tareas a desarrollar.

Gerencia de Protección de Activos de Información

a. Inventario de riesgo tecnológicos o amenazas

Como resultado del análisis de riesgo tecnológico, se obtiene un inventario de amenazas tecnológicas, evaluadas para cada activo informático. En esta etapa el sector a cargo de la cuantificación de las amenazas deberá realizar un inventario de todas aquellas amenazas que se presentan en la Entidad.

Como premisa se toma que la tecnología se encuentra garantizada, es decir cubierta económicamente por contratos con proveedores de TI, por duplicación de servidores, y por redundancia de equipos críticos.

Al margen de lo expuesto en el párrafo anterior, tener a disposición del banco la totalidad de las amenazas involucradas en la actividad habitual, puede llegar a ser útil en caso que en el futuro alguno de los motivos que garantizan la tecnología no sean más válidos.

b. Cuantificación de las Amenazas

Dado el inventario de amenazas de la entidad, se debe asignar una frecuencia de ocurrencia a cada amenaza por activo informático.

Finalizado el análisis de riesgo tecnológico (ciclo anual), la Gerencia de Protección de Activos de la Información debe remitir las bases a la Gerencia de Gestión Integral de Riesgos para su correspondiente mapeo con riesgos operacionales de cada área analizada.

Una vez obtenidas las matrices de riesgos operacionales cuantificadas (Ver apartado siguiente), la Gerencia de Gestión Integral de Riesgos pondrá en conocimiento a la Gerencia de Protección de Activos de Información de aquellas amenazas que fueron mapeadas con riesgos operacionales con el objetivo de conciliar entre ambos sectores la información en caso de que existan diferencias en los análisis.

Gerencia de Gestión Integral de Riesgos – Relevamiento de Riesgos

A partir del inventario de amenazas tecnológicas con frecuencia de ocurrencia, se debe proceder a la cuantificación del impacto en el negocio o procesos de soporte de los riesgos por medio de los Formularios de Mapeo.

Todas las metodologías soportadas en el formulario de de Mapeo se sustentan en aproximaciones a través de la utilización del juicio experto de los referentes de riesgo operacional de las distintas unidades operacionales. Se busca la medición aproximada basadas en elementos cualitativos (opiniones de expertos) y cuantitativos de los impactos residuales.

Se exponen las tareas a desarrollar:

a. Identificación de Riesgos y Planteo del Escenario

Se selecciona la unidad organizacional sobre la cual se identificarán y evaluarán los riesgos. En caso que la misma ya posea un mapa de riesgos, es necesario validar si los mismos se mantienen vigentes (en el caso que no se hayan podido mitigar totalmente o que no se hayan modificados los procesos y subprocesos que lo originan) y se investiga acerca de los nuevos controles que hayan aplicado a fin de actualizar la cuantificación anterior.

Una vez analizados los procesos y subprocesos ejecutados por el sector, se identifican los riesgos que lo afectan.

Para cada riesgo, se debe determinar un escenario probable. La elaboración del escenario implica buscar las condiciones necesarias para que se presente la pérdida en base a la experiencia registrada (elemento subjetivo). Se destaca en este punto que el escenario debe referirse al planteo de una situación posible o real y que posibilite la medición cuantitativa del riesgo.

El escenario debe relacionarse con el evento que origina el riesgo. De esta manera, se distinguen cuatro tipos de riesgos a partir del origen del evento:

i. Riesgos Operacionales puros: su origen se relaciona con la operatoria habitual del Banco sin que estén relacionados a activos informáticos.
ii. Riesgos Tecnológicos puros: su origen se relaciona en forma exclusiva con activos informáticos que se encuentran garantizados, por lo que no son tratados para su cuantificación.

iii. Riesgos que surgen de un evento/amenaza de TI y que se relacionan con riesgos operacionales: estos forman parte de la integración de riesgos operacionales con tecnológicos, y se debe cuantificar aquellas posibles pérdidas en el negocio causadas por amenazas de los activos informáticos (aplicaciones de negocios, aplicaciones de software base, hardware, etc.)

Dentro del último grupo, se pueden presentar dos clases de riesgos; los que se relacionan con la amenaza de tecnológica de forma dependiente y los que lo hacen de forma independiente.

- *Riesgos Dependientes*: Se presenta en los casos en donde una amenaza de TI genera las pérdidas asociadas al escenario A y B en forma simultánea.
- *Riesgos Independientes:* Se presenta en los casos en donde una amenaza de TI genera las pérdidas asociadas al escenario A o B pero el origen de la amenaza no es el mismo.

b. Cuantificación

Posteriormente a las reuniones de la Gerencia de Gestión Integral de Riesgo con la unidad organizativa en análisis, con la identificación de riesgos correspondiente con los escenarios de ocurrencia, se procede a la cuantificación.

La cuantificación de los riesgos significa la estimación una frecuencia promedio, frecuencia máxima, impacto promedio e impacto máximo, tomando como período de ocurrencia al año (para no influenciar las mediciones con estacionalidades).

- *Frecuencia promedio*: Número de veces que se espera que ocurra la pérdida al año.
- *Frecuencia máxima*: Número de veces que se espera que ocurra la pérdida al año en relación al escenario de máximo impacto.
- *Impacto promedio:* Indica, en caso de que se produzca la pérdida, a cuánto ascendería ésta en términos monetarios medios.

- *Impacto Máximo*: Este concepto consiste en la pérdida probable en el contexto de un escenario pesimista dentro de una situación "razonable", esto es, sin llegar a considerar eventos catastróficos.

Teniendo en consideración al escenario planteado para cada riesgo se realiza la cuantificación de cada uno de los puntos anteriores. No es posible definir un criterio de cuantificación único para todos los riesgos (al margen de la evaluación de riesgos por sus impactos residuales), con lo cual el criterio del analista de riesgo cumple un rol sumamente importante a la hora de sugerir los valores. Sin embargo también se debe contemplar que los mismos deben ser razonables para el producto analizado.

En aquellos casos en donde no se pueda obtener una cuantificación certera, es posible definir escenarios de cuantificación mínima. Lo descripto anteriormente está por la necesidad de incluir en el análisis al menos un escenario, por más poco probable (o de bajo impacto) que sea para que sea contemplado en el cálculo de CE.

Para facilitar la tarea de cuantificación se dejan a disposición las siguientes preguntas a realizar a las unidades organizacionales mapeadas durante la evaluación de riesgos:
Frecuencia:

- "¿Cuántas veces al año/mes se presenta el escenario que genera esta pérdida?"
- "Cantidad de casos donde al año/mes donde se presenta el escenario que genera esta pérdida"
- "Cantidad de casos donde al año/mes donde se presenta el escenario que genera esta una pérdida máxima"
- "¿Con que frecuencia se presenta el escenario que genera esta pérdida?"
- "¿Se podría contemplar un escenario en donde 1 vez cada X años ocurra el evento?"

Impacto:

- "¿Cuál sería un impacto medio asociado al escenario?"

- Impacto asociado a amenazas de TI de riesgos nuevos no mapeados anteriormente: "¿Si llegara a ocurrir (el evento de TI), cuanto podría llegar a ser la pérdida media?"
- Impacto medio (escenario mínimo): Horas-hombre: Se necesita consultar las horas incurridas de cada uno de los integrantes involucrados en la resolución del problema junto con su salario bruto. De esta manera se puede llegar a una estimación mínima del costo de resolución. (Horas x Salario por Hora x Cantidad de Personas)

Impacto Máximo:

- Dado el escenario del impacto medio, ¿Cuál podría ser la peor pérdida posible en base a los registros disponibles?"
- Escenario mínimo: Ídem al caso anterior pero contemplando una mayor cantidad de personal asignado u horas.

Una vez construidas las matrices de autoevaluación con los riesgos ya cuantificados, se debe poner en conocimiento de TI aquellos riesgos que fueron mapeados con amenazas.

En este punto es importante destacar qué frecuencia se utiliza con dos fines específicos:

- Para gestión de riesgos, es decir a los efectos de mitigación, seguimiento y reporte. Se puede informar la frecuencia estimada desde la óptica de riesgo operacional o la frecuencia informada para cada amenaza por TI, lo que sea más representativo. En el caso de utilizar la frecuencia de TI, es necesario un cálculo auxiliar previo para asignar la frecuencia de la amenaza a un producto específico.

- Para la matriz de riesgo que es imput del cálculo de capital económico, se debe incorporar las amenazas con la frecuencia de TI y el impacto en el negocio estimado desde la óptica de riesgo operacional.

c. Matriz de riesgo para Capital Económico

Como imput de capital económico, es necesario distinguir dos tipos de riesgos:

- Riesgos Operacionales puros: la preparación de la matriz se mantiene sin modificaciones, es decir se informan Procesos, Subprocesos, Taxonomía de riesgo, impactos y frecuencias.

- Amenazas tecnológicas: es necesario tomar de la matriz de riesgos operacionales las amenazas que mapean con los mismos y eliminarlos de la matriz mencionada ut supra. En cambio, se deben tomar las amenazas identificadas y generar la matriz de sistemas con la frecuencia que surge del análisis de TI y sumarizar los impactos en el negocio de riesgo operacional, teniendo en cuenta si son riesgos dependientes o independientes.

Para ejemplificar el armado de matrices se presente la siguiente sucesión de tablas:

Tabla 7 - Inventario de Amenazas de TI

Amenaza	Frecuencia
Amenaza 1	10
Amenaza 2	128
Amenaza 3	30

Tabla 8 - Matriz de Riesgos para gestión de RO

PRODUCTO	PROCESO	SUBPROCESO	Taxonomía	Factor de Riesgo	Amenaza	Frec. Media	Frec .Máxima	Impacto medio	Impacto Máximo
Producto 1	Proceso 1	Subproceso 1	Taxonomía 1	x1		10	2	1500	150000
Producto 1	Proceso 1	Subproceso 1	Taxonomía 2	x2	Amenaza 1	1	0.5	8500	75000
Producto 1	Proceso 1	Subproceso 2	Taxonomía 3	x3	Amenaza 2	200	30	100	3400
Producto 1	Proceso 2	Subproceso 1	Taxonomía 4	x4	Amenaza 1	20	8	18000	260000
Producto 1	Proceso 2	Subproceso 1	Taxonomía 5	x5		2	1	4300	9000

Tabla 9 - Matriz de Riesgos Operacionales para Capital Económico

PRODUCTO	PROCESO	SUBPROCESO	Taxonomía	Factor de Riesgo	Frec Media	Frec Máxima	Impacto medio	Impacto Máximo
Producto 1	Proceso 1	Subproceso 1	Taxonomía 1	x1	10	2	1500	150000
Producto 1	Proceso 2	Subproceso 1	Taxonomía 5	x5	2	1	4300	9000

Tabla 10 - Matriz de Riesgos Tecnológicos para Capital Económico

PRODUCTO	PROCESO	SUBPROCESO	Taxonomía	Factor de Riesgo	Frec Media	Frec Máxima	Impacto medio	Impacto Máximo
Sistemas	Sistemas	Sistemas	Sistemas	Amenaza 1	10	10	26500	335000
Sistemas	Sistemas	Sistemas	Sistemas	Amenaza 2	128	128	100	3400

b) Mejora de comunicación a través de un circuito estandarizado.

Para darle un marco formal de ejecución de la identificación y evaluación de riesgos se plantea el siguiente esquema de comunicación interna a soportar por la herramienta de ERM (Electronic Record Management). La principal ventaja de la utilización del circuito a plantear es la posibilidad de hacer el seguimiento del tiempo usado para los subprocesos antes mencionados, es decir, utilizar el indicador de gestión “Tiempo de ciclo” (para mayor detalle, consultar C. Trabajo de Campo, Capítulo 2: Aplicación de la Metodología, 2.4. Mediciones y controles).

El esquema de comunicación se define de la siguiente manera:

Tabla 11 Circuito de Comunicación Formal

ERM - Gestión de Riesgos Operacionales				
Identificación y evaluación de riesgos operacionales				
nº	**Descripción**	**Origen del requerimiento**	**Destinatario del requerimiento**	**Detalle**
1	Inicio de Identificación y Evaluación de Riesgos	Analista de Riesgo Operacional	Gerente de Unidad Organizacional en estudio	Se requiere la apertura del mapeo de riesgos. Se adjunta la documentación pertinente de disponibilidad anterior(*)
2	Designación de Referente de Riesgo Operacional	Gerente de Unidad Organizacional en estudio	Referente de Riesgo Operacional	Se da la instrucción para comenzar con la identificación y evaluación de riesgos, y empiezan las reuniones de trabajo con los colaboradores de GGIR
Reuniones de trabajo, contacto vía mail, teléfono, para plasmar los riesgos operacionales de la unidad organizativa en los formularios de mapeo de riesgos y de autoevaluación (solo si se detectan nuevos riesgos).				
3	Aprobación de formularios de mapeo de riesgos y autoevaluación	Referente de Riesgo Operacional	Gerente de Unidad Organizacional en estudio	Se elevan los formularios completos para su aprobación y firma
4	Revisión de la información	Gerente de Unidad Organizacional en estudio	Analista de Riesgo Operacional	Se verifica la correcta integración de los formularios, firma los formularios y adjunta los mismos al expediente
5	Aceptación de la información	Analista de Riesgo Operacional	Jefe de Departamento de Riesgo Operacional	Se analiza la información recibida, si cumple con la normativa interna de Riesgo Operacional, y lo eleva a su superior.
6	Toma conocimiento	Jefe de Departamento de Riesgo Operacional	Gerente de GGIR	Se eleva la información de lo actuado, adjuntando los formularios generados.

7	Comunicación al Gerente/ Subgerente General	Gerente de GGIR	Gerente/ Subgerente General	Se eleva la información de lo actuado, a la Gerencia o Subgerencia General a la cual pertenece la unidad organizativa abordada, adjuntando los formularios generados.

(*) Incluye: Formulario de mapeo de riesgos operaciones anteriores, formulario de mapeo actualizado, formulario de autoevaluación de riesgos, observaciones de auditoría interna, asientos contables de pase a pérdida con origen en riesgos operacionales, otra información pertinente.

El esquema desarrollado en el apartado anterior solo contiene lo referido a la comunicación formal contenida en la herramienta ERM. Por otro lado se reconoce el desarrollo de comunicación informal (mails, llamados telefónicos y reuniones), que debe incluirse en manual de procedimiento para dar un marco de gestión visible, que pueda utilizarse, por ejemplo, como prueba de auditorías.

c) Modificación de criterios para la cuantificación de riesgos.

Del análisis de los manuales de procedimiento previos a las modificaciones propuestas y de los formularios de autoevaluación, se concluyó que en la evaluación de los riesgos, los valores informados hacían foco en el riesgo inherente. Para mejorar la gestión de los riesgos, homogenizar la base de riesgos, y alinear los objetivos de gestión con las salidas de capital económico, se propone una modificación en la manera de cuantificar riesgos (ya sea relacionado a amenazas tecnológicas o no).

Esta modificación se plasma en el formulario de mapa de riesgos y posteriormente en el sistema de administración de riesgos (SARO).

Durante el proceso de evaluación de riesgos se propone:

- Incorporar el parámetro de frecuencia máxima: Número de veces que se espera que ocurra la pérdida al año en relación al escenario de máximo impacto.
- Incorporar Clasificaciones de taxonomía nivel 2 y 3 del BCRA de la Com A 4904.

- La gestión de riesgos debe realizarse de acuerdo a localización del riesgo en las matrices de Pérdida Esperada Media y Pérdida Esperada Máxima con respecto a la frecuencia media.

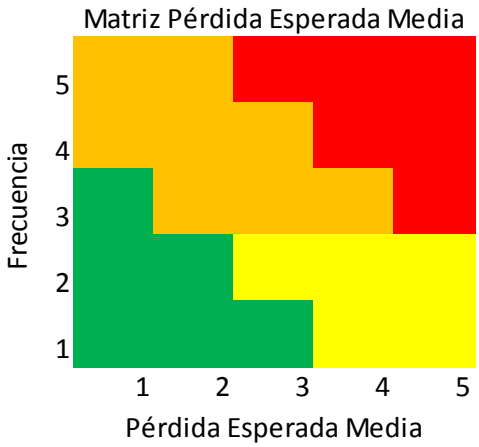


Ilustración 12 Matriz de Pérdida Esperada Media

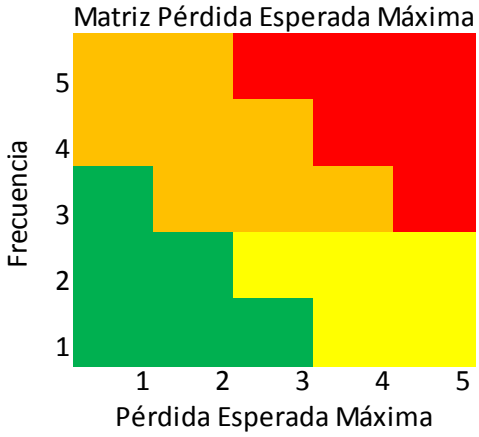


Ilustración 13 Matriz Pérdida Esperada Máxima

De esta manera, al completar los datos cuantitativos de Impacto Medio por Evento, Impacto Máximo por Evento, Frecuencia Media y Frecuencia Máxima, se calculan:

- Pérdida Esperada Media= Frecuencia Media x Impacto Medio por Evento.
- Pérdida Esperada Máxima = {(Frecuencia Media – Frecuencia Máxima) x Impacto Medio por Evento } + (Frecuencia Máxima x Impacto Máximo por Evento)

Se plantea la siguiente tabla de conversión para las Pérdidas Esperadas:

Tabla 12 Conversión Pérdidas Esperadas

	Pérdida Esperada en $	
Impacto	Desde	Hasta
1	$ 0	$ 500,000
2	$ 500,001	$ 1,000,000
3	$ 1,000,001	$ 1,750,000
4	$ 1,750,001	$ 2,750,000
5	$ 2,750,001	

La tabla de conversión de frecuencias media no se modifica.

Con la nueva cuantificación, se designa para cada riesgo un valor de exposición al riesgo según la ubicación de las matrices antes referenciadas, presentándose las siguientes combinaciones de valoración que deben guiar las acciones sobre el riesgo.

Tabla 13 Valoración y acciones sobre riesgos

P. E. Media	P. E. Máxima	Gr.	Acciones sobre Riesgo
BAJA	BAJA	1	Riesgo aceptado, seguimiento anual.
BAJA	MEDIA		
BAJA	ALTA	2	Riesgo con seguimiento semestral. Plan de mitigación con foco en las pérdidas, ejemplo autorizaciones por monto de operación.
MEDIA	MEDIA		
BAJA	MUY ALTA	3	Riesgo con seguimiento anual. Transferir riesgo, ejemplo contratación de seguros.
ALTA	ALTA	4	Riesgo con seguimiento semestral. Plan de mitigación con foco en la frecuencia de ocurrencia, ejemplo muestreos aleatorios sobre operaciones.
ALTA	MUY ALTA		
MUY ALTA	MUY ALTA	5	Requiere un Plan de Mitigación Inmediato. Desarrollo de indicadores con seguimiento mensual.

Todos los cambios desarrollados, se introducen en los formularios de Mapeo de Riesgos (ANEXO VI) y Autoevaluación de Riesgos (ANEXO VII).

La aplicación del nuevo criterio descripto, permitirá ajustar las acciones sobre los riesgos, y alinear los esfuerzos de gestión con los esfuerzos de capital (alocación de capital económico por riesgo operacional).

2.4. Mediciones y controles

A partir del análisis del proceso actual se ha observado que no existen medidas de eficiencia y eficacia del proceso. Por esto mismos que se busca implementar determinados indicadores para monitorear la gestión. La finalidad de estos indicadores es detectar desvíos en la gestión y al mismo tiempo definir las acciones a activar ante estos resultados no esperados. La aplicación sistemática del ejercicio permite la mejora continua del proceso.

Indicador I

Denominación	**Tiempo de ciclo (Identificación y evaluación)**
Proceso	Gestión de Riesgos Operacionales
Subprocesos	Identificación y Evaluación de Riesgos
Descripción	Medición del tiempo promedio de finalización de mapeo de proceso y riesgos operacionales por unidad organizacional
Objetivo	Medir el tiempo para la identificación y evaluación de riesgos operacionales en una unidad organizativa
Unidad de medida	Día
Cálculo	Diferencia entre la fecha de cierre del ERM (Electronic Record Manager) y la fecha de inicio del mismo
Fuente de datos	Expediente Electrónico de cada unidad organizativa
Estándar a alcanzar	7 días
Frecuencia de medición	Trimestral
Desvío aceptable	+30%
Acciones Correctivas	Intervención de Gerente de GIR ante responsable de unidad organizativa a mapear

Indicador II

Denominación	Nivel de integración con riesgo tecnológico
Proceso	Gestión de Riesgos Operacionales
Subprocesos	Identificación y Evaluación de Riesgos
Descripción	Medición del porcentaje de riesgos operacionales relevados incluyendo riesgos tecnológicos respecto a los riesgos totales relevados en un momento dado.
Objetivo	Medir el avance de la integración de riesgos operacionales y tecnológicos
Unidad de medida	%
Cálculo	Cociente entre cantidad de riesgos relevados con la la nueva metodología y la cantidad de riesgos totales
Fuente de datos	SARO - Reporte de riesgos por procesos
Estandar a alcanzar	100% en un año
Frecuencia de medición	Trimestral
Desvío aceptable	-20%
Acciones Correctivas	Análisis de soporte externo Modificación de asignaciones y prioridades a recursos

Indicador II

Denominación	Nivel de Capital Económico
Proceso	Gestión de Riesgos Operacionales
Subprocesos	Reporte
Descripción	Medición del porcentaje de capital regulatorio por riesgo operacional que representa el capital económico por riesgo operacional.
Objetivo	Medir la gestión de riesgo operacional (alcance a nivel entidad) en relación al capital regulatorio por riesgo operacional. Medida de benchmark del alcance de la gestión y calidad de análisis.
Unidad de medida	%
Cálculo	Cociente entre capital económico por riesgo operacional y capital regulatorio por riesgo operacional
Fuente de datos	Informe de Autoevaluación de Capital - Régimen de Capital Regulatorio (ambos a Diciembre)

Estándar a alcanzar	20% (promedio para entidades financieras de similar estructura y negocio)
Frecuencia de medición	Anual (a Diciembre)
Desvío aceptable	-30%
Acciones Correctivas	Exteriorización antes Comité de GIR

Durante la ejecución de los subprocesos de Identificación y evaluación se pueden cometer los siguientes errores:

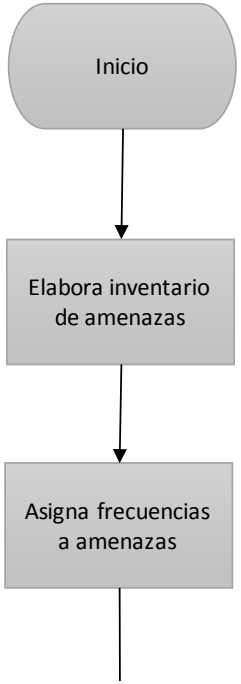
- Falta de integración de riesgos operaciones y tecnológicos: Ante la identificación de un riesgo operacional relacionado a una amenaza tecnológica, esta relación debe quedar plasmada en el mapeo de riesgos.
    - Control: incorporar en el formulario de mapeo y en SARO una validación que ante la selección de una taxonomía de riesgo vinculada a TI muestre una alerta para indicar la amenaza relacionada.
- Inconsistencia en datos de frecuencia media máxima, impacto medio y máximo.
    - Control: incorporar en el formulario de mapeo y en SARO una validación sobre los valores ingresados.
- Errores en la carga de mapeos en SARO. Luego de cerrados los ERMs con la documentación completa, los procesos, subprocesos, riesgos y sus valoraciones deben ser cargados en SARO. En este momento pueden existir errores de transcripción.
    - Control: incorporar en el flujo de actividades un control cruzado entre el analista junior y el analista senior para verificar la correcta incorporación de datos.

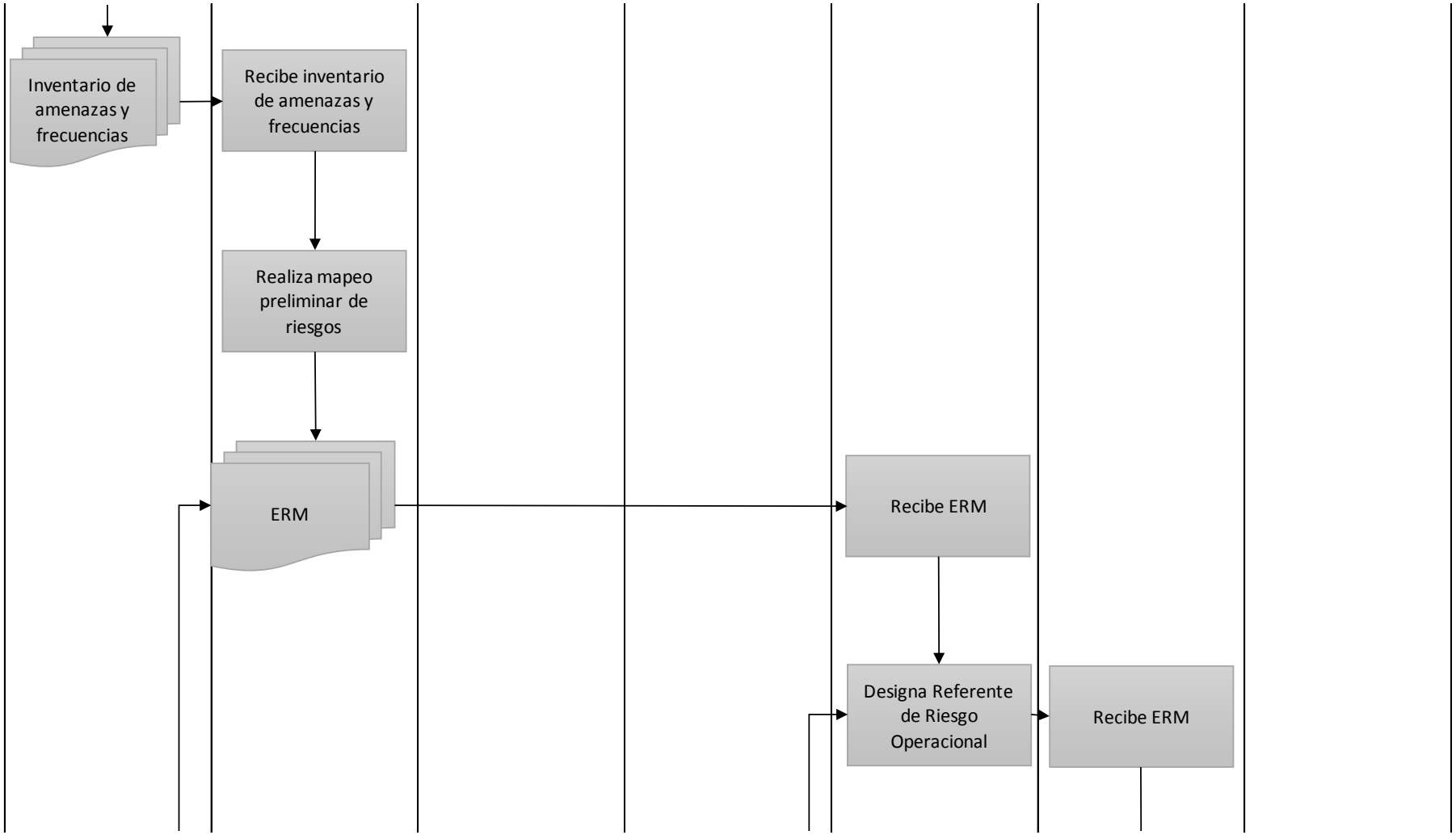
2.5. Implementación

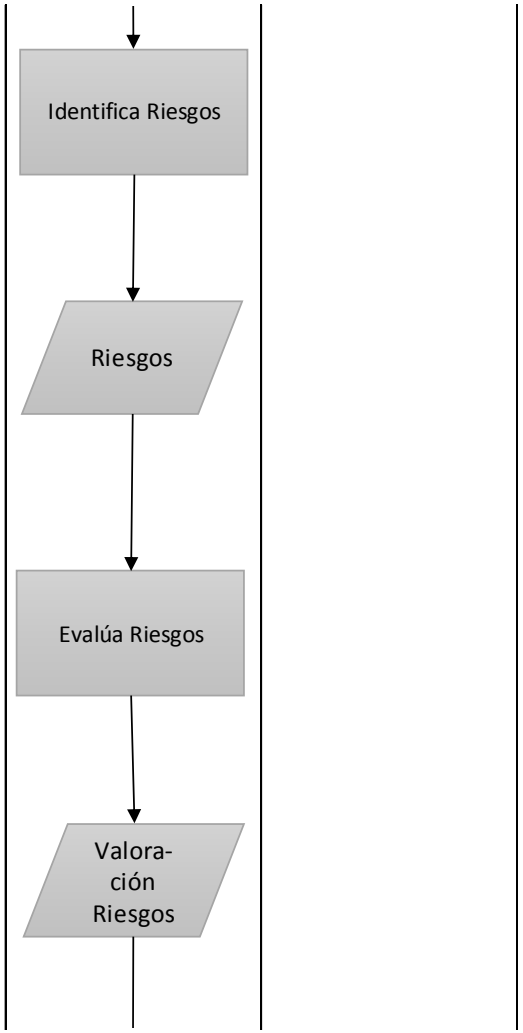
La incorporación de las mejoras desarrolladas en los puntos anteriores, permite obtener el nuevo diagrama de flujo del proceso de gestión de riesgo operacional,

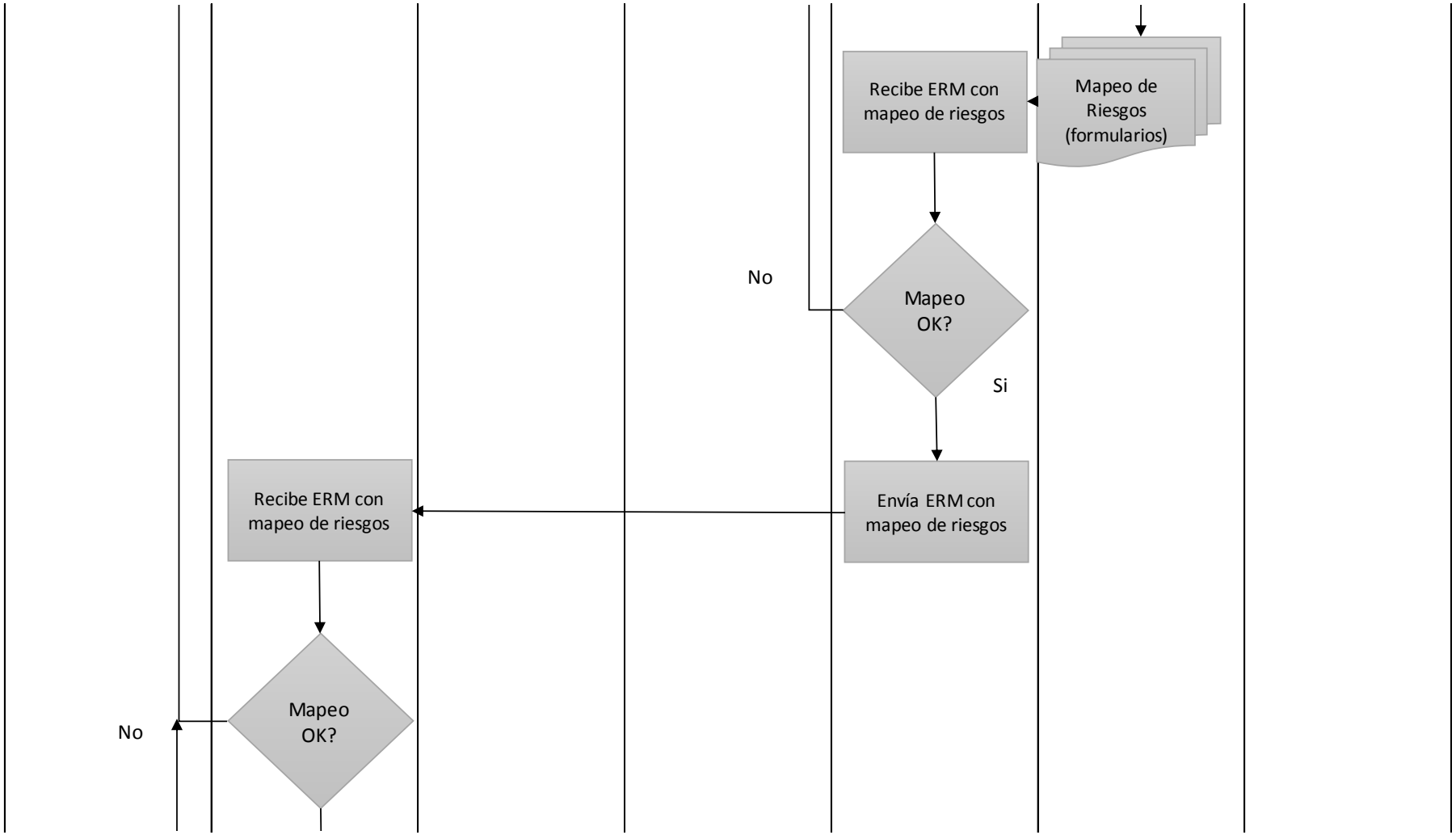
puntualmente en lo referido a la identificación y cuantificación de riesgos operacionales considerando además los tecnológicos.

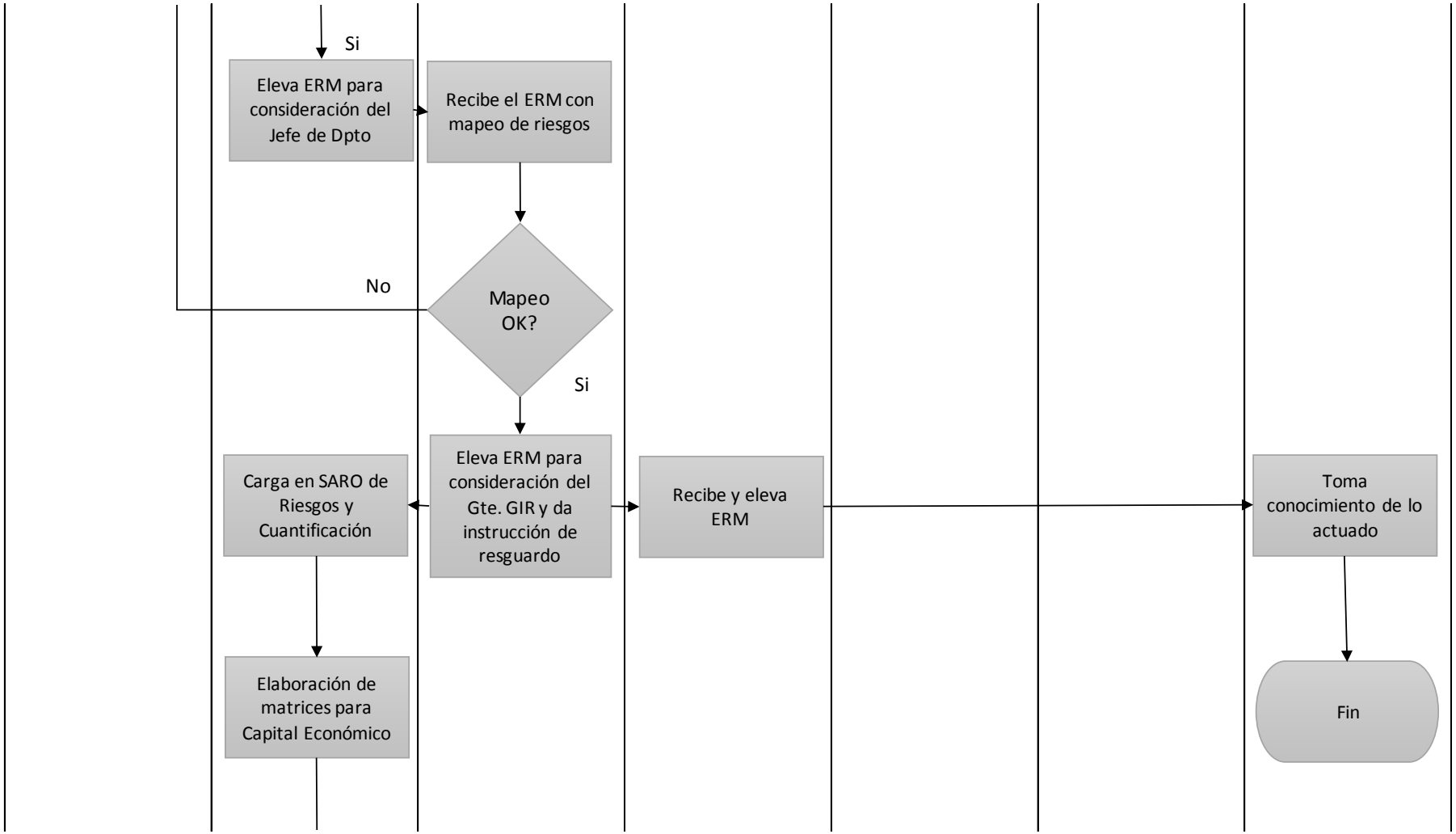
Ilustración 14 Flujograma Mapeo de Riesgos - Fuente: elaboración propia.

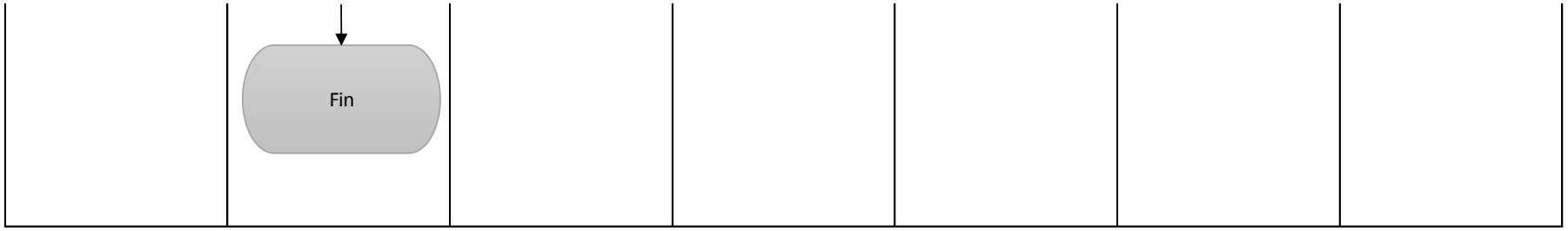
Analista de Gerencia de Protección de Activos de la Información	Analista Gerencia de Gestión Integral de Riesgo	Jefe de Departamento Gerencia de Gestión Integral de Riesgo	Gerente de Gerencia de Gestión Integral de Riesgo	Gerente de la Unidad Organizativa	Referente RO de la Unidad Organizativa	Gerente/ Sub Gerente General de la Unidad Organizativa
						


Inventario de amenazas y frecuencias
Recibe inventario de amenazas y frecuencias
Realiza mapeo preliminar de riesgos
ERM
Recibe ERM
Designa Referente de Riesgo Operacional
Recibe ERM


Identifica Riesgos
Riesgos
Evalúa Riesgos
Valora-
ción
Riesgos


Recibe ERM con mapeo de riesgos
Mapeo de Riesgos (formularios)
No
Mapeo OK?
Si
Recibe ERM con mapeo de riesgos
Envía ERM con mapeo de riesgos
Mapeo OK?
No


Si
Eleva ERM para consideración del Jefe de Dpto
Recibe el ERM con mapeo de riesgos
No
Mapeo OK?
Si
Carga en SARO de Riesgos y Cuantificación
Eleva ERM para consideración del Gte. GIR y da instrucción de resguardo
Recibe y eleva ERM
Toma conocimiento de lo actuado
Elaboración de matrices para Capital Económico
Fin


Fin

Capítulo 3: Aplicación sobre producto de Plazo Fijo

En el presente capítulo se muestra la aplicación real de la mejora de proceso de gestión de riesgos operacionales, puntualmente en lo que respecta a la identificación y evaluación de riesgos en el producto de Plazo Fijo, incluyendo los riesgos tecnológicos, y tomando en cuenta los nuevos criterios de cuantificación.

Previo al mapeo de riesgos del producto Plazo Fijo, se obtuvo la matriz de amenazas de tecnológicas[8].

Tabla 14 Inventario de Amenazas de TI

Grupo de amenazas	Amenazas TI	Frec. Global
Errores/ Falencias/ Fallas de los sistemas que puedan afectar la operatoria directa	Errores de procesamiento o de cálculo	8
	Secuencia de ejecución de procesos inadecuada	11
	Falencias de integración por fallas o ausencias de interfaces	23
	Performance insuficiente	8
	Interrupción del procesamiento de datos	11
Inconvenientes con el resguardo/mantenimiento/ ingreso/egreso de Documentación dentro de las Bases de datos	Datos históricos en formatos no compatibles	12
	Procedimientos deficientes para copias de seguridad y recuperación de información	14
	Degradación de los soportes de copias de respaldo de la información	14
Inconvenientes en el mantenimiento de la aplicación o hardware	Falencias de mantenimiento de la aplicación	7
	Mantenimiento de la configuración/parametrización	28
	Falencias de mantenimiento del hardware	7
	Condiciones inadecuadas de temperatura y/o humedad	7
	Falencias de mantenimiento de la aplicación (VM)	8
	Falencias de mantenimiento de la plataforma (GVM)	7
	Falencias de mantenimiento de los dispositivos de telecomunicaciones	7
Inconvenientes propios de TI	Falencias en el tratamiento de incidentes y anomalías de la aplicación	30
	Cambios no autorizados a programas	17
	Falta de correspondencia entre programas fuentes y ejecutables	30
	Pérdida de programas fuentes	21
	Cambios no autorizados a la plataforma	17

[8] Por tratarse de información sensible, se han modificado los valores de la tabla.

	Incompatibilidad con otros activos de información	14
	Contaminación mecánica o electromagnética	14
	Corte de suministro eléctrico	17
	Cambios no autorizados al hardware	17
	Errores de Instalación/Configuración de los administradores	17
	Falencias en el tratamiento de incidentes y anomalías de la plataforma	17
	Emanaciones electromagnéticas	15
	Responsabilidades no definidas para este canal electrónica	32
	Riesgos no analizados para este canal electrónico	17
	Falta de Trazabilidad de la información cursada por este canal	17
	Interrupción del servicio del canal electrónico	17
	Errores de Configuración de los administradores de la red	17
	Falencias en el tratamiento de incidentes y anomalías de la red	17
	Ancho de banda insuficiente	17
	Cambios no autorizados a los dispositivos de telecomunicaciones	18
Inconvenientes relacionados a la vulneración de jerarquías entre usuarios dentro del banco	Pérdida de programas fuentes	9
	Superposición de funciones incompatibles en usuario(s)	12
	Alteración de la configuración/parametrización	5
	Uso de recursos del hardware no autorizados	27
	Cambios no autorizados al canal	5
	Cambios no autorizados a la plataforma (GVM)	5
	Cambios no autorizados a programas (VM)	5
	Uso de recursos de la plataforma no autorizados (GVM)	27
	Acceso remotos no autorizados	5
Errores de operación de los usuarios	Errores de operación de los usuarios	30
	Introducción de información incorrecta	28
	Errores de operación de los administradores	14
Inconvenientes relacionados a Ataques Externos (Fraudes, robos etc).	Acceso no autorizado a la información	7
	Suplantación de la identidad del usuario	7
	Uso de recursos de la plataforma no autorizados	24
	Acceso no autorizado a la información soportada por el software de base	24
	Introducción/Difusión de software malicioso	7
	Difusión de información no autorizada	4
	Interceptación de información	7
	Robo virtual	7
	Ataque destructivo	7

	Robo	7
	Interceptación de información (Sniffing)	7
	Suplantación de identidad (Spoofing)	4
	Introducción / Difusión	4

Además del inventario de amenazas, fue necesario identificar aquellas taxonomías de riesgo operacional que se corresponden con riesgo tecnológico, obteniendo el siguiente listado:

Tabla 15 Taxonomías de RO que mapean con amenazas de TI

Tipos de Eventos (N1)	Categorías (N2)	Taxonomías (N3)	Mapea con TI?
1. Fraude interno	1.1. Actividades no autorizadas	Ingreso no autorizado o con niveles excesivos a los sistemas de información	SI
		Asignación de accesos a los sistemas de información con capacidades que exceden la definición funcional	SI
2. Fraude externo	2.2. Seguridad de los sistemas	Daño por intromisión en los sistemas informáticos	SI
		Robo de información	SI
		Inadecuada configuración en la infraestructura tecnológica para servicios externos	SI
		Escasa protección de malware	SI
4. Clientes, productos y prácticas empresariales	4.1. Adecuación, divulgación de información y confianza	Inadecuadas prácticas en la implementación de los mecanismos de guarda de confidencialidad para los datos sensitivos y/o en tránsito	SI
	4.3. Productos defectuosos	Falta de protección o inadecuada implementación en las prestaciones a los clientes por canales tecnológicos (ATM, Internet, Celular, etc)	SI
5. Daños a activos materiales	5.1. Desastres y otros acontecimientos	Pérdidas por fallas en la infraestructura tecnológica	SI
		Alteraciones en las bases de datos por inadecuada configuración en la seguridad	SI
6. Incidencias en el negocio y fallas tecnológicas	6.1. Sistemas	Fallas en la infraestructura tecnológica	SI
		Fallas en los sistemas operativos	SI
		Fallas en los sistemas de información	SI
		Problemas y/o inadecuada gestión en las telecomunicaciones	SI
		Interrupción en la prestación de servicios públicos	SI

		Interrupción en la operatoria de los canales de servicios (ATM, Internet, Celular, etc)	SI
7. Ejecución, gestión y finalización de procesos	7.1. Recepción, ejecución y mantenimiento de operaciones	Errores de validación en integridad en la introducción de datos, mantenimiento o descarga de datos	SI
		Ejecución errónea de modelos / sistemas	SI
		Fallas por inadecuado control de correlación en el procesamiento de sistemas	SI
		Fallas en la distribución de los datos o información generada	SI
	7.2. Seguimiento y presentación de informes	Fallas, inadecuación o carencias en el registro de las actividades en la infraestructura tecnológica para el procesamiento de datos	SI
		Falta inadecuación o carencias en el registro de las actividades de los sistemas de información	SI
	7.4. Gestión de cuentas de clientes	Acceso no autorizado a cuentas de clientes	SI
		Inadecuada configuración en los accesos en los sistemas de información	SI

Posteriormente, en trabajo conjunto de las gerencias involucradas se obtuvo el mapa de riesgos del producto Plazo Fijo[9]:

[9] Por la sensibilidad de los datos, se han cambiado valores de frecuencias e impactos, al mismo tiempo que cierta información permanece oculta.

Gerencias Operaciones y Producto Individuo - Fecha de Mapeo: 20/09/2016

Linea	Producto	Proceso	Subproceso	Según "A" 4904			Riesgo Declarado	Escenario/ Controles y Mitigantes / Observaciones	Ef. Mitigante	Riesgo Medio	Riesgo Max	Riesgo Residual - Anual				Prov. de Serv.	% de Act. cubre	RTI	Grupo Amenaza	Amenza
				N1	N2	N3						Frec. Prom.	Frec. Max.	Impacto Prom. por Evento	Impacto Max. por Evento					
BANCA MINORISTA	PASIVAS - PLAZOS FIJOS	ALTA DE CUENTA Y DE CERTIFICADO	ALTA DE PLAZO FIJO - TRADICIONAL	Ejecución, gestión y finalización de procesos	Aceptación de clientes y documentación	Documentos inexistentes / incompletos	Factor de riesgo I	Sin descripción	2	BAJO	BAJO	14	1	$ 20,000	$ 130,000	N/A	N/A	#N/A		
				Ejecución, gestión y finalización de procesos	Aceptación de clientes y documentación	Errores por parte de la Entidad vinculados a la gestión de cuentas de clientes	Factor de riesgo II	Sin descripción	3	MEDIO	MEDIO	11	1	$ 110,000	$ 325,000	N/A	N/A	#N/A		
				Ejecución, gestión y finalización de procesos	Gestión de cuentas de clientes	Registros incorrectos de clientes (con generación de pérdidas).	Factor de riesgo III	Sin descripción	3	MEDIO	MEDIO	10	1	$ 156,000	$ 10,520,000	N/A	N/A	#N/A		

		ALTA DE CUENTA Y DE CERTIFICADO	ALTA DE PLAZO FIJO POR INTERNA	Ejecución, gestión y finalización de procesos	Recepción, Ejecución y Mantenimiento de Operaciones	Errores de validación en integridad en la introducción de datos, mantenimiento o descarga de datos	Factor de riesgo IV	Sin descripción	**2**	BAJO	BAJO	8	0.5	$ 5,700	$ 38,450	N/A	N/A	SI	Errores de operación de los usuarios	Introducción de información incorrecta
				6. Incidencias en el negocio y fallas tecnológicas	6.1. Sistemas	Fallas en los sistemas de información	Factor de riesgo V	Sin descripción	**2**	BAJO	BAJO	12	0.2	$ 6,850	$ 68,000	N/A	N/A	SI	Inconvenientes en el mantenimiento de la aplicación o hardware	Mantenimiento de la configuración/ parametrización
			LINK (POR ATM O HOMEBANKING)	6. Incidencias en el negocio y fallas tecnológicas	6.1. Sistemas	Problemas y/o inadecuada gestión en las telecomunicaciones	Factor de riesgo VI	Sin descripción	**3**	BAJO	BAJO	1	0.5	$ 91,050	$ 910,500	N/A	N/A	SI	Errores/ Falencias/ Fallas de los sistemas que puedan afectar la operatoria directa	Errores de procesamiento o de cálculo
		CONTABILIZACION	SALDOS Y PROCESOS	Ejecución, gestión y finalización de procesos	7.1. Recepción, ejecución y mantenimiento de operaciones	Fallas por inadecuado control de correlación en el procesamiento de sistemas	Factor de riesgo VII	Sin descripción	**4**	ALTO	ALTO	360	4	$ 875	$ 2,690	N/A	N/A	SI	Errores/ Fallas/ Fallas de los sistemas que puedan afectar la operatoria directa	Performance insuficiente

DEFINICIONES COMERCIALES	SOPORTE TECNOLÓGICO	Fraude Interno	Actividades no autorizadas	Asignación de accesos a los sistemas de información con capacidades que excedeb la definicion funcional	Factor de riesgo XVII	Sin descripción	**1**	BAJO	BAJO	0.2	0.1	$ 5,960	$ 62,530	N/A	N/A	SI	7. Inconvenientes relacionados a Ataques Externos (Fraudes, robos etc).	Acceso no autorizado a la información
GENERACION NOTIFICACION CUENTA INMOVILIZADA	PLAZO FIJO INMOVILIZADO	Ejecución, gestión y finalización de procesos	Recepción, Ejecución y Mantenimiento de Operaciones	Incumplimiento de plazos o responsabilidades	Factor de riesgo VIII	Sin descripción	**5**	ALTO	ALTO	365	1.25	$ 75	$ 180	N/A	N/A	#N/A		

OPERACIONES CENTRALIZADAS DE PLAZO FIJO	ALTAS Y BAJAS DE PLAZO FIJO	Ejecución, gestión y finalización de procesos	Recepción, Ejecución y Mantenimiento de Operaciones	Errores de validación en integridad en la introducción de datos, mantenimiento o descarga de datos	Factor de riesgo IX	Sin descripción	**2**	BAJO	BAJO	1	0.5	$ 91,000	$ 610,500	N/A	N/A	SI	Errores de operación de los usuarios	Introducción de información incorrecta
	ALTAS Y BAJAS DE PLAZO FIJO LINK	Ejecución, gestión y finalización de procesos	Recepción, Ejecución y Mantenimiento de Operaciones	Fallas por inadecuado control de correlación en el procesamiento de sistemas	Factor de riesgo X	Sin descripción	**2**	BAJO	BAJO	1	0.5	$ 2,450	$ 20,500	N/A	N/A	SI	Errores de operación de los usuarios	Introducción de información incorrecta

PAGO DE CERTIFICADO DE PLAZO FIJO	AUTORIZACION DE PAGO	Ejecución, gestión y finalización de procesos	Recepción, Ejecución y Mantenimiento de Operaciones	Errores de validación en integridad en la introducción de datos, mantenimiento o descarga de datos	Factor de riesgo XI	Sin descripción	**2**	BAJO	BAJO	0.5	0.25	$ 140,000	$ 1,890,000	N/A	N/A	SI	Inconvenientes en el mantenimiento de la aplicación o hardware	Mantenimiento de la configuración/ parametrización
	PAGO DE PF EN SUCURSAL ORIGEN	Ejecución, gestión y finalización de procesos	Recepción, Ejecución y Mantenimiento de Operaciones	Falta de Control y/o autorización	Factor de riesgo XII	Sin descripción	**1**	BAJO	BAJO	0.5	0.25	$ 148,500	$ 2,011,500	N/A	N/A	#N/A		
		Ejecución, gestión y finalización de procesos	Gestión de cuentas de clientes	Pérdida o daño de activos de clientes por negligencia	Factor de riesgo XV	Sin descripción	**2**	BAJO	BAJO	0.5	0.25	$ 322,080	$ 3,400,600	N/A	N/A	#N/A		
		Fraude Externo	Seguridad en los Sistemas	Daño por intromisión en los sistemas informáticos	Factor de riesgo XVI	Sin descripción	**2**	BAJO	BAJO	0.2	0.1	$ 418,000	$ 2,500,010	N/A	N/A	SI	7. Inconvenientes relacionados a Ataques Externos (Fraudes, robos etc).	Acceso no autorizado a la información
		Fraude Interno	Actividades no autorizadas	Ingreso no autorizado o con niveles escesivos a los sistemas de información	Factor de riesgo XVIII	Sin descripción	**1**	BAJO	BAJO	0.2	0.1	$ 95,000	$ 4,800,900	N/A	N/A	SI	7. Inconvenientes relacionados a Ataques Externos (Fraudes, robos etc).	Acceso no autorizado a la información

El análisis de riesgo indica que de los 18 riesgos operacionales sobre el producto de Plazo Fijo, el 61% (11 riesgos) están relacionados a amenazas tecnológicas.

Al mismo tiempo se identifican dos riesgos medios, sobre los cuales se debe realizar un seguimiento semestral, 2 riesgos altos sobre los cuales se debe desarrollar un plan de mitigación y ejecutar el seguimiento de acuerdo a las fechas de avance comprometidas en mismo plan. El resto de los riesgos son bajos y se encuentran aceptados.

En lo que respecta a la integración para capital económico las matrices quedan definidas de la siguiente manera:

Tabla 16 Imput para Capital Económico - Riesgos Operacionales

PRODUCTO	PROCESO	SUBPROCESO	Taxonomía	Factor de Riesgo	Frec Media	Frec Máxima	Impacto medio	Impacto Máximo
PASIVAS - PLAZOS FIJOS	ALTA DE CUENTA Y DE CERTIFICADO	ALTA DE PLAZO FIJO - TRADICIONAL	Documentos inexistentes / incompletos	Factor de riesgo I	14	1	$ 20,000	$ 130,000
PASIVAS - PLAZOS FIJOS	ALTA DE CUENTA Y DE CERTIFICADO	ALTA DE PLAZO FIJO - TRADICIONAL	Errores por parte de la Entidad vinculados a la gestión de cuentas de clientes	Factor de riesgo II	11	1	$ 110,000	$ 325,000
PASIVAS - PLAZOS FIJOS	ALTA DE CUENTA Y DE CERTIFICADO	ALTA DE PLAZO FIJO - TRADICIONAL	Registros incorrectos de clientes (con generación de pérdidas).	Factor de riesgo III	10	1	$ 156,000	$ 10,520,000
PASIVAS - PLAZOS FIJOS	GENERACION NOTIFICACION CUENTA INMOVILIZADA	PLAZO FIJO INMOVILIZADO	Incumplimiento de plazos o responsabilidades	Factor de riesgo VIII	365	1.25	$ 75	$ 180
PASIVAS - PLAZOS FIJOS	PAGO DE CERTIFICADO DE PLAZO FIJO	PAGO DE PF EN SUCURSAL ORIGEN	Falta de Control y/o autorización	Factor de riesgo XII	0.5	0.25	$ 148,500	$ 2,011,500

PASIVAS - PLAZOS FIJOS	PAGO DE CERTIFICADO DE PLAZO FIJO	PAGO DE PF EN SUCURSAL ORIGEN	Pérdida o daño de activos de clientes por negligencia	Factor de riesgo XV	0.5	0.25	$ 322,080	$ 3,400,600
PASIVAS - PLAZOS FIJOS	PLAZO FIJO EMBARGADO	PLAZO FIJO EMBARGADO /LEVANTAMIENTO	Falta de Control y/o autorización	Factor de riesgo XIII	0.5	0.25	$ 3,000	$ 1,250,000

Tabla 17 Imput para Capital Económico – Riesgos Tecnológicos

PRODUCTO	PROCESO	SUBPROCESO	Taxonomía	Factor de Riesgo	Frec Media	Frec Máxima	Impacto medio	Impacto Máximo
SISTEMAS	SISTEMAS	SISTEMAS	SISTEMAS	Introducción de información incorrecta	28	28	$ 174,700	$ 1,654,500
SISTEMAS	SISTEMAS	SISTEMAS	SISTEMAS	Mantenimiento de la configuración/ parametrización	28	28	$ 146,850	$ 1,958,000
SISTEMAS	SISTEMAS	SISTEMAS	SISTEMAS	Errores de procesamiento o de cálculo	8	8	$ 91,050	$ 910,500
SISTEMAS	SISTEMAS	SISTEMAS	SISTEMAS	Performance insuficiente	8	8	$ 875	$ 2,690
SISTEMAS	SISTEMAS	SISTEMAS	SISTEMAS	Acceso no autorizado a la información	7	7	$ 518,960	$ 7,363,440

Capítulo 4: Líneas de trabajo adicionales

En la presente sección se mencionan los nuevos proyectos de trabajo que surgen de la mejora de proceso desarrollada hasta este punto, que no son abordados con profundidad en este trabajo de aplicación por estar por fuera del alcance definido previamente.

4.1. Capacitaciones globales y capacitaciones para referentes de riesgo operacional.

El proceso de gestión de riesgos operacionales requiere una evolución cultural en la organización. El mandato de obligatoriedad que impone el organismo de contralor por aceptación de las mejores prácticas de los acuerdos de Basilea, por sí solo no motiva al esfuerzo de la generación de información de calidad para la gestión de riesgos.

Es por este motivo, que se proponen dos líneas de acción para la capacitación de los colaboradores de la institución financiera:

- Capacitación masiva a través de la plataforma de e-learning que dispone la entidad, que tenga como destinatarios a todos los colaboradores. La finalidad de esta capacitación es poner en conocimiento de todos los involucrados en la entidad sobre la existencia de los riesgos operacionales, su marco normativo y origen, y sobre la gestión misma de los riesgos en términos generales.

- Capacitación presencial para referentes de riesgo operacional. Esta capacitación busca informar a detalle la gestión de los riesgos operacionales, para facilitar la identificación y evaluación de riesgos además del seguimiento y mitigación de los mismos. El contacto personal y la posibilidad de evacuar dudas en el momento son ventajas a la hora de lograr un mayor compromiso de los proveedores de información a la Gerencia de Gestión Integral de Riesgos.

Esta recomendación constituye en sí una línea adicional de aplicación, por lo que no será desarrollado a profundidad en el presente trabajo.

4.2. Actualizaciones de manuales involucrados.

Todos los cambios desarrollados hasta este punto, deben ser trasladados a la normativa interna, particularmente en los manuales de procedimientos administrativos de Riesgo Operacional y de Riesgo Tecnológico.

Por la extensión del este trabajo de aplicación, esta mejora se deja planteada como una línea de trabajo adicional. Como guía para la actualización, puntualmente es deseable incluir lo desarrollado en los puntos 1, 3 y 4 de la presente sección además del siguiente

checklist para orientar las acciones de los analistas de riesgo operacional durante el relevamiento preliminar, previo al abordaje de una unidad organizativa para el mapeo de sus riesgos:

I. Verificar que el área a mapear esté incluida en el plan de mapeos del año. Si no se está incluida o si la fecha no coincide con la planeada, plantear la justificación

II. Revisar el Manual Orgánico Funcional para identificar procesos y subprocesos

III. Revisar de mapeos previos para adjuntar al ERM

IV. Revisar observaciones de auditoría e incluirlas en el mapeo anterior como propuesta de actualización.

V. Revisión de los dos últimos Informes de Pérdidas por Riesgo Operacional e incluir en el detalle de los riesgos si tiene eventos recientes.

VI. Revisión de mapeos residuales para identificar si alguno de los riesgos antiguos (sin mayores datos que su descripción) pertenece a la unidad organizativa a mapear.

Al mismo tiempo, el manual debe incluir el diagrama de flujo matricial desarrollado previamente, de los subprocesos de identificación y evaluación de riesgos operacionales y tecnológicos desarrollado previamente.

4.3. Modificación del Manual Funcional Orgánico (MOF).

Dado el alcance del trabajo, el presente punto no será desarrollado en detalle. Sin embargo se plantea la necesidad de que la Gerencia de Organización y Proceso realice una modificación estructural del manual funcional orgánico para que dentro de cada unidad organizativa, definida al nivel que resulte conveniente luego de los análisis pertinentes, tenga funciones relacionadas a la gestión de riesgo operacional.

El manual orgánico funcional es el que determina la estructura formal de la entidad financiera y asigna misiones, funciones, atribuciones, responsabilidades, define las relaciones de autoridades internas, de participación y los entregables de cada puesto predefinido.

Para una ágil concientización respecto a la gestión de riesgos operacionales y para elevar el nivel de compromiso y de respuesta, se propone agregar dentro de los entregables de un área el mapeo de riesgos operacionales con posterior validación de la Gerencia de Gestión Integral de Riesgos.

Puntualmente para la Gerencia de Gestión Integral de riesgo: agregar la función de incluir en el análisis de riesgos a los riesgos tecnológicos considerando los impactos en el negocio de los mismos, en consonancia a lo evaluado por la Gerencia de Protección de Activos de la Información.

A la Gerencia de Protección de Activos de la Información: agregar la función de informar sobre lo actuado respecto a riesgos tecnológicos a la GGIR y prestar colaboración para la incorporación de los mismos a su gestión de riesgos.

4.4. Adecuaciones en el Sistema de Administración de Riesgos Operacionales.

Como consecuencia de los cambios en la gestión de RO, el sistema que la soporta debe adecuarse a fin de simplificar las tareas a ejecutar, y mantener la trazabilidad de datos que son utilizados en los reportes elaborados.

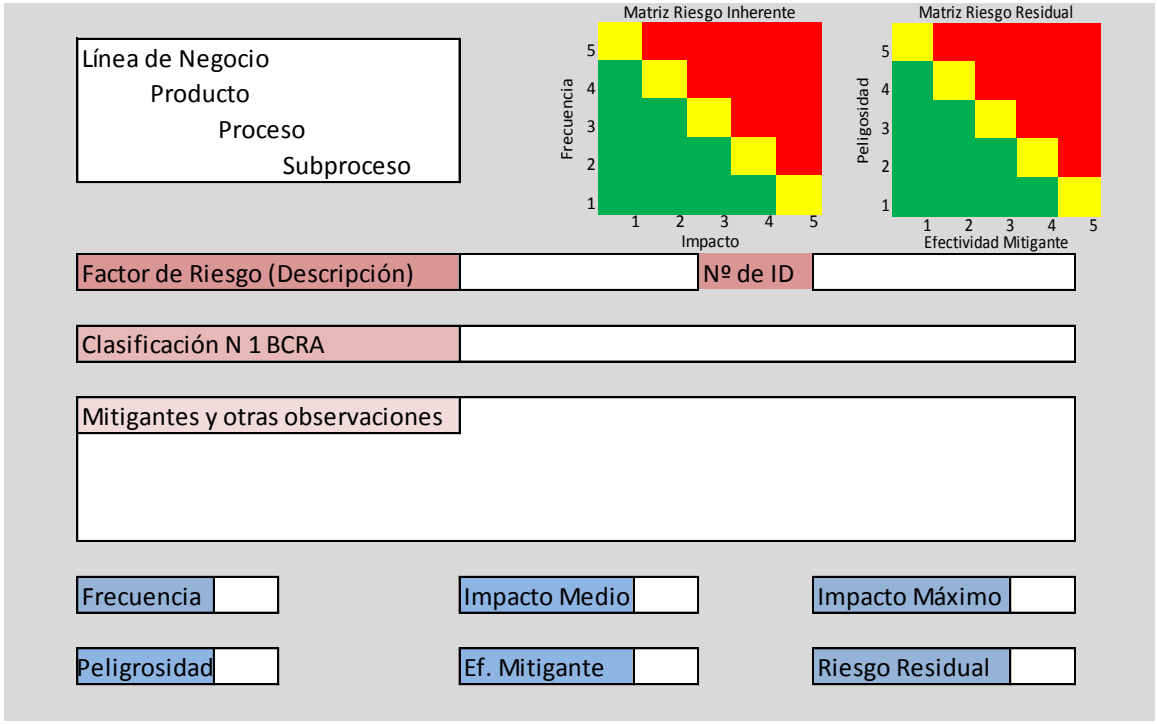
No es objetivo de este trabajo de aplicación desarrollar la especificación funcional de los módulos del sistema interviniente, sin embargo se enumeran a continuación los cambios mínimos a implementar:

- Incorporar campo de Amenaza que se selecciona automáticamente del inventario de amenazas que provee la Gerencia de Protección de Activos de la Información.
- Incorporar campo de Riesgo Dependiente. Posibilidad de cargar el nº de ID interno del riesgo con el que se relaciona de forma dependiente (en el caso de que tenga

una amenaza asociada). Debe existir una validación para que al momento de ingresar el nº de ID, este sea corresponda con un riesgo vigente.

- Incorporar campo de frecuencia máxima.
- Incorporar validación de manera tal que frecuencia máxima sea menor o igual a la frecuencia media.
- Incorporar validación Impacto promedio sea menor o igual que impacto máximo.
- Agregar campos que se completen automáticamente de Pérdida Esperada Media y Pérdida Esperada Máxima. La Pérdida Esperada Media se debe calcular como el producto entre la frecuencia media y el impacto medio. La Pérdida Esperada Máxima se define como la sumatoria entre el producto de la diferencia entre la frecuencia promedio y la máxima por el impacto promedio, más el producto entre la frecuencia máxima y el impacto máximo.
- Agregar validación Pérdida Esperada Media sea menor o igual a la Pérdida Esperada Máxima.
- Incorporar campos de clasificación a nivel 1 y 2 de riesgo operacional que tome automáticamente todo el universo de taxonomías descriptas en la Com. A 4904 del BCRA.
- Incorporar listado de taxonomías operacionales que tienen relación con una amenaza tecnológica, de esta manera se puede desarrollar una validación tal que al cargar un riesgo con una taxonomía relacionada a una amenaza salte un alerta de que debe cargar una amenaza.
- Eliminar la matriz de riesgo inherente.
- Eliminar la matriz de riesgo residual.
- Crear la matriz de pérdida media esperada y frecuencia media.
- Crear la matriz de pérdida máxima esperada y frecuencia media.

Con estas modificaciones propuestas, se tiene como principal objetivo fortalecer el control interno, limitando los errores y desvíos durante la etapa de carga de los riesgos en



el sistema.

Ilustración 15 Pantalla SARO actual

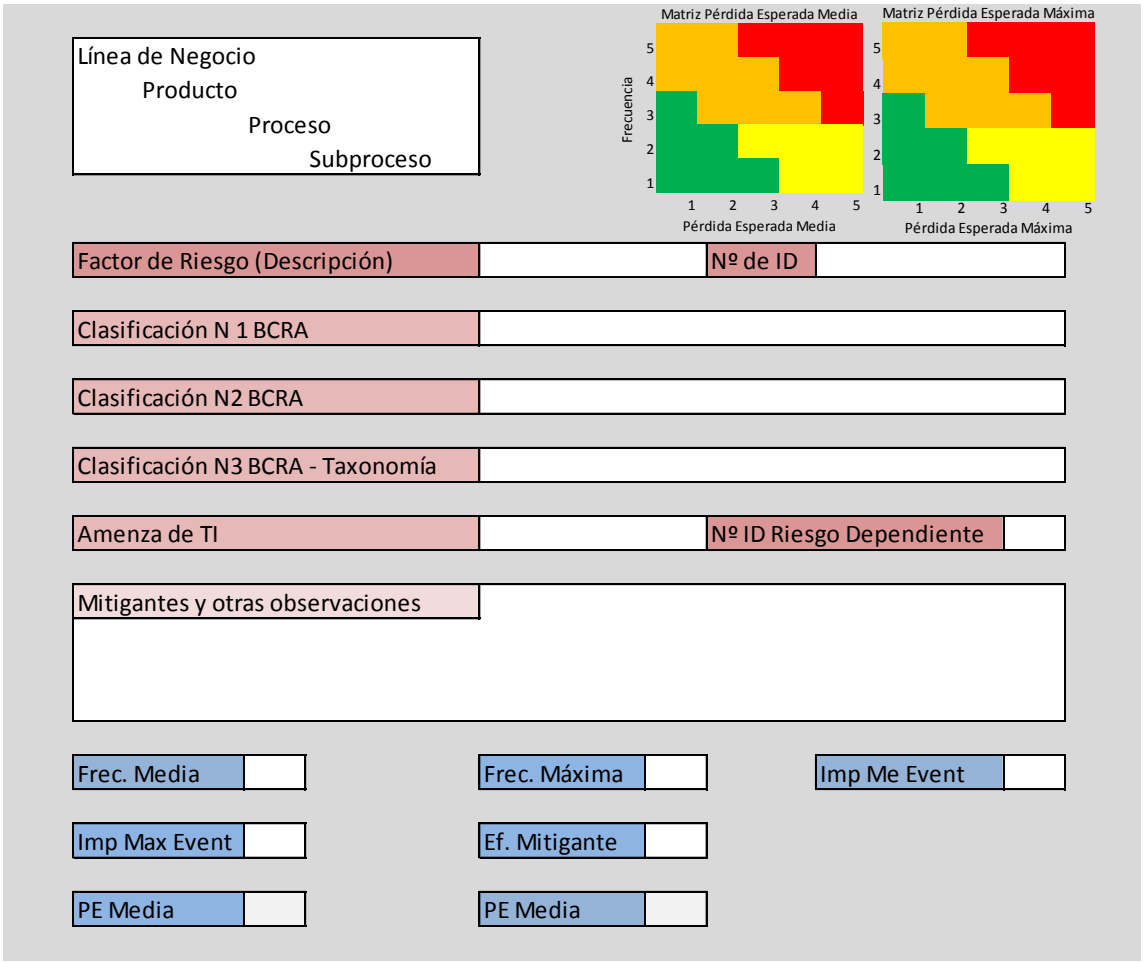


Ilustración 16 Pantalla SARO con Modificaciones

III. CONCLUSIONES

El trabajo final comenzó con el objetivo de mejorar el proceso de gestión de riesgos operacionales, de forma tal que incluyera a los riesgos tecnológicos.

Durante la aplicación de la metodología seleccionada del marco teórico desarrollado, puntualmente durante el diagnóstico del proceso a mejorar, se detectaron otros factores claves a modificar a fin de que el proceso sea eficiente y eficaz.

Entre los aspectos críticos de la gestión de riesgos operacionales se mencionan:

- Proceso incompleto, ya que no incluye los riesgos tecnológicos.
- Demoras prolongadas, por la burocracia, falta de cultura organizacional sobre los riesgos operacionales.
- Criterios de evaluación no uniformes.

Con un enfoque integral sobre el proceso, se desarrollaron tres soluciones integradoras:

- Integración de riesgos operacionales y tecnológicos
- Mejora de comunicación a través de un circuito estandarizado
- Modificación de criterios de cuantificación de riesgos.

En forma adicional, se plantearon cuatro líneas de trabajo complementarias que podrán ser objeto de futuros trabajos de aplicación, siendo estas:

- Capacitaciones globales y para referentes de riesgos
- Actualizaciones de manuales
- Actualización de funciones de unidades organizacionales
- Adecuación al Sistema de Administración de Riesgos Operacionales

Como entregable obtenido a partir del trabajo se destaca el diagrama de flujo matricial, que constituye una herramienta de alta utilidad para los sectores usuarios.

Por otro lado, también es destacable el desarrollo de indicadores para medir la gestión propia de riesgos, el grado de avance en el proyecto de integración y para identificar desvíos de la actividad con las acciones para su corrección.

En lo que respecta a la aplicación de las mejoras en el producto de Plazo Fijo, se obtuvieron los siguientes resultados:

- Se identificaron y cuantificaron 18 riesgos operacionales de los cuales 2 riesgos son medios, sobre los que se deben realizar un seguimiento semestral, 2 riesgos altos sobre los cuales se debe desarrollar un plan de mitigación y ejecutar el seguimiento de acuerdo a las fechas de avance comprometidas en mismo plan. El resto de los riesgos son bajos y se encuentran aceptados.

- El 61% (11 riesgos) están relacionados a amenazas tecnológicas

De estos resultados, se puede inferir que si bien el proceso está controlado y no expuesto a un número significativo de riesgos, existe una alta dependencia a factores tecnológicos que deben ser controlados y monitoreados por expertos del área. Esta información, debe ser tenida en cuenta por la alta gerencia a la hora de asignar prioridades y recursos en el mantenimiento y mejora de productos ofrecidos por la entidad.

Se puede concluir que el proceso ha sido mejorado en sus aspectos principales, de forma tal que los riesgos tecnológicos se encuentran dentro de la gestión de los riesgos operacionales, y al mismo tiempo se han planteado las pautas de trabajo para obtener los mapas de riesgos homogéneos, inclusive con una reducción en los tiempos de ejecución y un consiguiente ahorros de costos.

Por otro lado, el proceso tiene un potencial de mejora a futuro con la implementación de las líneas de acción adicionales y con la culturización de la organización respecto a la gestión de riesgos operacionales.

Queda como principal desafío la aplicación de la metodología aquí descripta en los demás procesos de negocios del Banco SA y sobre la totalidad de los productos ofrecidos a los clientes.

IV. BIBLIOGRAFÍA

Bank for International Settlements. (Enero de 2001). *El Nuevo Acuerdo de Capital de Basilea*. Recuperado el 23 de Mayo de 2016, de El Nuevo Acuerdo de Capital de Basilea: http://www.bis.org/publ/bcbsca03_s.pdf

Bank for International Settlements. (Diciembre de 2010). *Basilea III: Marco regulador global para reforzar los bancos y sistemas bancarios* . Recuperado el 2013 de Mayo de 2016, de Basilea III: Marco regulador global para reforzar los bancos y sistemas bancarios: http://www.bis.org/publ/bcbs189_es.pdf

Bank for International Settlements. (Octubre de 2010). *La respuesta del Comité de Basilea a la crisis financiera: informe al G-20*. Recuperado el 20 de Mayo de 2016, de La respuesta del Comité de Basilea a la crisis financiera: informe al G-20: http://www.bis.org/publ/bcbs179_es.pdf

Bank for International Settlemet. (Junio de 2006). *Convergencia internacional de medidas y normas de Capital*. Recuperado el 23 de Mayo de 2016, de Convergencia internacional de medidas y normas de Capital: http://www.bis.org/publ/bcbs128_es.pdf

BCRA. (2006). Comunicación "A" 4609. *Requisitos mínimos de gestión, implementación y control de los riesgos relacionados tecnología informática y sistemas de información*.

BCRA. (2009). Comunicación "A" 4904. *Régimen Informativo para Supervisión Trimestral / Anual (R.I. - S.) - "Base de datos sobre eventos de Riesgo Operacional"*.

BCRA. (2013). Comunicación "A" 5398. *Lineamientos para la gestión de riesgos en las entidades financieras. Clasificación dedeudores. Previsiones mínimas por riesgo de incobrabilidad.*

BCRA. (s.f.). *Banco Central de la República Argentina*. Recuperado el 02 de 11 de 2016, de http://www.bcra.gov.ar/SistemasFinancierosYdePagos/Entidades_financieras.asp

Dumas, M. (2013). *Fundamentals of Business Process Management.* Springer.

Harrington, J. (1991). *Business Process Improvement.* McGraw Hil.

International Organization for Standardization. (s.f.). *About us: International Organization for Standardization*. Recuperado el 10 de Octubre de 2016, de Sitio web de International Organization for Standardization: http://www.iso.org/iso/home/about.htm

VII. ANEXOS

ANEXO I: MINUTA DE REUNIÓN

FECHA: / /

LUGAR:

OBJETIVOS DE LA REUNIÓN:

- Tema 1
- Tema 2

PARTICIPANTES:

APELLIDO Y NOMBRE	ÁREA / SECTOR

TEMAS TRATADOS:

ANEXO II: ENTREVISTAS SOBRE PROCESOS DE GESTIÓN DE RIESGO OPERACIONAL

Preparación de la Entrevista

1) Posiciones a entrevistar:
   a) Gerente de Gestión Integral de Riesgo
   b) Gerente de Protección de Activos de la información
   c) Jefe de Departamento Riesgo Operacional
   d) Jefe de Departamento Riesgo de TI y Cumplimiento
   e) Analista Riesgo Operacional
   f) Analista Riesgo de TI
2) Cuestionario: Se elabora una estructura de cuestionarios con distintos enfoques de acuerdo a las posiciones a entrevistar. Las preguntas son abiertas por lo que al momento de las mismas se da la posibilidad de repreguntar y de analizar si es necesario indagar sobre un punto en particular que sea de interés.
   a) <u>Destinado a Gerentes:</u>
      i) ¿Existen políticas y lineamientos claros en cuento a la gestión de riesgo en la organización?
      ii) ¿Qué nivel de involucramiento de la alta gerencia con respecto a estas políticas de riesgos se observa?
      iii) ¿Cómo se podría lograr una mayor aprensión de esta política en la alta gerencia?
      iv) ¿Podría describir el proceso de gestión de riesgos operacionales en forma general?
      v) ¿Cuál es el output más relevante del proceso? ¿Se utiliza para la toma de decisiones? ¿A qué nivel?
      vi) ¿Qué nuevas necesidades se detectan que podrían ser satisfechas con una modificación en el proceso?
   b) <u>Jefes</u>

i) ¿Podría describir el proceso de gestión de riesgo operacional? ¿Qué alcance y objetivos plantea? ¿Cuáles son sus límites? ¿Cuáles son los principales clientes?

ii) Además de las políticas y lineamientos generales, ¿existen manuales de riesgo operacional?

iii) En la ejecución del proceso, ¿existe documentación de respaldo de lo actuado? ¿Es completa? ¿La documentación se registra en formularios estandarizados? En caso de ser afirmativo, por favor proveer los formularios que sean utilizados.

iv) ¿Se tienen las herramientas de gestión adecuadas para soportar el proceso? Fundamente su respuesta.

v) Al informar los resultados del proceso, ¿se tienen en claro los objetivos? ¿Cuál es el nivel de interés que se muestra en los destinatarios?

vi) ¿Existen indicadores para medir la eficacia y la eficiencia del proceso? ¿Cuáles son? ¿Podría describirlos?

vii) ¿Qué nivel de compromiso se observa de los colaboradores del área?

c) Analistas

i) ¿Podría describir el proceso de gestión de riesgo operacional? ¿Qué alcance y objetivos plantea? ¿Cuáles son sus límites? ¿Cuáles son los principales clientes?

ii) ¿Cuáles son las herramientas sobre las que se ejecutan las tareas diarias? ¿Son sencillas de utilizar?

iii) Respecto a las políticas, lineamientos generales y manuales, ¿son fáciles de entender? Están a disposición de los involucrados en el proceso?

iv) ¿Qué documentación se maneja durante la ejecución del proceso? ¿Qué papeles de trabajo de utilizan? ¿Estos son redundantes o son necesarios?

3) Tiempo aproximado de entrevista: 1 hs 30 minutos.

4) Lugares de entrevistas:

a) Gerentes: Oficina personal del entrevistado

b) Jefes y analistas: Salas de reuniones reservadas en Banco SA

Salida (output) de las entrevistas

5) Se documentarán los resultados.

6) Se entregará una copia al entrevistado, solicitando su conformación, correcciones o adiciones.

7) Archivar los resultados de la entrevista.

ANEXO III: FORMULARIO DE MAPEO DE RIESGO OPERACIONAL

Gcia - Dpto - Fecha de Mapeo: ___ - ___-201__

Linea	Producto	Proceso	Subproceso	Riesgo Declarado	Impacto	Frecuen.	R.Inherente	Peligros.	Ef. Mitigante	R.Residual	Observaciones / Controles / Mitigantes	Frecuencia Anual (1)	Impacto Prom. Por Año en $	Impacto Máximo por Año en $ (1)	Aud. Interna (AMB)	Indi ca do res	Formula o calculo Umbral	Vinculo con Proveedor	% de Act. que cubre

Las columnas en resaltadas del "Mapa de Riesgo Operacional" se llenan de la siguiente manera:

Columna Frecuencia Anual: De acuerdo a la Tabla de la solapa "TablaConv", se indicará un número dentro del rango “Desde – Hasta”.
Ejemplo: Si el riesgo que se está evaluando puede ocurrir, en caso de fallar los mitigantes 1 y 2 veces al mes, la “Frecuencia Anual” deberá ser un numero entre 12 y 24 (De acuerdo a juicio experto).

Columna Impacto Promedio de eventos ocurridos en el Año en $: Estimación del importe promedio de ocurrencias en un año, en el caso de fallas de los mitigantes. De existir eventos, se debe completar con el promedio de pérdida por evento del último año.

Columna Impacto Máximo en el Año en $: Estimación del importe máximo de pérdida individual que podría ocasionar la materialización de este riesgo, en caso de que los mitigantes fallen, de acuerdo a la tabla de la solapa "TablaConv". (Debe ser mayor al impacto promedio).

Efectividad del Mitigante: De acuerdo a la Tabla de la solapa "TablaConv" y utilizando juicio experto, indicar en escala de 1 a 5, siendo 1 el mitigante más efectivo.

Columna Auditoria Interna (AMB): Si existiera alguna observación de auditoria interna sobre este riesgo, indicar si la observación es de A = Riesgo Alto, M = Riesgo Medio o B = Riesgo Bajo

Columna Indicadores: Se completara únicamente si el riesgo residual esta en Rojo, en ese caso se indicara el nombre del indicador

Columna Fórmula o Cálculo: Se completara únicamente si el riesgo residual esta en Rojo, en ese caso se indicara como está compuesto el Numerador y denominador del indicador de la columna anterior.

Columna Vinculo con Proveedor: Se indicará, si existen, el nombre/s de/los proveedores externos que estén relacionados con ese riesgo.

Columna de % Actividad que cubre: Se Indicará el porcentaje de participación del Proveedor Externo en el proceso que genera el riesgo que se está analizando.

	Impacto Máximo Anual	
Impacto	Desde	Hasta

	Frecuencia Anual	
Frecuencia	Desde	Hasta

1	$ 0	$ 119,999
2	$ 120,000	$ 499,999
3	$ 500,000	$ 999,999
4	$ 1,000,000	$ 9,999,999
5	$ 10,000,000	

1	0.01	0.99
2	1	23.99
3	24	47.99
4	48	119.99
5	120	

ANEXO IV: FORMULARIO DE AUTOEVALUACIÓN DE RIESGO OPERACIONAL

AUTOEVALUACION DE RIESGOS OPERACIONALES

FECHA DE AUTOEVALUACION: ___ / ___/ _____

GERENCIA / SUBGERENCIA:	
LINEA:	
PRODUCTO:	
PROCESO:	
SUBPROCESO:	
Responsable/ Area a la que pertenece:	
Descripcion del Riesgo:	
TIPO DE RIESGO INVOLUCRADO: _____ Según Com. "A" 4904: 1) Fraude, 2) Relaciones laborales, 3) Prácticas con clientes, 4) Productos y negocios, 5) Daños a activos, 6) Alteraciones de la actividad, 7) Ejecución de procesos	
FACTOR, ORIGEN O CAUSA: _____ 1) Políticas y procedimientos, 2) Controles, 3) RRHH, 4) Automatización, 5) Calidad de información, 6) Normas, 7) Supervisión	
CONTROLES QUE SE REALIZAN Y MITIGANTES QUE SE APLICAN (Actuales y a Implementar o sugeridos): (Indique tambien resultados obtenidos)	
NORMAS, SISTEMAS y LISTADOS INVOLUCRADOS (Del Banco y del BCRA):	
SECTORES INVOLUCRADOS:	
IMPACTO: _____ (1 a 5) (Ver tabla de conversión al dorso)	Tiene conocimiento si hubo perdidas contabilizadas a causa de este riesgo? **SI / NO**
FRECUENCIA: _____ (1 a 5) (Ver tabla de conversión al dorso)	
OBSERVACIONES DE AUDITORIA INTERNA (Si hubiera relacionada con este riesgo):	
VINCULACION CON OTROS RIESGOS (de Mercado, de Credito, etc):	

Existen otros sectores involucrados en la generación, propagación o mitigación de este riesgo

Sector **Involucrado**	**Acciones mitigantes y controles realizadas** (De existir, haga referencia a evidencia documental o soporte de sistemas)

Reservado para consideraciones del encuestado

_____

Firma y sello responsable

ANEXO V: FORMULARIO DE PLAN DE MITIGACIÓN

GERENCIA DE GESTION INTEGRAL DE RIESGO

Plan de Mitigación de Riesgos Operacinal

Gerencia:		**Fecha Relevamiento**
Subgerencia:		___/ ___/ _____

Fecha vencimiento:	___/ ___/ _____	**Porcentaje de Avance:**	%

Línea	**Producto**	**Proceso**	**Subproceso**

Riesgo

Riesgo Inherente:	
Riesgo Residual:	

Controles Existentes:

Planes de Mitigación

Indicadores

Firma Responsable
Proceso

Firma Responsable
Producto

ANEXO VI: FORMULARIO DE MAPEO DE RIESGOS (MODIFICADO)

Dpto - SubGerencia - Gerencia - Fecha de Mapeo:

Linea	Producto	Proceso	Subproceso	Según "A" 4904			Riesgo Declarado	Escenario/ Controles y Mitigantes / Observaciones	Ef. Mitigante	Riesgo Medio	Riesgo Max	Riesgo Residual - Anual				Proveedor de Servicios	% de Act. que cubre	RTI	Grupo Amenaza	Amenza
				N1	N2	N3						Frec. Prom.	Frec. Max.	Impacto Prom. por Evento	Impacto Max. por Evento					
																		#N/A		
																		#N/A		
																		#N/A		

Las columnas se completan de la siguiente manera:

Columnas LINEA, PRODUCTO, PROCESO, SUBPROCESO. Se completan de acuerdo a las incluidas en el Sistema de Administración de Riesgo Operacional (SARO)

N1, N2 y N3: Se debe indicar una clasificación del riesgo en distintos niveles de acuerdo a la Com A 4904 - Anexo "Tabla Tipos de Evento"

Riesgo Declarado: Se refiere a los factores de riesgo que generan la posibilidad de pérdidas.

Escenario/Controles y Mitigantes/ Observaciones: El escenario se refiere a una descripción de las condiciones bajo la cual se produce el riesgo. Controles y mitigantes actuales y deseados (con número de seguimiento)

Efectividad del Mitigante: Indicar en escala de 1 a 5, siendo 1 el mitigante más efectivo que se puede aplicar en el proceso, según juicio experto.

Columnas: RIESGO MEDIO, RIESGO MAXIMO Y VALORACION. Se completan automáticamente de acuerdo a los valores ingresados en las cuatro columnas que se describen seguidamente.

Frecuencia Promedio: Basándose en el escenario planteado, la cantidad de veces que produce en promedio el riesgo.

Frecuencia Máxima: Basándose en el escenario planteado, la cantidad de veces que produce el impacto máximo.

Impacto promedio: De acuerdo al escenario planteado, el importe de pérdidas que se espera por cada evento en el que se materializa el riesgo.

Impacto máximo: De acuerdo al escenario planteado, el importe de pérdidas máximo se espera en un evento en el que se materializa el riesgo.

Columna Vinculo con Proveedor: Se indicará, si existen, el nombre/s de/los proveedores externos que estén relacionados con ese riesgo.

Columna de % Actividad que cubre: Se Indicará el porcentaje de participación del Proveedor Externo en el proceso que genera el riesgo que se está analizando.

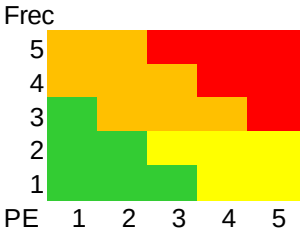
Detalle de los imputs (celdas hacen referencias a los valores cargados en la pestaña de mapeo)**:**

Riesgo Declarado	Escenario/ Controles y Mitigantes / Observaciones	Frecuencia Promedio		Frecuencia Máxima		Impacto promedio por evento		Impacto Máximo por evento	
0	0	0	Descripción	0	Descripción	0	Descripción	$ -	Descripción
0	0	0	Descripción	0	Descripción	0	Descripción	$ -	Descripción
0	0	0	Descripción	0	Descripción	0	Descripción	$ -	Descripción

Tabla conversión para cuantificación de Riesgo

	Frecuencia Anual	
Frecuencia	Desde	Hasta
1	0.00	1.00
2	1.10	12.00
3	12.10	36.00
4	36.10	100.00
5	100.10	

	Pérdida esperada en $	
Impacto	Desde	Hasta
1	$ -	$ 500,000.00
2	$ 500,001.00	$ 1,000,000.00
3	$ 1,000,001.00	$ 1,750,000.00
4	$ 1,750,001.00	$ 2,750,000.00
5	$ 2,750,001.00	



ANEXO VII: FORMULARIO DE AUTOEVALUACIÓN DE RIESGO (MODIFICADO)

AUTOEVALUACION DE RIESGOS OPERACIONALES

FECHA DE AUTOEVALUACION: ___ / ___/ _____

GERENCIA / SUBGERENCIA:	
LINEA:	
PRODUCTO:	
PROCESO:	
SUBPROCESO:	
Responsable/ Area a la que pertenece:	
Descripcion del Riesgo:	
TIPO DE RIESGO INVOLUCRADO: _____ Según Com. "A" 4904: 1) Fraude, 2) Relaciones laborales, 3) Prácticas con clientes, 4) Productos y negocios, 5) Daños a activos, 6) Alteraciones de la actividad, 7) Ejecución de procesos	
FACTOR, ORIGEN O CAUSA: _____ 1) Políticas y procedimientos, 2) Controles, 3) RRHH, 4) Automatización, 5) Calidad de información, 6) Normas, 7) Supervisión	
CONTROLES QUE SE REALIZAN Y MITIGANTES QUE SE APLICAN (Actuales y a Implementar o sugeridos): (Indique tambien resultados obtenidos)	
NORMAS, SISTEMAS y LISTADOS INVOLUCRADOS (Del Banco y del BCRA):	
SECTORES INVOLUCRADOS:	
Tiene conocimiento si hubo perdidas contabilizadas a causa de este riesgo? **SI / NO**	
ESCENARIO DE OCURRENCIA:	
OBSERVACIONES DE AUDITORIA INTERNA (Si hubiera relacionada con este riesgo):	
VINCULACION CON OTROS RIESGOS (de Mercado, de Credito, Tecnológicos, etc):	

Existen otros sectores involucrados en la generación, propagación o mitigación de este riesgo

Sector Involucrado	**Acciones mitigantes y controles realizadas** (De existir, haga referencia a evidencia documental o soporte de sistemas)

Reservado para consideraciones del encuestado

Firma y Sello del Responsable