UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURIMAC

FACULTAD DE ADMINISTRACIÓN

ESCUELA ACADÉMICO PROFESIONAL DE ADMINISTRACIÓN DE EMPRESAS

RIESGO OPERACIONAL Y NIVEL DE GESTIÓN DE LA CAJA DE PENSIONES MILITAR POLICIAL, 2014

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN ADMINISTRACIÓN DE EMPRESAS

AUTORA:

BACH. ANDREA LUCÍA GUTIÉRREZ LEYVA

ASESOR:

Mgt. MAURO HUAYAPA HUAYNACHO

ABANCAY – APURÍMAC

2016

UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

FACULTAD DE ADMINISTRACIÓN

ESCUELA ACADÉMICO PROFESIONAL DE ADMINISTRACIÓN DE EMPRESAS

RIESGO OPERACIONAL Y NIVEL DE GESTIÓN DE LA CAJA DE PENSIONES MILITAR POLICIAL, 2014

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADA EN ADMINISTRACIÓN DE EMPRESAS

AUTORA:

BACH. ANDREA LUCÍA GUTIÉRREZ LEYVA

ASESOR:

Mgt. MAURO HUAYAPA HUAYNACHO

JURADO:

PRESIDENTA: LIC. ADM. MARINA VILCA CÁCERES

PRIMER MIEMBRO: Mgt. SILVIA SOLEDAD LÓPEZ IBÁÑEZ

SEGUNDO MIEMBRO: Ing. GREGORIO CHINO GAUNA

ABANCAY – APURÍMAC
2016

Culminándose con la siguiente determinación, aprobándose por unanimidad con la nota de (14) CATORCE. Con las comunicación de las observaciones del caso para el mejoramiento del trabajo tesis, se concluye el evento académico, siendo las dieciocho horas del mismo día firmando al pie los presentes en señal de conformidad, así como el aspirante.

Universidad Nacional Micaela Bastidas de Apurimac
FACULTAD DE ADMINISTRACION
E.A.P.A.E
Lic. Adm. José Yudberto Vilca Ccolque
D. Asoc. Ordinario
PRESIDENTE

Universidad Nacional Micaela Bastidas de Apurimac
FACULTAD DE ADMINISTRACION
Escuela Académico Profesional de Administración de Empresas
Lic. Adm. Rosario L. Valer Montesinos
DOC. ASOC. ORDINARIO
PRIMER MIEMBRO

SEGUNDO MIEMBRO

45910822.
BACH. SONIA CHIPA MENDOZA.

Acta de Sustentación y Defensa de tesis "Riesgo operacional y nivel de gestión de la Caja de pensiones militar policial, 2014" de la Bachiller Gutiérrez Loayza Andrea Lucía para optar el título profesional de Licenciada en Administración de Empresas (Viernes 28/agosto/2015 En el Auditorio de la facultad de administración ubicado en la ciudad universitaria, Avenida Garcilazo S/n del Distrito de Tamburco, siendo las 12:00 horas del día 28 de agosto de 2015. En atención al memorando multiple N°098-2015-D-EAPA-FA-UNAMBA-Ab, se dieron cita los miembros del jurado de valuación y sustentación de tesis denominada "Riesgo operacional y Nivel de Gestión de la Caja de Pensiones militar policial, 2014" presentada por la Bachiller Gutiérrez Loayza Andrea Lucía para

López Ibañez (primer miembro) y M.Sc. Gregorio Cauna Chino (Segundo miembro). Estando cumplido con la documentación y procedimientos administrativos de la aspirante para optar el título profesional de Licenciado en Administración de empresas, se procedió al acto académico de la exposición y sustentación de tesis en el tiempo de 20 (veinte) minutos y en cumplimiento del reglamento de grados y títulos de la Universidad y Facultad. Cumplido el tiempo estipulado se procedió a la etapa de preguntas de los jurados dando inicio con las preguntas del M.Sc. Gregorio Cauna Chino (Segundo miembro), de similar forma procedió la Mg. Silvia Soledad López Ibañez (primer miembro) y finalmente las preguntas de la Dra. Marina Vilca Cáceres (presidenta). Cumplido esta fase se pasó a deberse la evaluación final de la sustentación y defensa de tesis, actos desarrollado de forma privada entre el jurado resaltando consolidado las evaluaciones y notas determinandose los siguientes: determinandose con la determinación, aprobándose por unanimidad con la nota de (15) quince. Con la comunicación de las observaciones del caso para el mejoramiento del trabajo de tesis, se concluye el acto académico, siendo catorce horas con cinco minutos, firmando al pie los presentes en señal de conformidad, así como la aspirante.

UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURIMAC
Lic. Adm. Marina Vilca Cáceres
DOCENTE ASOCIADO

UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURIMAC
FACULTAD DE ADMINISTRACIÓN
Mgt. Silvia Soledad López Ibañez
DOCENTE ORDINARIO

M.Sc. Gregorio Cauna Chino.

Andrea J. Gutierrez
DNI 45867768

RIESGO OPERACIONAL Y NIVEL DE GESTIÓN DE LA CAJA DE PENSIONES MILITAR POLICIAL, 2014

DEDICATORIA

A Dios, porque cada vez que sentí que no podía seguir, me mando motivos, experiencias y personas que me ayudaron a ponerle color a mis días.

A papá, que en estos últimos años me ha llenado de lecciones y de motivos para lograr este objetivo.

A Victoria, porque gracias a su apoyo incondicional logré culminar con este proyecto.

A mi familia, porque a su manera me ayudan a perseguir mi bienestar.

A todos mis amigos, porque sé que mis logros son los suyos.

AGRADECIMIENTO

En primer lugar, quiero agradecer a mis compañeros de trabajo del Departamento de Recaudación y Liquidaciones de la Caja de Pensiones Militar Policial, en especial a Hery Caballero (Jefe del departamento) por su apoyo y comprensión a lo largo de todos estos meses.

Al Prof. Mauro Huayapa Huaynacho, por el tiempo y dedicación que empleó para apoyarme en la realización de este proyecto.

Así mismo, quiero expresar mi más cálido agradecimiento a todas aquellas personas que, a lo largo de toda mi formación profesional me brindaron su apoyo en todo el sentido de la palabra; y a todas aquellas personas que indirectamente colaboraron con este logro.

AUTORIDADES UNIVERSITARIAS

Dr. Leonardo Prada Cárdenas
RECTOR

Mgt. Mauro Huayapa Huaynacho
VICE-RECTOR ACADÉMICO

Ing. Wilson Mollocondo Flores
VICE-RECTOR DE INVESTIGACIÓN

Mgt. Víctor Carmelino Vargas Godoy
DECANO DE LA FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

Mgt. Rosario Leticia Valer Montesinos
DIRECTORA DE LA ESCUELA ACADÉMICO PROFESIONAL DE ADMINISTRACIÓN DE EMPRESAS (e)

Abancay, octubre del 2016

Mg. Leticia Valer Montesinos

DIRECTORA DE LA ESCUELA ACADÉMICA PROFESIONAL DE ADMINISTRACIÓN

Ciudad.-

ASUNTO: Conformidad de informe final de tesis para optar el título profesional de Licenciada en Administración de la Bachiller en Ciencias Administrativas Andrea Gutiérrez

Es grado dirigirme a usted para saludarle y a la vez manifestarle que, el suscribe en calidad de asesor de tesis titulado "Riesgo Operacional y Nivel de Gestión de la Caja de Pensiones Militar Policial, 2014"; presentado por la Bachiller en Ciencias Administrativas Andrea Lucía Gutiérrez Leyva; doy la conformidad respectiva al informe final , considerando que la recurrente ha cumplido con el levantamiento de observaciones realizado en la sustentación de tesis y todos procedimientos establecidos en el reglamento general de grados y títulos de la UNAMBA.

Sin otro particular me suscribe a usted, reiterando las muestras de mi aprecio y estima personal.

Atentamente.

MIEMBROS DEL JURADO

RIESGO OPERACIONAL Y NIVEL DE GESTIÓN DE LA CAJA DE PENSIONES MILITAR POLICIAL, 2014

Dra. MARINA VILCA CÁCERES
Presidenta del Jurado

Mgt. SILVIA SOLEDAD LÓPEZ IBAÑEZ
Primer Miembro

Msc. GREGORIO GAUNA CHINO
Segundo Miembro

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS Y GRÁFICOS

RESUMEN

La tesis denominada: **"Riesgo operacional y nivel de gestión de la Caja de Pensiones Militar Policial, 2014"** ha identificado el problema de investigación ¿Cuál es el grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014?. Ante la problemática, se propone la solución a través de la formulación de la siguiente hipótesis: existe un alto grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014. Este trabajo se ha orientado al siguiente objetivo: determinar el grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014. Por otro lado se tiene que esta investigación es sustantiva – básica. El nivel de investigación es descriptiva – correlacional. El método utilizado ha sido el deductivo. La población estuvo compuesta por 116 trabajadores de las diferentes dependencias de la Caja Militar Policial. La muestra estuvo constituida por 89 trabajadores de la Caja Militar Policial. Las técnicas utilizadas para tener la información fueron las encuestas y análisis documental. Como corolario del trabajo se tiene que el resultado más importante está dado porque el 69.7% de los encuestados acepta que casi siempre existe un alto grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014.

Palabras claves: riesgo operacional, nivel de gestión, Caja de Pensiones Militar Policial.

ABSTRACT

The thesis entitled: "Operational risk and management level Military and Police Pension Fund, 2014" has identified the research problem What is the degree of relationship between operational risk and the level of management of the Fund of Pension Military Police 2014 ?. Faced with the problem, the solution through the formulation of the following hypothesis is proposed: a high degree of relationship between operational risk and the level of management Military and Police Pension Fund, 2014. This work has focused on the following objective: determine the degree of relationship between operational risk and the level of management Military and Police Pension Fund, 2014. On the other hand: this research is substantive - basic. The level of research is descriptive - correlational. The method used was deductive. The population consisted of 116 workers of different units of the Military Police Fund. The sample consisted of 89 workers of the Military Police Fund. The techniques used to get information were surveys and document analysis. As a corollary of the work has to be the most important result is given as 69.7% of respondents agree that there is almost always a high degree of relationship between operational risk and the level of management Military and Police Pension Fund, 2014.

Keywords: operational risk management level, Military and Police Pension Fund.

INTRODUCCIÓN

El presente trabajo de investigación lleva por título "Riesgo operacional y nivel de gestión de la Caja de Pensiones Militar Policial, 2014", para optar el título profesional de Licenciado en Administración, presentado por la Bachiller en Ciencias Administrativas Andrea Lucia Gutiérrez Leyva.

La temática de la investigación está orientada determinar el grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014.

La estructura que se ha considerado en la presente tesis se compone de 04 capítulos. El Capítulo I comprende el marco teórico; el Capítulo II: hipótesis y variables; el Capítulo III: la metodología de la investigación y el Capítulo IV corresponde a resultados y discusión. Para el desarrollo de la tesis, se ha tomado como base teórica las referencias bibliográficas consultadas.

Se espera que la presente tesis cumpla con las exigencias del Reglamento General de Grados y Títulos de la Universidad Nacional Micaela Bastidas de Apurímac.

La Autora.

CAPÍTULO I

MARCO TEÓRICO

1.1. ANTECEDENTES

Al referirnos a la gestión de riesgos específicamente, se observa que está ligada en gran medida a la gestión de riesgos en el sector financiero, ya que estas empresas empezaron a involucrar dentro de sus estructuras organizacionales un área de riesgo operacional.

Para efectos de establecer parámetros para la estandarización y regularización de los diferentes tipos de riesgos se creó el Comité de Basilea en junio de 1999.

A fines de junio de 2004, se dio a conocer el documento "Convergencia Internacional de Medidas y Normas de Capital", y para ser simplificado, se denominó Nuevo Marco de Capital o **Basilea II** (Hanson García & Salazar Noriega, 2005). Basilea II define al **Riesgo Operativo** como las pérdidas resultantes de procesos, personal o sistemas internos inadecuados o defectuosos o bien acontecimientos externos. Incluye el riesgo legal y excluye el riesgo estratégico y de reputación (Hanson y Salazar, 2015)

El trabajo de investigación presentado por (Fernández Laviada & Martínez García, 2006), que buscaba conocer el grado de avance alcanzado por las entidades financieras españolas en la gestión de las áreas claves del riesgo operacional, concluye que: **i)** en los últimos años el sistema financiero español ha realizado grandes esfuerzos en la gestión del R.O, y en consecuencia, en poco tiempo se han alcanzado importantes avances, pudiendo afirmar que en líneas generales se encuentra al nivel de los principales sistemas financieros de otros países…; **ii)** no se puede negar el origen del creciente interés demostrado por este riesgo en las exigencias de capital de Basilea, con las que la mayoría de las entidades, aun siendo excesivas, siguen conformes. Sin embargo, todas seguirán con sus procesos en este ámbito, aun en el caso en que Basilea se hubiese retractado,

porque se ha comprobado que es necesario la ayuda a la creación de valores de las entidades; **iii)** introducir de forma generalizada el RO en la cultura de las organizaciones será el principal reto al que deberán enfrentarse las entidades que quieran implantar con éxito un marco completo de gestión del RO. Sin embargo, la gestión correcta y completa de este riesgo no sólo les servirá para cumplir con la normativa y regulación vigente sino que les permitirá, además, reducir las pérdidas por fallos operacionales, los riesgos de control y mejorar la calidad de los servicios, lo que finalmente redundará en una mayor protección del accionista; **iv)** en la actualidad todas las entidades encuestadas ya han adoptado la definición del RO propuesta por Basilea, aunque la clasificación de eventos y clasificación por líneas de negocio sigue planteando problemas a la hora de su implantación en la práctica. Las pérdidas operacionales por "ejecución, entrega y gestión de procesos", junto con los "fraudes internos y externos" son las categorías más frecuentes y de mayor impacto para la mayoría de las encuestadas (Fernández, 2006)

La tesis presentada por (Ávalos Ruiz, 2012), titulada "Análisis, diseño e implementación del sistema de riesgo operacional para entidades financieras – SIRO", para optar en grado de Magíster en Informática mención en Ingeniería del Software, en la Escuela de Posgrado de la Pontificia Universidad Católica del Perú; cuyo objetivo fue diseñar e implementar el Sistema de Riesgo Operacional, incluyendo el módulo de gestión de eventos de pérdida, basado en la continuidad de la plataforma creada de riesgo operacional, que es la base para llegar a la gestión cuantitativa, con el objetivo de poder realizar una gestión integral de riesgo para el sector financiero del Perú; la que arriba a las siguientes conclusiones: **i)** el uso de un software libre para el desarrollo es un requerimiento de los especialistas en manejo de riesgo operacional para evitar los costes excesivos en la adquisición de licencias y el servicio de implantación del sistema; **ii)** la utilización del sistema de riesgo operacional en las entidades financieras integra las

distintas áreas de negocio y procesos de gestión de la organización ayudando y automatizando a la gestión del riesgo operacional por parte del área de gestión de Riesgo.

1.2. BASES TEÓRICAS

1.2.1. RIESGO OPERACIONAL: REVISIÓN DE SU REGULARIZACIÓN Y DE LOS AVANCES EN LA UNIÓN EUROPEA

Según (Fernández Laviada & Martínez, 2010) El principal detonante en el desarrollo que ha experimentado el riesgo operacional en los últimos años es el trabajo del Comité de Supervisión Bancaria de Basilea (CSBB) y, en particular, el Nuevo Acuerdo de Capital que modifica el Acuerdo de 1988.

No obstante, eso no significa que el riesgo operacional no fuese supervisado ni gestionado antes, sino que:

- La supervisión del riesgo operacional, fue considerado por mucho tiempo como un riesgo de naturaleza eminentemente cualitativa –a diferencia de los riesgos de crédito y de mercado, cuyo tratamiento regulatorio ha consistido tradicionalmente en la exigencia de unos requerimientos mínimos de capital– se hacía únicamente desde un punto de vista cualitativo, evaluando el riesgo inherente, el entorno de control y revisando las auditorías internas.
- La gestión del riesgo operacional, muy ligado a los errores y fallos en los sistemas (riesgo operativo), tenía un alto componente reactivo, surgiendo a partir de los fallos más significativos. Al estar tan fragmentado, se gestionaba de forma individualizada y no se veía como una parte más integrada en la gestión de los riesgos de la entidad. El riesgo operacional está presente en todas las actividades, de ahí que nadie se responsabilizase de él, hasta la fecha, de una manera global,

recayendo su responsabilidad de manera particular en la gerencia de las diferentes áreas.

1.2.1.1.COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA

Basilea II propone un tratamiento más sensible a los riesgos y plantea un marco tendente a garantizar la gestión integral y proactiva del riesgo operacional, concretándolo en tres pilares, tal y como se explica a continuación:

PILAR 1. REQUERIMIENTO DE CAPITAL:

Establece tres métodos, de sofisticación creciente, para calcular el capital regulatorio exigido, con base en la evaluación cualitativa del riesgo operacional y a los eventos de pérdidas producidas:

- El **Método del Indicador Básico (BIA),** el más sencillo, consiste en aplicar un porcentaje fijo, α (alfa), del 15%, dado por el regulador, a un indicador de la exposición al riesgo operacional (ingresos brutos).
- El **Método Estándar (SA)** sigue el mismo sistema, pero se exige a las entidades que dividan su actividad en ocho líneas de negocio. El cálculo consiste en aplicar unos porcentajes fijos, β (betas) (fijados entre un 12% y un 18%) a un indicador de la exposición al riesgo operacional (ingresos brutos) en cada una de las líneas de negocio, para después sumar los importes obtenidos para las diferentes líneas de negocio.

  Una variante del método estándar es el denominado **Método Estándar Alternativo (ASA),** donde se utiliza como indicador de riesgo la inversión crediticia *"loans and advances (LA)"* en lugar del ingreso bruto, en dos líneas de negocio, la de banca minorista y la de banca comercial, únicamente bajo la aprobación previa del supervisor.

- **Modelos Avanzados o Modelos AMA**, para aquellas entidades que cumplan los rigurosos criterios generales cualitativos y cuantitativos establecidos por Basilea. Las entidades podrán utilizar a efectos regulatorios, previa aprobación del supervisor, el resultado de sus modelos internos, que habrán diseñado según sus necesidades propias de gestión.

PILAR 2. PROCESO DE SUPERVISIÓN:

Incide en la importancia de una gestión cualitativa del riesgo operacional como herramienta clave para toda la organización. Supervisa los marcos de control establecidos en las entidades y, según el caso, propone o exige cambios en los procesos o amplía los requerimientos de capital exigido.

PILAR 3. DISCIPLINA DEL MERCADO:

Fija las bases de la información a revelar a terceros en cuanto a la metodología utilizada, la exposición al riesgo por cada línea de negocio y el tipo de evento de pérdida que se haya producido.

Precisamente, entre los hitos de este nuevo acuerdo cabe destacar el hecho de que recomiende que el riesgo operacional sea definido como una categoría de riesgo independiente que además debe ser cubierta por capital regulatorio.

La primera vez que el CSBB demostró su interés por el riesgo operacional fue con el documento de 1998 "Operational Risk Management", en el cual manifestaba que "gestionar dicho riesgo empezaba a ser una característica importante de una buena gestión de riesgos en los mercados financieros modernos".

Más tarde, en el primer documento a consulta del nuevo acuerdo publicado en junio de 1999, el CSBB hacía pública su intención de aumentar las exigencias de capital para

cubrir "otros riesgos", incluyendo el riesgo operacional, al reconocer que las entidades se veían afectadas por otros riesgos distintos del riesgo de crédito y de mercado hasta entonces considerados.

Pero hasta que no se publicó el segundo documento a consulta, en enero del 2001, que exigía unos requerimientos de capital por este riesgo sobre la base del Pilar 1, el riesgo operacional no pasó a formar parte de las agendas de la mayoría de las altas direcciones.

En las primeras fases de redacción del Nuevo Acuerdo del Consejo de Basilea (NACB) hubo un intenso debate sobre si los requerimientos de riesgo operacional deberían recogerse en el Pilar 1 o en el Pilar 2 y finalmente, debido a la magnitud que había tenido este riesgo en crisis recientes y al desarrollo progresivo de estos modelos, se decidió exigir unos requerimientos específicos de capital. Aunque sobre todo en el tratamiento de los modelos avanzados, la regulación del Pilar 1 alcanza tal grado de flexibilidad que, en la práctica, se aproxima a las características intrínsecas del Pilar 2.

Otro de los mayores hitos de Basilea II ha sido dar una definición al riesgo operacional. Aunque pudiera parecer irónico, el riesgo más antiguo y reconocido en el sector, hasta la redacción del NACB, y a diferencia de lo que ocurría en otros riesgos, no contaba con una definición común. Mientras que para algunas entidades era un concepto muy amplio, básicamente todo aquello que quedaba fuera del riesgo de crédito o de mercado, para otras se limitaba a los fallos operativos o de procesos, es decir, riesgo operativo.

El Institute of International Finance (IIF), un grupo privado de investigación y apoyo que ofrece sus servicios a grandes bancos intenacionales, creo entre 1999 y el 2000 el *Working Group on Operational Risk (WGOR)* y un subgrupo del mismo, el *Industry Technical Working Group on Operational Risk (ITWGOR)*, ambos con el objetivo

fundamental de responder al primer documento consultivo del Comité de Basilea de junio de 1999.

Los tres trabajaron en la publicación de diferentes documentos sobre el riesgo operacional y en octubre del 2000, el ITWGOR adelantaba una definición de riesgo operacional usada por el IFF y que fue tomada como referente a partir de ese momento por el resto del sector financiero. La definición, aunque ligeramente modificada, fue la que después adoptó el Comité de Basilea en su documento *"Operational Risk"* de enero del 2001, documento que, a su vez, sirvió de soporte para el segundo documento consultivo del NACB. La definición consensuada fue la siguiente:

"El riesgo operacional es el riesgo incurrir en pérdidas directas o indirectas como consecuencia de inadecuados o erróneos procesos internos, personal o sistemas, o como consecuencia de acontecimientos externos.

Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional".

Posteriormente, en septiembre del 2001, el Comité de Basilea en el documento *"Regulatory Treatment of Operational Risk"* modificó ligeramente la definición, eliminando la referencia a las pérdidas directas e indirectas, con lo que la definición definitiva fue:

"El riesgo operacional es el riesgo de pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal o los sistemas internos, o bien como consecuencia de acontecimientos externos.

Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional".

Además de aportar una definición consensuada, este documento proporciona por primera vez una clasificación detallada del tipo de evento de pérdida que servía de guía para delimitar el concepto y ayudar a homogeneizar su registro en las bases de datos sobre pérdidas en las diferentes líneas de negocio, para el cálculo del capital regulatorio posterior.

En definitiva, se está reconociendo formalmente que el riesgo operacional es un riesgo más de la actividad bancaria, que ha aumentado considerablemente en los últimos años y que atrae el interés y la preocupación de instituciones, supervisores y académicos.

Al igual que este Comité, los reguladores de otros países han trabajado –y lo siguen haciendo- en normativas, recomendaciones y legislaciones de diferente índole que afectan de algún modo al riesgo operacional y su gestión.

1.2.1.2.LA COMISIÓN EUROPEA

La Comisión Europea (CE) ha seguido, como observadora, el trabajo de los distintos grupos del CSBB, ya que debía adaptar las recomendaciones de Basilea a la realidad europea y transformarlas en un texto legislativo aceptable para todos los países miembros de la Unión Europea (UE).

El Acuerdo de Capitales de 1988 se reflejó en la Directiva 89/647/CEE consolidada en la Directiva 2000/12 (que reagrupa en un texto único las siete directivas existentes relacionadas con la regulación de entidades de crédito).

En cuanto a la nueva regulación se decidió que, en lugar de plasmarse en una nueva directiva, modificase la Directiva 2000/12 así como la Directiva 6/1993 de adecuación de capital en empresas de inversión y entidades de crédito.

En el marco de la UE, a diferencia del NACB, la nueva regularización será de aplicación a todas las entidades de crédito y empresas de inversión autorizadas bajo la Directiva de Servicios de Inversión.

Tras la publicación definitiva de Basilea II, la CE presentó el 14 de junio de 2004 su propuesta de modificación de Directiva para su tramitación en el Consejo y el Parlamento europeo. Y finalmente, el 30 de junio de 2006 se publicaron los textos definitivos de las Directivas Europeas en materia de Capital, denominadas globalmente Directiva de Requerimientos de Capital (CRD, por sus siglas en inglés).

El proceso ha sido paralelo al de Basilea, por lo que conociendo el trabajo del CSBB se conoce también el realizado por la CE. La norma europea presenta algunas diferencias con las recomendaciones de Basilea, no solo en el aspecto formal sino también de contenido, en ocasiones debido a las especificidades de los sistemas financieros europeos o a los acuerdos alcanzados en el ámbito europeo en materia de discrecionalidad nacional.

Tras ello, en los siguientes meses, cada uno de los Estados miembros de la UE ha ido trasponiendo las Directivas a sus normativas nacionales para la entrada en vigor en enero del 2007 del enfoque del indicador básico y estándar para riesgo operacional y las obligaciones derivadas de los Pilares 2 y 3. En enero del 2008 entró en vigor los enfoques más complejos que, para el riesgo operacional son los enfoques AMA.

En el caso de España, como el proceso legislativo europeo, por el que se adoptaba el nuevo Acuerdo de Capital, llevaba un retraso importante, el Banco de España fue manteniendo diversas reuniones con las asociaciones bancarias y las entidades, a lo largo del 2006, para transmitirles las primeras reflexiones y facilitar su implantación.

Por otra parte, el Ministerio de Economía y Hacienda con la participación del Banco de España y la Comisión Nacional del Mercado de Valores, creó un grupo de trabajo de

alto nivel encargado de estudiar la forma más adecuada de incorporar las directivas a la normativa española, analizando qué elementos deberían contenerse en la Ley y cuáles en el Real Decreto que la desarrolle, mientras que las partes más técnicas se incluirían en una Circular que debe ser emitida por el Banco de España. Cabe indicar que el 29 de diciembre, el Banco de España hizo público el borrador de la Circular de Solvencia con la que traspondrá a España la Directiva comunitaria.

Mientras se elaboraba esta normativa, el Banco de España publicó en junio del 2006 el documento "Implantación y validación de enfoques avanzados de Basilea II en España" con el que pretende dar a conocer los objetivos, los criterios, el calendario y la documentación básica necesaria para la implantación de los enfoques avanzados previstos en la nueva normativa de recursos propios, así como en el contenido de los procesos de validación de dichos enfoques, que han de llevarse a cabo a efectos de que puedan servir de base para el cálculo de los recursos propios mínimos exigibles a una entidad de crédito.

Por último, en el ámbito europeo, en el año 2004 se creó el Comité Europeo de Supervisores Bancarios (CEBS, por sus siglas en inglés), con el cometido fundamental de contribuir a una implantación consistente de las Directivas comunitarias y fomentar la convergencia europea de las prácticas supervisoras de los Estados miembros.

En el ámbito de aplicación de la Directiva de Capital, el CESB publicaba el 11.07.2005 en Consultation Paper "Validation and Assessment of the Risk Management and Risk Measurement System", más conocido en el sector como CP10 y más reciente, en abril 2006, ha publicado la guía "Guidelines on the Implementation, Validation and Assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches" que orienta sobre la implementación y validación de los modelos internos.

1.2.1.3.REINO UNIDO

La Autoridad Reguladora de servicios Financieros en el Reino Unido, la FSA *(por sus siglas en inglés, Financial Services Authority),* es un órgano independiente no gubernamental que regula la industria de servicios financieros en este país y al que se le ha atribuido una amplia gama de competencias legislativas e investigadoras, así como la facultad de establecer los medios que garanticen el cumplimiento de esas leyes.

La autoridad del Reino Unido fue uno de los primeros reguladores en abordar el tema desde su origen. Prueba de ello son los dos documentos que publicó en 1999, "Allocating Regulatory Capital for Operational Risk" y el CP35 "Senior Management Arrangements, Systems and Controls", incluso antes de que se hubiera incluído este riesgo entre las exigencias de Basilea.

Para reforzar su trabajo, la FSA constituyó en mayo del 2002 The Operational Risk Implentation Advisory Group (ORIAG), pasando a finales del 2003 a ser el Operational Risk Standing Group (ORSG), y que agrupa a expertos en riesgo operacional tanto de la FSA como del sector.

El objetivo de este grupo consultivo es proporcionar un foro para discutir las normas relacionadas con la aplicación de los requisitos del NACB y de la Directiva de la CE sobre la adecuación del capital para las instituciones de crédito y las firmas de inversión. Aquí cabe resaltar que la FSA emitió diferentes rangos de normas y documentos para alcanzar sus objetivos de regulación. En primer lugar, los Consultation Paper o CP (documentos a consulta), donde se expone la propuesta de la FSA y se pide al sector que dé su opinión al respecto. En segundo lugar, los Feedback Statement o FS (sumario de respuestas de consulta), donde se detallan respuestas de las entidades y si la FSA ha cambiado su posición como resultado de las anteriores. Si el FS necesita contener políticas entonces en su lugar se emite un Policy Statement o PS (declaración de

política). El resultado de toda esta actividad se refleja en los cambios que va asumiendo el Handbook o Manual del FSA y en concreto en la sección llamada "The Prudential Sourcebook for Banks, Building Societies and Investment Firms" (BIPRU).

El trabajo más importante para el desarrollo del riesgo operacional ha sido el Consultation Paper (documento a consulta) o CP142 *"Operational Risk Systems and Controls"*, emitido a consulta en julio del 2002 y que esboza la política de sistemas y controles de riesgo operacional propuestas por la FSA. De este borrador cubría dos normas que serían aplicables a todas las entidades afectadas por el NACB:

- La SYSC 3A *"Operational Risk: Systems and Controls"* que ofrece una guía sobre las principales áreas que debe considerar una entidad al gestionar el riesgo operacional, cubriendo por tanto un gran abanico de temas como el riesgo del personal, los sistemas de tecnología, la seguridad informática, la continuidad de los negocios o el *outsourcing*.
- La PRU 6.1 *"Operational Risk: Prudential Systems and Controls"* que ofrece una guía sobre los aspectos que la entidad deberá considerar al establecer y mantener un marco de gestión para la identificación, valoración, seguimiento y control del riesgo operacional.

Tras varios meses de debate y trabajo revisando cómo la gestión del riesgo operacional iba evolucionando en las entidades, en concreto en 22 firmas que estaban en forma activa desarrollando sistemas para la gestión del riesgo operacional, la FSA presentó en julio 2003 la *Policy Statement* (Declaración de Política) o PS *"Building a framework for Operational Risk Management: the FSA's Observations"* y unos meses más tarde, en octubre 2003, publicó el *"Near Final Text on Prudential Risk Systems and Controls"*. El propósito de estas declaraciones era recoger los principales resultados de la revisión realizada e informar sobre el progreso del sector en el desarrollo e

implementación de sistemas para la gestión del riesgo operacional en comparación con el borrador propuesto en el CP142, pero en ningún caso son normas de obligado cumplimiento, al menos hasta que sean trasladadas al Manual de la FSA.

Así, la FSA pretende servirse de experiencias previas para llevar a cabo la elaboración de una guía acerca de los principios reguladores que deben seguirse en el Reino Unido para la aplicación de la Directiva. Como norma general, la FSA no persigue proporcionar a las empresas una guía en forma de pautas prescriptivas, sino en forma de principios. Además pretende, siempre que sea posible, aplicar unas reglas y guías que resulten completas y proporcionales a la naturaleza, alcance y complejidad de las actividades de la empresa.

1.2.1.4.ESTADOS UNIDOS

Durante todo el proceso de revisión del NACB, los diferentes reguladores americanos se han caracterizado por seguir su propio camino en temas clave, y el riesgo operacional no ha sido la excepción.

The Office of the Comptroller of the Currency (OCC), el *Board of Governors of the Federal Reserve Systems* (Board), la *Federal Deposit Insurance Corporation* (FDIC) y la *Office or Thrift Supervision* (OTS), conocidas en su conjunto como las Agencias (Agencies), publicaron el 04.08.2003 para su consulta por el sector dos documentos que presentaban las propuestas de modificación de la regulación de capital en los Estados Unidos (*Risk Based Capital Standards*), que hasta ese momento se regía por las normas basadas en l primer Acuerdo de Capital de Basilea (Basilea I) aprobadas en 1989.

Las revisiones propuestas fueron publicadas en mismo día en el Federal Register y recogidas en dos documentos:

- El primero, un *Advance Notice of Proposed Rulemaking* (ANPR) *"Risk Based Capital Guidelines; Implementation of New Basel"* que presentaba la opinión de las Agencias en relación al marco propuesto para implementar el Nuevo Acuerdo en EEUU.
- Y el segundo documento que a su vez está dividido en dos secciones:

  La primera, *Draft Supervisory Guidance* (DSG) *with request for comment "Internal Ratings – Based Systems for Corporate Credit"*, donde se describen las expectativas de los supervisores sobre las entidades que pretendieran adoptar un enfoque avanzado para la medición del riesgo crédito. La guía pretende ofrecer a supervisores y entidades una clara descripción de los componentes esenciales y características de un marco IRB aceptable.

  La segunda, *Draft Supervisory Guidance* (DSG) *with request for comment "Operational Risk Advanced Measurement Approaches for Regulatory Capital (AMA guidance)"*, donde se resaltan las expectativas de los supervisores sobre las entidades que pretendan adoptar un enfoque avanzado para la medición del riesgo operacional.

En ambos casos las Agencias buscaban la opinión y posición del sector sobre el marco propuesto por el NACB, aportando sus criterios, describiendo los aspectos regulados y proponiendo su propio marco.

Tras casi tres años de debate, modificaciones y múltiples retrasos, y ante la expectativa del resto del mundo bancario, el 30.03.2006 las Agencias publicaron un borrador

preliminar acerca de cómo se iba a implementar el Nuevo Acuerdo en los Estados Unidos. La propuesta de esa norma sería de aplicación obligatoria únicamente para los bancos americanos internacionalmente activos y de carácter opcional para el resto de entidades. Finalmente, el 05.09.2006 se hizo público el borrador definitivo, *Notice of Proposed Rulemaking to Implement Basel II Risk-Based Capital Requirements in the United States for large, Internationally Active Banking Organizations, conocido como Basel II NPR*, publicado en el número 185 del Federal Register el 25 del mismo mes y abierto a debate hasta finales de enero 2007.

Con relación al riesgo operacional, la OCC había publicado previamente en julio 2003 el documento *"Supervisory Guidance on Operational Risk Advanced Measurement Approaches for Regulatory Capital"*. El propósito de esta guía era presentar las expectativas las Agencias sobre las entidades que usan enfoques avanzados para calcular las exigencias de capital por riesgo operacional bajo la nueva regulación. En ella se identifican las reglas que deben respetar y mantener las entidades para usar los enfoques avanzados en el cálculo del capital, y proporcionando con ellas la base para un buen marco de gestión del riesgo operacional.

Por otra parte, *The Securities and Exchange Commission* (SEC), regulador principal de los bancos de inversión y brokers-dealers sorprendía a todos cuando en octubre 2003 anunciaba la publicación de dos normas (*proposed rules*) con las que presentaba un marco similar al del CSBB:

- *"Supervised Investment Bank Holding Companies"*, y
- *"Alternative Net Capital Requirements for Broker-Dealers that are Part of Consolidated Supervised Entities"*.

En las notas a pie de página de la primera norma propuesta la SEC incluía una nueva definición de riesgo operacional:

"El riesgo operacional es el riesgo de pérdida debido a fallo de los controles dentro de la entidad, incluyendo, pero no limitándose a, límites excedidos no identificados, operaciones no autorizadas, fraude en operaciones o en las funciones del back-office, personal sin experiencia, y unos inestables y fácilmente accesibles sistemas informatizados".

La norma separa el riesgo legal como una categoría independiente del riesgo operacional y también lo define más detalladamente que el NACB. Con ello la SEC discrepa con otros reguladores americanos en la estructura de su marco.

1.2.2. CLASIFICACIÓN DE RIESGOS

Según (Arranz Álamo & Rodríguez López, 2010), la clasificación de los riesgos que se vaya a utilizar en el análisis dependerá del tipo de entidad y de la tipología de actividades que desarrolla y mercados en los que opera. Estos pueden ser: ***i) Riesgo de crédito:*** es la posibilidad de sufrir pérdidas derivadas de que el deudor no cumpla completamente sus obligaciones contractuales. Dentro de esta categoría se encuentran: *riesgo de insolvencia:* es el riesgo asociado a la solvencia del prestatario, es decir, a la capacidad de devolución de las deudas contraídas, así como del coste de las mismas en tiempo y forma, al acreedor; *riesgo país:* existe un riesgo soberano para los acreedores de los estados o de las entidades garantizadas por ellos, en cuanto pueden ser ineficaces las acciones contra el prestatario, y un riesgo de transferencia, que es el de los acreedores extranjeros de los residentes de un país con respecto a que dicho país pueda

experimentar una incapacidad general para hacer frente a sus deudas, por carecer de la divisa o divisas en que aquéllas estén denominadas; ***ii) Riesgo de mercado*:** es la posibilidad de sufrir pérdidas derivadas de movimientos adversos en los precios de mercado de los instrumentos negociables con los que opera la entidad. *Riesgo de posición/precio:* es la posibilidad de sufrir pérdidas derivadas de movimientos adversos en los precios de mercado de los instrumentos negociables con los que opera la entidad en tipo, en plazo, en precio que actúan como cobertura las unas de las otras. *Tipo de interés:* es la posibilidad de sufrir pérdidas por el impacto potencial de cambios en los tipos de interés sobre los beneficios de la entidad o sobre el valor neto de sus activos. *Tipo de cambio:* es la posibilidad de que fluctuaciones adversas en los tipos de cambio de las monedas en las que están denominados los activos, pasivos y operaciones de fuera de balance de la entidad, generen pérdidas; ***iii) Riesgo de liquidez*:** es la posibilidad de sufrir pérdidas por no tener fondos líquidos disponibles para hacer frente a las obligaciones de pago; ***iv) Riesgo estratégico*:** es el que se genera por las políticas de gestión y control establecidas o por decisiones sobre nuevas estrategias empresariales, nuevos productos, mercado, etc. en el caso de que su planificación o ejecución presenten defectos o no se consigan los resultados esperados; ***v) Riesgo operacional*:** según la definición adoptada en BIS II, es la posibilidad de sufrir pérdidas como consecuencia de la existencia de procesos, sistemas, equipos técnicos y humanos inadecuados, o por fallos en los mismos, así como por acontecimientos externos. Se incluyen los riesgos de fraude interno y externo, relaciones laborales y seguridad en el puesto de trabajo, clientes productos y prácticas empresariales, daños a activos materiales, incidencias en el negocio y fallas en los sistemas y ejecución, entrega y gestión de procesos; ***vi) Riesgo reputacional*:** es la posibilidad de pérdidas como consecuencia de informaciones que afectan negativamente a la percepción que los

clientes o los mercados tienen de la entidad. Se incluyen el riesgo de imagen y el de información; ***vii) Riesgo legal:*** posibilidad de sufrir pérdidas derivadas de incumplimiento de la normativa vigente o de relaciones contractuales defectuosamente constituidas. Se incluye también el riesgo fiscal, por cuanto puede ocasionar pérdidas por el incumplimiento de la normativa tributaria correspondiente.

1.2.2.1.RIESGO OPERACIONAL

Según el Comité de Supervisión Bancaria de Basilea (2004), en sus documentos sobre Convergencia Internacional de Medidas y Normas de Capital, señala que "el riesgo operacional se define como el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos".

De acuerdo a Basilea II, el riesgo operacional lo define como el riesgo de pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal o los sistemas internos, o bien como consecuencia de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional.

De la misma manera la Superintedencia de Banca y Seguros, definió el riesgo operacional como la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación. En tanto que el riesgo legal (Diario El Peruano, 2009, p. 28), lo define como la posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o

acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros (SBS, 2009)..

1.2.2.1.1. CATEGORÍAS DEL RIESGO OPERACIONAL

De acuerdo al (Comité de Basilea de Supervisión Bancaria, 2004), las categorías del riesgo operacional son:

a) ***Fraude interno***: referido a pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicada, al menos, una parte interna a la empresa; no se consideran los eventos asociados con discriminación en el trabajo.

   Asimismo, (Arranz Álamo & Rodríguez López, 2010) indica que es la posibilidad de sufrir pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales.

   Esta categoría incluye eventos como: fraudes crediticios, hurto (con participación de personal de la empresa), operaciones no reveladas intencionalmente, operaciones no autorizadas con pérdidas pecuniarias, sobornos, extorsión, malversación, entre otros;

b) ***Fraude externo***: referido a pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero.

   Esta categoría incluye eventos como: robos, falsificación, circulación de cheques sin fondo, ataques informáticos, robo de información, entre otros;

c) ***Relaciones laborales y seguridad en el puesto de trabajo***: se refiere a pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad/discriminación en el trabajo.

Esta categoría incluye acciones relacionadas a la remuneración, beneficios sociales, extinción de contratos, normas de higiene, indemnización a trabajadores discriminación, entre otros;

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

Esta categoría considera acciones como violación de privacidad, confusión de cuentas, prácticas inadecuadas de negocios o mercado, como prácticas ajenas a la competencia, manipulación del mercado, etc.;

e) ***Daños a activos materiales***: Pérdidas derivadas de daños o perjuicios a activos físicos como consecuencia de desastres naturales u otros eventos de fuentes externas. Esta categoría incluye pérdidas materiales por desastres, pérdidas humanas por causas externas por vandalismo o terrorismo, etc.

f) ***Interrupción del negocio y fallas en los sistemas:*** Pérdidas derivadas de incidencias o interrupciones en el negocio y de fallas en los sistemas relacionados al hardware, software, telecomunicaciones, interrupciones e incidencias en suministros.

g) ***Ejecución, entrega y gestión de procesos:*** Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores. Esta categoría incluye eventos asociados con: captura de transacciones, ejecución y mantenimiento, monitoreo y reporte, entrada y documentación de clientes, gestión de cuentas de clientes, contrapartes de negocio, vendedores y proveedores.

1.2.2.1.2. TIPOLOGÍA Y CODIFICACIÓN DE LOS EVENTOS DEL RIESGO OPERACIONAL

DEFINICIÓN DE EVENTO Y PÉRDIDA

Según (Anduig Aldea & López Álvarez, 2010) el paso previo a la clasificación de un evento según su tipología y la línea de negocio a la que pertenece, siguiendo las directrices establecidas por Basilea II, es comprobar que cumple los requisitos para que pueda ser considerado un evento de riesgo operacional.

Define evento de riesgo operacional, lo adoptado por Basilea, "un evento de riesgo operacional es la pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal y los sistemas internos o bien de acontecimientos externos", incluyéndose en esta definición el riesgo legal (jurídico) y excluyéndose el riesgo estratégico, de negocio y el riesgo de reputación.

Dado que pueden existir eventos que generen pérdidas y otros no, se entiende por "pérdida operacional" todo impacto negativo o reducción registrada en la cuenta de resultados o en la situación patrimonial de la entidad que tenga un reflejo contable y haya sido provocado a consecuencia de cualquier evento cuya causa u origen este incluida en la definición de riesgo operacional.

Se puede observar que esta definición no incluye:

- Los costes de oportunidad.
- El contenido de las cuentas transitorias: el evento no debería registrarse hasta que no genere imputación en las cuentas definitivas.
- Los eventos que generen un impacto positivo para la entidad.

Junto a esto se deben cumplir unos criterios específicos para la determinación de los eventos que son los siguientes:

- No corresponde a ninguno de los riesgos excluidos. Es decir no es consecuencia de un riesgo estratégico, de negocio o de reputación.
- Es susceptible de tener reflejo contable.
- Y además: es consecuencia de deficiencias en el diseño de los procedimientos establecidos o de los controles establecidos, o ha sido causado por un error humano en la ejecución de tareas asignadas o en el equipamiento necesario para el buen funcionamiento de los procesos, o ha sido ocasionado por algún suceso externo no controlable por la entidad.

Una vez establecido que se trata de un evento con pérdida operacional, se deberá proceder a su clasificación según los criterios indicados por Basilea II.

CLASIFICACIÓN DE EVENTOS

Basilea determina que los eventos, tanto para la asignación de capital como para la gestión del riesgo operacional por las entidades (objeto último del documento) deben estar clasificados según los criterios indicados a continuación:

1.2.2.1.2.1. EVENTOS POR TIPOLOGÍA (CAUSA)

El marco a utilizar en la clasificación de los eventos de riesgo operacional por la causa que lo ha motivado responde a lo establecido por el Comité de Supervisión Bancaria de Basilea en el Anexo 7 del documento "International Convergence of Capital Measurement and Capital Standards" emitido el mes de junio 2004.

Los eventos deberán clasificarse al nivel de descripción más bajo que la entidad considere idóneo para gestionar su riesgo operacional. A fin de facilitar las tareas de clasificación de los eventos, garantizando el tratamiento completo, coherente, los criterios de clasificación deberán seguir unos principios que aseguren la asignación a:

- Categorías mutuamente excluyentes.
- Categorías homogéneas para toda la entidad.
- Categorías fáciles de entender.

Para la clasificación de cualquier evento se realizará atendiendo a las siguientes reglas:

- La causa inmediata (próxima) que lo ha provocado.
- Las causas específicas, priorizándolas sobre las causas genéricas.
- La causa determinante: en ocasiones, se presentarán eventos producidos por la existencia de varias causas simultáneas. Estos eventos se deberán clasificar en función de la causa que se considere origen o determinante para que se produzca.

Criterios a tener en cuenta en la clasificación de los eventos:

a) FRAUDE INTERNO

Para que un evento sea adscrito a la presente categoría, deben cumplirse los siguientes requisitos:

- **Intencionalidad y existencia de ánimo de lucro:** la acción (u omisión) debe perseguir un beneficio ilícito o soslayar regulaciones, leyes, etc. mediante engaño, ocultación, fraude o simulación, es decir, sacar provecho o conseguir un enriquecimiento personal para sí mismo o para un tercero, en perjuicio de la entidad. Se encuentran dentro de este concepto las acciones ilícitas que persiguen la mejora de la valoración del desempeño, el cumplimiento de retos, permiten la mejora de incentivos o pretenden ocultar determinado hechos o situaciones que pueden influir negativamente en estas valoraciones.

- **Necesidad de colaboración o participación interna:** la acción precisa de participación de una persona vinculada con la entidad. Deberá existir prueba suficiente de dicha colaboración interna mediante propia investigación y/o fallo judicial que haya permitido identificar a él/los responsable/s. En caso de que no se den estas circunstancias el evento será clasificado como "fraude externo".

FRAUDE INTERNO: ACTIVIDADES NO AUTORIZADAS

El evento ha de aunar las dos condiciones indicadas (existencia de ánimos de lucro, aunque éste no pueda asociarse directamente a una ganancia económica, e intervención de una persona vinculada a la entidad) y se haya originado como consecuencia de la transgresión o incumplimiento de la

política, normas y procedimientos internos de la entidad y facultades o atribuciones otorgadas sin que la acción pueda ser calificada de delito.

FRAUDE INTERNO: HURTO Y FRAUDE

El evento ha de aunar las dos condiciones indicadas y que la acción pueda ser tipificada como delito según la legislación vigente (código penal) y sea sancionable por los órganos jurisdiccionales.

b) FRAUDE EXTERNO

Se catalogarán los eventos que presenten las siguientes causas:

- Intencionalidad y existencia de ánimo de lucro.
- Inexistencia de pruebas de colaboración o participación interna.
- Daños ocasionados en inmuebles en el supuesto de un intento de acceder a las instalaciones de la entidad en el caso de robos y atracos.
- Pérdidas derivadas de secuestros y sus eventuales rescates.

FRAUDE EXTERNO: HURTO Y FRAUDE

Pérdidas ocasionadas por las causas arriba citadas que no tengan su origen en la vulneración de la integridad de los sistemas informáticos.

No obstante, cuando el origen de las pérdidas sea por sustracción de soportes magnéticos o de base de datos o de información confidencial (códigos de accesos, claves, etc.) éstas se clasificarán en esta subcategoría.

FRAUDE EXTERNO: SEGURIDAD DE LOS SISTEMAS

Se incluirán las pérdidas provocadas por una acción externa mediante la vulneración de la integridad de los sistemas informáticos de la entidad

utilizando las líneas de comunicación existentes o las utilidades puestas a disposición de terceros.

c) RELACIONES LABORALES Y SEGURIDAD EN EL PUESTO DE TRABAJO

Incluye los eventos con pérdidas y deriva de actuaciones incompatibles con la legislación o con acuerdos relacionados con la gestión de recursos humanos:

RELACIONES LABORALES

Contiene todas las pérdidas relacionadas con los despidos improcedentes (relacionados con eventos operacionales y que no respondan a decisiones estratégicas o de negocio) y costes relacionados con eventuales demandas por incumplimientos de acuerdos laborales y prácticas de selección y contratación.

HIGIENE Y SEGURIDAD EN EL PUESTO DE TRABAJO

Eventos cuyas pérdidas están relacionadas con multas e indemnizaciones satisfechas como consecuencias del incumplimiento de la normativa laboral y de las condiciones de seguridad e higiene en el trabajo, accidentes laborales, etc. Se excluyen de esta categoría las originadas por la responsabilidad civil derivada de eventuales accidentes en el propio centro de trabajo que afecten a clientes u otras personas no vinculadas con la entidad, que se clasificará en la categoría de "clientes, productos y prácticas empresariales".

DIVERSIDAD Y DISCRIMINACIÓN

Agrupa todas las pérdidas relacionadas con demandas por prácticas discriminatorias en las políticas de retribución, o de selección, etc.

d) CLIENTES, PRODUCTOS Y PRÁCTICAS EMPRESARIALES

En esta categoría se incluyen los eventos con pérdidas derivadas:

- Del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos o de la naturaleza o diseño de un producto.
- Multas, sanciones, indemnizaciones y gastos ocasionados por litigios por infracciones de la normativa vigente y el marco jurídico existente cometidas por la entidad.
- Reclamaciones de clientes que hayan sufrido un quebranto económico o se consideren perjudicados por la acción u omisión de la entidad en la comercialización de productos o servicios.

ADECUACIÓN, DIVULGACIÓN DE INFORMACIÓN Y CONFIANZA

Se incluirán los eventos con quebrantos generados por reclamaciones de clientes en relación con el proceso de comercialización de productos o servicios. Por lo general, las causas se deberán a eventuales abusos de confianza, divulgación de información privada y confidencial, ventas agresivas realizadas por algún gestor comercial en las que se haya suministrado información parcial (sobre indicaciones financieras, precios, plazos…) o insuficiente (ocultación de riesgos asociados a un producto), etc.

PRÁCTICAS EMPRESARIALES O DE MERCADO IMPROCEDENTES

Agrupa los eventos con pérdidas (multas, sanciones, indemnizaciones y gastos) originadas por infracciones de la regulación vigente que, a diferencia de la anterior subcategoría, no haya sido realizada por un gestor individualmente sino como política de la entidad o de una de sus líneas. Son los eventos relacionados con prácticas ajenas a la competencia (aplicación de tarifas abusivas, acuerdos de precios entre partes que vulneren regulaciones sobre competencia, acciones para alterar los mecanismos de determinación de precios de mercados, etc.), utilización de información privilegiada en beneficio de la entidad, evasión de capitales, etc.

PRODUCTOS DEFECTUOSOS

Contiene las pérdidas cuya afectación es masiva (afecta a todos los contratos, o a un subconjunto de ellos, de un producto comercializado) originadas por sanciones y penalizaciones a consecuencia de su comercialización sin la respectiva autorización o por reclamaciones de clientes perjudicados por:

- Normas que contravengan la legislación.
- La utilización de modelos de valoración erróneos
- Sistemas de análisis de riesgos defectuosos, etc.

Si fueran consecuencia de incidencias concretas se clasificarán en la subcategoría anterior "prácticas empresariales o de mercado improcedentes".

SELECCIÓN, PATROCINIO Y RIESGOS

Incluye los eventos cuyas pérdidas hayan sido ocasionadas por reclamaciones de clientes que consideran se ha hecho un uso inadecuado de los condicionantes pactados con la entidad en la gestión discrecional de patrimonios.

ACTIVIDADES DE ASESORAMIENTO

Servirá para clasificar las indemnizaciones que se hayan satisfecho a clientes como resultado de pérdidas que tienen su origen en recomendaciones erróneas y/o asesoramientos deficientes.

e) DAÑOS A ACTIVOS MATERIALES

En esta categoría se clasificarán las pérdidas que hayan sido originadas por daños sufridos en activos materiales a consecuencia de desastres naturales u otros acontecimientos.

No todos los eventos en los que se produzca un daño en un activo físico deben ser clasificados dentro de esta categoría, sino que habrá que determinar cuál ha sido el factor determinante del evento, pues en caso de que el móvil haya sido obtener un beneficio ilícito la pérdida deberá clasificarse como "fraude interno" o "fraude externo".

f) INCIDENCIAS EN EL NEGOCIO Y FALLOS EN LOS SISTEMAS

Contempla las pérdidas que han sido causadas por fallos en los sistemas informáticos de la entidad, es decir, por un deficiente funcionamiento del hardware que dé servicio a la entidad (cualquiera sea su ubicación y su propiedad) y al software cuyo desarrollo, mantenimiento y/o implantación competencia exclusiva de la unidad de sistemas de información de la entidad.

Por tanto, los eventos originados por:

- El error derivado en la utilización de aplicaciones departamentales mantenidas por el usuario y otras herramientas ofimáticas puestas a su disposición, tales como hojas de cálculo, tratamientos de texto, etc. no deberán clasificarse en esta categoría, sino en "ejecución, entrega y gestión de procesos".
- El fallo de elementos del equipamiento técnico necesarios para la realización de cualquier trabajo en la entidad (sistemas de impresión, dispositivos de transmisión de imágenes, equipamiento de oficina-terminales, laptops, etc.) sí deberán clasificarse en esta categoría.
- Interrupciones de los servicios (agua, energía eléctrica, líneas de comunicaciones –voz y datos-, etc.) que ocasionen fallos en los sistemas, también deberán clasificarse en esta categoría.

g) EJECUCIÓN, ENTREGA Y GESTIÓN DE PROCESOS

En la presente categoría se incluirán las pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

Por tanto se encuadrará dentro de este grupo toda pérdida originada por un evento en el que concurran las siguientes condiciones:

- Que haya sido provocado por acción u omisión en la ejecución de operaciones, errores cometidos de forma involuntaria en la operativa y gestión de procesos.
- Que la transacción origen de la pérdida no se encuentre vinculada al proceso de comercialización de productos o servicios.
- Que no haya supuesto un beneficio directo para la entidad.

Son errores involuntarios en la ejecución de procesos cuya ejecución no ha supuesto un beneficio directo para la entidad.

RECEPCIÓN, EJECUCIÓN Y MANTENIMIENTO DE OPERACIONES

Incluye los eventos con pérdidas consecuencia de errores en la introducción y mantenimiento de datos, ejecución deficiente de procedimientos de control, fallos en los procesos de presentación de documentos y, en general, cualquier fallo en el funcionamiento de los procesos habituales de la entidad no contemplados en las siguientes subcategorías.

SEGUIMIENTO Y PRESENTACIÓN DE INFORMES

Pérdidas consecuencia de errores involuntarios en el suministro de información obligatoria para la entidad (en contenidos y plazos de entrega) que deba remitirse a terceros (clientes, inversores, organismos e instituciones, etc.) cualquiera que sea el medio el por el que se cursen (correo, fax, etc.), excepto si la transmisión se efectúa mediante sistemas telemáticos, en cuyo caso la pérdida se clasificará como "incidencias en el negocio y fallos en los sistemas".

ACEPTACIÓN DE CLIENTES Y DOCUMENTACIÓN

Se incluyen todas las pérdidas ocasionadas por errores cometidos en el proceso de formalización de cualquier tipo de contratos que ocasionen la inexistencia, pérdida o defectos de forma en los mismos (de clientes, proveedores, etc.) y los errores o deficiencias en la documentación y justificación de toda clase de operaciones que afecte a la fuerza ejecutiva del contrato o suponga el deterioro de la posición mantenida por la entidad en su defensa jurídica.

GESTIÓN DE CUENTAS CLIENTES

Se asignarán todas las pérdidas provocadas por la errónea ejecución o negligente tratamiento de instrucciones y órdenes impartidas por clientes. Estos errores pueden producirse en la ejecución de instrucciones individuales (generalmente cometidos por fallos cometidos por una sola persona) y suelen estar relacionados con transacciones como transferencias de fondos, domiciliación de pagos, etc.

CONTRAPARTES COMERCIALES

Agrupan los eventos con pérdidas causadas por el incumplimiento involuntario de obligaciones contractuales de la entidad con otras contrapartidas no clientes.

DISTRIBUIDORES Y PROVEEDORES

Incorporan todas las pérdidas derivadas de litigios mantenidos con proveedores y distribuidores en general y los que supongan una interrupción imprevista de servicios por parte del proveedor (por quiebra, huelga prolongada). Si la actividad que realiza un proveedor es, por su naturaleza, propia de la entidad, el evento se clasificará en la subcategoría "recepción, ejecución y mantenimiento de operaciones".

1.2.2.1.2.2. EVENTOS SEGÚN LÍNEAS DE NEGOCIO

La definición de un procedimiento de uso generalizado en la asignación de eventos a líneas de negocio resulta compleja debido a la diversidad de estructuraciones internas de las entidades; además, en muchos casos las líneas de negocio de la entidad no coinciden con las propuestas por Basilea II.

La dificultad aumenta cuando el evento se ha originado en unidades administrativas o de soporte comunes a diversas unidades de negocio. En estos casos la clasificación depende en cada entidad según criterios internos de distribución que deberán ser validados por los organismos supervisores.

a) FINANZAS CORPORATIVAS

Se entiende por finanzas corporativas los servicios financieros que pueda prestar una entidad financiera relacionados con las siguientes actividades:

- Operaciones financieras en el mercado de valores (salida a bolsa, ampliación de capital, emisión de bonos, etc.).

- Proceso de exclusión de los mercados financieros.
- Fusiones y adquisiciones.
- Privatizaciones.
- Emisiones de deuda y capital en mercados privados.
- Valoración de empresas.
- Dirección de préstamos sindicados (banco agente y/o banco asegurador).
- Banca de inversiones (toma de participaciones con carácter permanente, capital de riesgo).

b) NEGOCIACIÓN Y VENTAS

Recoge los resultados procedentes de las posiciones de la entidad mantenidas por motivos de negociación.

Esta posición se mantiene ex profeso para su venta a corto plazo y/o con el propósito de aprovechar fluctuaciones de los precios, reales o esperadas, a corto plazo, o de obtener beneficios procedentes del arbitraje. Comprende actividades de:

- Negociación de posiciones propias.
- Intermediación en el mercado monetario.
- Creador de mercado.

c) BANCA MINORISTA

Se compone por los ingresos obtenidos por intereses de préstamos y anticipos a clientes minoristas y a las PYME con tratamiento de minorista y a los clientes de banca privada, deduciendo los costes derivados de la financiación

de la inversión crediticia más las comisiones relacionadas con actividades minoristas tradicionales y los ingresos procedentes de los derechos de cobro adquiridos frente a minoristas, procedentes de las actividades típicamente minoristas como:

- Servicios bancarios (transferencias, cambio de moneda, etc.).
- Depósitos y fondos reembolsables.
- Financiaciones (préstamos, créditos, arrendamientos financieros, etc.).
- Prestación de garantías y avales.
- Asesoramiento inversión.

d) BANCA COMERCIAL

Se componen por los ingresos por intereses de préstamos y anticipos a empresas, bancos y a soberanos (deuda con el Estado), así como los ingresos procedentes de los derechos de cobro adquiridos frente a empresas y deduciendo los costes derivados de financiación con dicha inversión crediticia, más las comisiones relacionadas con actividades tradicionales de banca comercial, incluidos garantías, letras de cambio, etc.

e) LIQUIDACIÓN Y PAGOS

Recoge los ingresos brutos procedentes de comisiones, cuotas netas obtenidas por prestar servicios de liquidación y pago a contrapartes mayorista. Incluyen las siguientes actividades:

- Servicios de transferencia de fondos.
- Emisión y administración de medios de pago.
- Servicios de pago contra entrega de títulos.

f) SERVICIOS DE AGENCIA

Engloba los ingresos brutos procedentes del depósito y custodia de activos y ajenos a la entidad, incluyendo instrumentos de capital, depósitos y servicios similares tales como gestión de efectivo y garantías colaterales.

g) ADMINISTRACIÓN DE ACTIVOS

Recoge la administración de activos, fundamentalmente los ingresos procedentes de la gestión de patrimonios por cuenta de terceros, tales como:

- Gestión de fondos de inversión
- Gestión de fondos de pensiones
- Gestión discrecional de carteras (banca privada)

h) INTERMEDIACIÓN MINORISTA

Comprende los ingresos de gestión de órdenes para la contratación o venta de productos financieros en el mercado por cuenta de terceros:

- Recepción y transmisión de órdenes en relación con uno o más productos financieros.
- Ejecución de órdenes en nombre de terceros.

1.2.2.1.2.3. OTRAS CLASIFICACIONES DE EVENTOS

Para la gestión del riesgo operacional es conveniente tener los eventos clasificados por otros criterios que pueden ser de ayuda en la gestión (prevención y/o minoración) del riesgo.

Estos criterios pueden, a la vez, ayudarnos en la construcción de la información por líneas de negocio:

- **Procesos:** facilitan el establecimiento de medidas correctoras en aquellos procesos que presentan pérdidas. Asimismo, mediante la asignación de la responsabilidad de los procesos a líneas de negocio nos puede auxiliar en la clasificación por líneas de forma similar.
- **Productos:** permiten el seguimiento y análisis de los productos con mayor riesgo operacional en sus procesos y que precisan medidas correctoras para disminuir el riesgo operacional de la entidad. Asignando los productos a cada una de las líneas de negocio nos ayudará a la clasificación por líneas.
- **Clientes:** la segmentación de los clientes de la entidad ayudará, al vincular cada pérdida con el cliente o segmento de clientes afectados y obtener por agregación el importe total de pérdidas de cada segmento, a gestionar aquellos segmentos de clientes con mayor riesgo operacional. Mediante la asignación de cada segmento de clientes a una línea de negocio se podría obtener el total de pérdidas de una línea de negocio.
- **Centros:** algunas entidades cuentan con redes comerciales especializadas según negocio, de forma que oficinas físicas o contables e incluso sociedades jurídicas diferentes pueden identificarse formalmente con las líneas de negocio definidas por Basilea.

1.2.2.1.2.4. VALORACIÓN DE LOS EVENTOS

Criterios que facilitan la cuantificación de los eventos de forma homogénea, lo que permite obtención de resultados comparables y/o extrapolables al conjunto del sector.

a) Al identificar un evento se ha de considerar que éste puede generar múltiples pérdidas. La identificación y comunicación de eventos atenderá al evento principal (sin el cual, ninguna de las pérdidas asociadas se habrían producido).

Considerando estas premisas, se proponen las siguientes directrices:

- Los errores repetitivos se considerarán separadamente como eventos individuales.
- Impactos múltiples de un mismo suceso se agruparan en un mismo evento.
- Pérdidas aparentemente independientes, pero unidas por un plan de acción común, se considerarán como un único evento (por ejemplo una inundación que produce daños materiales en varias oficinas o un fraude realizado mediante múltiples transacciones).
- El impacto total de un evento deberá incluir todos los componentes de su cuantía, aun cuando parte de sus consecuencias o efectos se encuentren registrados en cuentas contables diferentes o estén contabilizadas en diferentes fechas.

b) Se recomienda incluir en el cálculo de la valoración únicamente los costes o gastos extraordinarios soportados por la ocurrencia del evento no deberán integrarse en la cuantía de la pérdida aquellos costes o gastos incurridos en la eliminación futura de los riesgos asociados a una determinada pérdida.

c) En el cálculo se debería incluir el coste de oportunidad en términos financieros (intereses y comisiones no percibidos), de operaciones realizadas pero no debería incorporar el lucro cesante asociado al evento (operaciones no materializadas o pérdidas de negocio derivadas del mismo).

d) En la valoración de las pérdidas de un evento en el que interviene alguna variable de mercado (tipo de cambio, de interés, precios de activos financieros, etc.) las pérdidas se deberían calcular aplicando los precios existentes en el momento de la identificación del evento.

e) Los eventos se deberían reportar siempre en una única moneda (si el impacto de un evento se ha producido en una moneda distinta), considerando el tipo de cambio existente a la fecha de contabilización en los libros de la entidad.

f) Si un evento de riesgo operacional afecta a activos fijos o activos inmateriales y la valoración se realiza atendiendo a criterios históricos, el impacto económico será, diferente al impacto contable. Con el objeto de fijar un criterio:

- Si el activo afectado es reemplazado se considerará como pérdida el precio de reposición del activo.
- Si el activo siniestrado no es reemplazado la pérdida se valorará teniendo en cuenta el precio de mercado del activo en el momento de producirse el evento. en el supuesto de que no sea conocido la pérdida se registrará considerando el valor del activo en libros.

1.2.2.1.2.5. RECUPERACIONES

Puede darse el caso de que se produzca recuperaciones, en parte o por el importe total, de las pérdidas. La recuperación constituye un hecho independiente del evento original y, por tanto, el evento se registrará por su impacto bruto.

Las recuperaciones se catalogan en:

a) **Recuperación directa:** es la que se logra tras las gestiones realizadas por la entidad. Por ejemplo en el caso de una entidad financiera, si se duplica una transferencia y el error no es detectado durante algún tiempo; cuando se identifica el error, la entidad recupera el importe de la pérdida de la contraparte.

b) **Recuperación indirecta:** es fruto de un acuerdo previo a la ocurrencia del evento suscrito anticipadamente con un tercero, como ocurre en el caso de indemnizaciones por el aseguramiento de siniestros. En consecuencia, las cantidades percibidas en concepto de seguros por siniestros se computarán de manera separada del importe de pérdida inicial (bruto) y del importe logrado por recuperación directa.

Se ha de procurar que todas las recuperaciones estén registradas en el base de datos de eventos de pérdidas, constando al nivel de evento la anotación del importe bruto de la pérdida y, perfectamente diferenciada, la anotación del importe de la recuperación, con una indicación explícita respecto al tipo de recuperación –directa o indirecta-, para facilitar el uso de la información a efectos de gestión del riesgo.

1.2.2.1.3. NATURALEZA E IMPACTO DEL RIESGO OPERACIONAL

Según (García Ribas, 2010) la principal característica del riesgo operacional es su extrema complejidad debido a la enorme variedad de causas que lo producen. En riesgo de crédito, solo hay una causa que produce el evento: el fallido o quiebra de la contrapartida. En riesgo de mercado la causa es el movimiento adverso del mercado, es decir, cuando los precios se mueven en la dirección opuesta a la que se ha pronosticado.

IMPACTO DEL RIESGO OPERACIONAL

El riesgo operacional se puede agrupar en cuatro categorías:

a) **Con impacto directo en la contabilidad:** cuando existe en la contabilidad que maneja la entidad una cuenta específica para reflejar esa pérdida sufrida como consecuencia de un evento, por ejemplo, un fraude. La totalidad del saldo de dichas cuentas corresponde a eventos de riesgo operacional. Por tanto, es fácil identificar el impacto del riesgo operacional.

b) **Con impacto indirecto en la contabilidad:** a menudo la contabilidad no diferencia entre las pérdidas debidas a eventos de riesgo operacional y los gastos ordinarios de una entidad. Un ejemplo sería los gastos incurridos al contratar una empresa de software para reparar o rehacer un programa que se ha dañado. En este caso, se ha producido un evento de riesgo operacional cuyo impacto es el coste de la reparación del mismo. Sin embargo, este gasto estará contabilizado junto con otros gastos ordinarios de informática, no atribuibles a eventos de riesgo operacional. Por tanto, los eventos que producen consecuencias indirectas permanecen ocultos en la contabilidad.

c) **Con impacto en lucro cesante:** determinados eventos de riesgo operacional no trascienden a la cuenta de resultados porque producen una pérdida de negocio futuro. Ejemplo de ello sería cuando un director de oficina se va a la competencia, llevándose con él a una parte de la clientela. Este tipo de eventos producen una pérdida de ingresos futuros o lucro cesante. Aquí la cuantificación es muy complicada porque el evento no ha dejado rastro contable. Solo se podría estimar el efecto.

d) **Sin impacto de ninguna clase:** puede ocurrir que un evento de riesgo operacional no tenga impacto económico. Determinados errores corregidos a

tiempo no trascienden. En estos casos, ni siquiera la estimación es posible. Sin embargo, es conveniente monitorizar estos eventos porque son el indicador de que algo está fallando.

RIESGO/BENEFICIO

Una característica de la naturaleza del riesgo operacional que lo diferencia del riesgo de crédito y del riesgo de mercado es que en el riesgo operacional se puede mantener un nivel bajo de riesgo sin perjudicar los beneficios, sin embargo en riesgo de crédito y de mercado el nivel de exposición determina casi siempre la expectativa de beneficio.

IMPACTO Y FRECUENCIA

Los eventos de riesgo operacional se caracterizan por dos parámetros: impacto y frecuencia. El impacto sería el valor económico del evento y la frecuencia se define como el número de ocurrencias anuales.

Atendiendo al efecto combinado de impacto y frecuencia, podemos distinguir claramente tres zonas:

a) **Zona de bajo impacto y baja frecuencia:** es la zona perfecta donde todos quisieran estar.
b) **Zona de bajo impacto y alta frecuencia:** es la zona donde mayormente se encuentran las entidades. es típico de la banca minorista, donde se producen muchos eventos pero de pequeño importe (por ejemplo: los fraudes de tarjetas de crédito). Cuando se encuentran en esta zona, las entidades deben gestionar para reducir la frecuencia mediante el establecimiento de controles o mejorando los existentes.

c) **Zona de alto impacto y baja frecuencia:** es la más peligrosa. Por tratarse de eventos de baja ocurrencia, en general corresponde a riesgos operacionales no identificados y, por lo tanto, no mitigados. Dado que no se puede gestionar la frecuencia, lo que se puede gestionar es el importe, es decir, si el evento ocurre (cosa inevitable) al menos que el impacto sea lo más pequeño posible. A esta zona también se le llama zona de plan de contingencia.

1.2.2.1.4. CAUSAS DEL RIESGO OPERACIONAL

El riesgo operacional está causado por muchos factores, la mayor parte de ellos son difíciles de identificar, incluso cuando ya se han producido los eventos. Sin embargo, la determinación de la causa del evento de riesgo operacional es fundamental para poderlo gestionar. Será necesario un análisis exhaustivo para llegar al fondo de la cuestión.

Aunque en teoría la secuencia de acontecimientos debería ocurrir: Causa – Evento – Consecuencia, en la práctica muchas veces las cosas suceden al revés o, mejor dicho, son descubiertas al revés. Por ejemplo, imponen una sanción económica a una entidad (consecuencia) por haber infringido una norma (evento) porque alguien sin conocimientos suficientes se equivocó (causa).

En este ejemplo podemos ver que la consecuencia es el detonante para reconstruir el evento, averiguar después cuál fue la causa y, por tanto, aplicar el remedio para que no vuelva a ocurrir (en este caso se daría formación a la persona que se equivocó).

TIPOLOGÍA DE LAS CAUSAS DEL RIESGO OPERACIONAL

El riesgo que causan los eventos es el que se llama riesgo residual, que no es más que la diferencia entre el riesgo intrínseco y el que somos capaces de mitigar mediante los controles.

Ejemplo: supongamos que queremos analizar el riesgo de error al marcar en el computador una orden de trasferencia que un cliente ha remitido por escrito. Si el formulario tiene 10 campos que debemos pasar a la aplicación, nos podríamos equivocar en cualquiera de ellos. Eso sería el riesgo operacional intrínseco.

Sin embargo, la aplicación informática que utiliza la entidad financiera incorpora una serie de filtros (controles) y campos automáticos que limitan las posibilidades de error (fecha, dirección, comisión de transferencia calculada, etc.). Gracias al diseño de la aplicación, el riesgo operacional intrínseco se ha visto reducido y el riesgo restante, aquél que no se puede evitar, se llama riesgo operacional residual.

Este ejemplo sirve para fijar los dos grandes grupos de causas del riesgo operacional:

- Las causas asociadas al riesgo operacional intrínseco.
- Las causas asociadas a controles deficientes y que, por tanto, también aumentan el riesgo residual.

En cuanto al primer grupo, podemos distinguir entre:

a) Recursos humanos:

- Perfil / formación de los RRHH.
- Rotación de recursos claves.
- Temporalidad.

Esta categoría es una de las más importantes, ya que sin una adecuada política de gestión de RRHH no se puede pensar en gestionar correctamente el riesgo operacional.

b) **Volúmenes:** los volúmenes de transacciones procesadas influyen en el riesgo operacional.

c) **Manualidad de procesos:** la escasa o nula mecanización de los procesos es una fuente de riesgo operacional.

d) **Tecnología:** aunque detrás de la tecnología siempre suele haber una persona, es conveniente segregar este segundo grupo de causas intrínsecas. Aquí englobamos tanto los aspectos de hardware (computadores, cableado, servidores, etc.), como los de software (conjunto de programas que rigen los aplicativos).

e) **Externas:** están constituidas por un conjunto de causas ajenas a la entidad, como son los grandes desastres (inundaciones, temblores, incendios, etc.).

En relación al segundo grupo de controles deficientes tenemos:

- *Seguridad física:* se refiere a los sistemas de seguridad tradicionales, como las alarmas antirrobo, controles de acceso en edificios, cajas fuertes, etc.
- *Seguridad lógica:* es la controla los accesos a los sistemas, ya sea la que protege los aplicativos como la referente a accesos por internet.
- *Segregación funcional:* cuando un mismo individuo puede ejecutar dos o más funciones incompatibles entre sí, se genera un riesgo evidente de fraude interno.

- *Adecuación de los aplicativos:* en muchos casos los aplicativos no incorporan los elementos de filtrado necesarios para mitigar el riesgo operacional o no cumplen los objetivos para los que fueron diseñados.
- *Documentos:* toda la operativa que se realiza debe quedar documentada (firma de contratos de descuentos) y comunicaciones a los clientes. Si esa documentación no se ajusta a derecho, la entidad pierde protección jurídica y por consiguiente puede dar lugar a pérdidas operacionales.

1.2.3. GESTIÓN DEL RIESGO OPERACIONAL

1.2.3.1. MARCO DE GESTIÓN

Según (Fernández Laviada & Martínez García, 2010), el riesgo operacional inherente a toda actividad, difícil de discernir, cuantificar y gestionar, representa uno de los grandes desafíos a los que enfrentan las instituciones del sector financiero; por lo que es necesario implementar un marco de gestión que permita un manejo adecuado de éste:

i. Organización

Definir un modelo organizativo adecuado es uno de los factores clave para configurar el marco de gestión del RO, tradicionalmente el departamento de auditoría interna se responsabilizaba de verificar la existencia de los adecuados controles para mitigar las pérdidas operacionales. El gran reto de las entidades está en crear un modelo organizativo que fomente el tratamiento homogéneo de la información sobre RO dentro de toda entidad, que asigne claramente las responsabilidades de gestión, control y supervisión y que cuente con una unidad centralizada de gestión del RO independientemente del departamento de auditoría interna, tal y como lo recomienda Basilea.

Dentro de una estructura, el primer paso es definir y contar con un responsable y, para ello, la creación de un departamento específico para RO debe ser la opción más acertada.

ii. Herramientas

El desarrollo del marco de gestión del riesgo operacional (RO) se fundamenta en el empleo de un conjunto de herramientas que permitan identificar y capturar las pérdidas operacionales así como la evaluación, seguimiento, control y reportan de los distintos riesgos: ***a) Base de datos de eventos***. Debe permitir capturar, autorizar y realizar un seguimiento adecuado de los eventos o sucesos de RO. que se producen en cada entidad, conocer el número y nivel de pérdidas, mitigar las mismas y, posteriormente cuantificar el capital mediante el modelo avanzado, en el caso en que este último se estime necesario tras el análisis previo de todos los costes y beneficios implicados. Además, la base de datos de eventos debe cumplir con dos objetivos generales: por un lado facilitar la gestión directa y el control local de los eventos ocurridos en cada una de las entidades y, por otro, permitir la

consolidación e integración de todos los eventos experimentados por la entidad para llevar a cabo un seguimiento y control global de los mismos, cumplir con las necesidades de reporting a la alta dirección y facilitar así el impulso de medidas de mitigación a nivel global; ***b) Cuestionarios de autoevaluación:*** El objetivo del cuestionario es identificar y evaluar, a través de una metodología principalmente cualitativa, el RO al que se expone la entidad o el área correspondiente en el desarrollo de su actividad a lo largo de sus procesos. Se compone de una lista de riesgos o preguntas que hacen referencia a todos los riesgos significativos a los que puede estar expuesta una entidad. El proceso para la identificación de estos riesgos es múltiple, pero habitualmente suele consistir en reuniones de trabajo con los expertos de cada una de las líneas de negocio o soporte para revisar las actividades, los procesos operativos y los controles establecidos. Otra vía es solicitar primero a dichos expertos la identificación de esos riesgos y después proceder a una revisión de los mismos. En cualquier caso, la responsabilidad última en este proceso recae en los propios expertos de líneas de negocio o soporte de la entidad; ***c) Indicadores de riesgo operacional:*** Los indicadores de RO (KRI´s de forma abreviada) permiten conocer el nivel de riesgo de una entidad de negocio en función de su actividad, el grado de gestión existente, o el correcto desempeño de los controles operativos de acuerdo con los niveles objetivo que se hayan establecido en cada caso. Normalmente muestran información resumida sobre el control y la actividad que se mide (estadísticas operativas y de personal, cuadres, conciliaciones, etc.) y generalmente se apoyan en las propias mediciones efectuadas por las áreas o departamentos de la entidad en su operativa diaria. Los valores de los indicadores deben servir, por un lado, para crear bases de datos y series históricas que permitan conocer en un futuro la existencia de correlaciones entre dichos valores y las

pérdidas de la base de eventos, y, por otro lado, para vincularlos directamente a la contestación de ciertas preguntas incluidas en los cuestionarios, buscándose también encontrar, de manera general, posibles correlaciones entre los mismos. La definición correcta de los indicadores es el punto más importante de todo el proceso. Para ello los coordinadores de RO de las unidades de negocio y soporte deben acordar cuáles serán los KRI´s más relevantes que se utilizarán, las características de los mismos y cómo se realizará exactamente la medición para obtener el valor final del KRI que debe imputarse en la base de datos de indicadores.

En el ámbito concreto del RO., se pueden identificar tres tipos de indicadores relevantes: **1)** ***Indicadores Descriptivos de Riesgo (Key Rish Indicators o KRI):*** tratan de cuantificar el nivel de riesgo de la entidad y se suelen configurar en función del grado de relevancia y representatividad a partir de los indicadores de rendimiento y de control; como por ejemplo: volumen de operaciones, rotación de personal, número de veces que cae el sistema, etc.: **2)** ***Indicadores Clave de Rendimiento o Volumen (Key Performance Indicador o KPI):*** se utilizan para controlar la eficacia operativa y activan señales de alerta si su valor se mueve fuera del ámbito establecido. Estas variables suelen proporcionar información sobre aspectos clave de la dimensión de la actividad como tamaño, volumen, importes, etc., que de uno u otro modo tienen relación directa con eventos de pérdida de tipo operacional; ***3) Indicadores Clave de Control (Key Risk Control o KCI):*** tratan de reflejar la efectividad de los controles; como por ejemplo: número de autorizaciones, números de confirmaciones pendientes, etc. (Vázquez Alonso, 2010).

La funcionalidad de una herramienta de indicadores de riesgo: requisitos particulares que debería cumplir una herramienta de indicadores:

- **Accesos:** todas las entidades deberían poder acceder a una base de datos corporativa de indicadores, pudiendo adaptar las características generales o específicas de los indicadores a las particularidades locales, según los criterios y perfiles establecidos;
- **Creación de indicadores por criterios:** ámbito (grupo, país, entidad), tipo de indicador (actividad y control) y tipo de captura (manual, automática), incorporando las características más relevantes de cada uno de ellos (periodicidad, tipo de riesgo, línea de negocio. Control, etc.)
- **Información básica del indicador:** descripción, tipo de indicador, tipos de riesgo y líneas de negocio, productos, controles y procesos asociados, etc.
- **Establecimiento de los umbrales o intervalos del indicador:** según el ámbito correspondiente, éstos podrían ser imputados manualmente por el experto o bien calculados centralmente a partir de dos parámetros (media y desviación típica) de las distribuciones de valores de los indicadores.
- **Envíos automatizados del indicador:** envíos a los usuarios según la periodicidad de envío establecida, con la posibilidad de hacerlo a petición.
- **Gestión de mediciones según plazos:** avisos a usuarios de las mediciones pendientes de indicadores que hayan pasado el periodo máximo de contestación.
- **Autorización:** validación de las mediciones de los indicadores, siguiendo un circuito de autorizaciones determinado.
- **Gestión de indicadores:** alta, baja, modificación y propagación del indicador, según los perfiles establecidos.

- **Obtención de puntuaciones de riesgo:** cualquier indicador debe permitir obtener, además de valores o mediciones, puntuaciones de riesgo. Son los intervalos del indicador los que nos permiten transformar las mediciones o valores de los indicadores a puntuaciones de riesgo.

Para poder obtener resultados agregados de los indicadores, es muy importante poder automatizar el proceso en función de la periodicidad del indicador y del periodo en que se realizan los cálculos. En este sentido los tipos de agregación posibles son los siguientes: suma, media, último dato, inserción, inserción repetida. Cada uno de ellos se utiliza en función de que la periodicidad del indicador sea menor o mayor a la periodicidad del informe que se realice. La utilización de un tipo concreto de agregación dependerá del tipo de indicador que se trate.

iii. Reporting

Dentro de todo marco de gestión de RO debe estar siempre incluida la función de reporting, que para ser eficaz debe asegurar que la información es comunicada con un grado de detalle diferente según receptor. Lógicamente las áreas de negocio y riesgos, junto al departamento de auditoría interna, recibirán más información y más detallada que la alta dirección y el Consejo de Administración, pero todos deben recibir informes sobre la situación del RO en la entidad.

1.2.3.2.ESTRUCTURAS DE GESTIÓN

Históricamente el riesgo operacional se ha gestionado de formas muy distintas. Cada entidad tiene una sensibilidad propia. El modelo de gestión que veremos a continuación se podría definir como un modelo híbrido, en el cual las áreas de negocio y las de control de riesgos comparten la gestión con cierto grado de independencia. Auditoría interna

también interviene en su rol habitual de revisión de los procedimientos y de la calidad de la información.

IMPLICACIÓN DEL CONSEJO DE ADMINISTRACIÓN/ALTA DIRECCIÓN

Los consejos de administración de las entidades deben ser conscientes de que el riesgo operacional es una clase distinta de riesgo que debe ser gestionada. Por tanto, sus funciones principales serían las siguientes:

- Aprobar la implantación del marco de gestión de riesgo operacional en la entidad, como una forma distinta de riesgo.
- Determinar, dentro de ese marco de gestión, los niveles de riesgo deseados por cada unidad de negocio/soporte.
- Aprobar la implantación de una estructura de gestión adecuada, en áreas centrales y en las unidades de negocio/soporte.
- Revisar de forma periódica el marco de gestión, con el objetivo de actualizarlo en función de la experiencia y las recomendaciones del Comité de Basilea.
- Asegurar que el marco de gestión del riesgo operacional y la información que se maneja se revisen regularmente por una auditoría independiente (interna y/o externa).

Los comités de dirección son los órganos responsables de llevar a cabo la implantación del marco de gestión aprobado previamente por el consejo de administración a través de toda la organización, asegurándose de que todo el personal conozca y entienda sus responsabilidades en la gestión de esta clase de riesgos. Sus principales funciones serían:

- Trasladar el marco de gestión aprobado por el consejo de administración en materia de políticas y procedimientos de trabajo a todas las unidades de negocio/soporte.

- Establecer una política de comunicación interna para asegurar que el personal esté informado.
- Incentivar la gestión del riesgo operacional mediante políticas de compensación y reconocimiento.
- Fomentar un ambiente de control y el uso de las herramientas de gestión del riesgo operacional.
- Dedicar recursos para la formación profesional de la plantilla en esta materia.

1.2.3.2.1. EL COMITÉ DE RIESGO OPERACIONAL

El comité de riesgo operacional es un órgano fundamental en la gestión del riesgo operacional de una entidad. Para llevar a cabo la mitigación es necesario contar con mecanismos de decisión que cubran todos los aspectos relevantes.

El comité de riesgo operacional estará constituido por el presidente (preferentemente un miembro del comité de dirección de la unidad), el secretario (coordinador del riesgo operacional de la unidad) y los miembros (un representante de cada una de las funciones presentes en la unidad). Es aconsejable que las personas que componen el comité conjuguen un conocimiento global de los procedimientos con una capacidad ejecutiva que facilite la toma de decisiones y su implantación.

El comité debe reunirse de forma periódica (mensual, trimestral, etc.) salvo en casos de emergencia (desastres, eventos graves, etc.), se debe hacer sobre la marcha.

Las funciones del comité son las siguientes:

- Analizar la situación actual de la unidad comparándola con el nivel de riesgo óptimo para cada uno de los factores de riesgo a que está expuesta.
- Establecer las medidas de mitigación adecuadas a fin de alcanzar los objetivos de riesgos definidos.
- Efectuar el seguimiento del nivel de riesgo operacional a través de la información proporcionada por las herramientas.
- Decidir cuándo es necesaria una actualización de las herramientas de gestión del riesgo operacional por causas de cambio de negocio, nuevos productos, cambios en los procesos, implantación de nuevos sistemas, etc.

Para cada factor tratado en el comité se estudiará el riesgo, valorando posibles soluciones y el coste de cada una de ellas, y se tomarán decisiones en términos de coste/beneficio sobre la solución a adoptar. El resultado final de este proceso será un plan de acción individualizado, con una descripción de la acción de mitigación acordada, la fecha de implantación prevista y la persona responsable de llevar a cabo la acción.

UNIDADES DE RIESGO OPERACIONAL

Ubicadas en el área de riesgos, constituyen el siguiente eslabón dentro de la estructura de gestión de la entidad. Estas unidades serán las responsables de la implantación del modelo de gestión apropiado. Para ello, las unidades de riesgo operacional diseñan y actualizan periódicamente las herramientas de gestión. La implantación se realiza en coordinación con las unidades de negocio y apoyo quienes, a su vez, nombran un responsable o coordinador del riesgo operacional.

Las unidades de riesgo operacional se encargan de difundir su conocimiento mediante cursos y presentaciones a las líneas de negocio/apoyo, fomentando así

una cultura común en torno a un lenguaje propio. Una vez implantada la estructura de gestión, es necesario establecer dos modelos de gestión diferenciados, el cualitativo y el cuantitativo.

LÍNEAS DE NEGOCIO Y CLASES DE RIESGO

Lógicamente las distintas tipologías de productos --y por consiguiente procesos- que se realizan en las entidades implican que los riesgos operacionales a los que están expuestos y los eventos que se producen sean distintos.

Estas diferencias las podremos ver por el tamaño de los eventos, por su recurrencia y por la clase de riesgo.

El Comité de Basilea propone que se analice el riesgo operacional por líneas de negocio y, para ello, propone una segmentación cuyo primer nivel es el siguiente:

a) Banca corporativa (gran empresa).

b) Banca minorista (individuos).

c) Banca de empresas (pequeñas y medianas empresas).

d) Tarjetas de crédito (como emisor).

e) Tesorería.

f) Gestión de activos.

g) Pagos y cobros (negocio de corresponsalía).

h) Intermediación minorista (sociedad de bolsa).

Es difícil encontrar entidades que posean todas estas líneas de negocios, incluso no es fácil que coincidan exactamente. En la práctica cada entidad utiliza las suyas.

En cuanto a la clase de riesgo, el Comité de Basilea también ha propuesto unas categorías estándares, que son las siguientes:

a) Ejecución de procesos.

b) Fraude interno y actividades no autorizadas.

c) Fraude externo.

d) Tecnología (hardware y software).

e) Recursos humanos (políticas de RRHH, normativa laboral, etc.).

f) Prácticas comerciales (formas de comercializar los productos).

g) Desastres (incendios, inundaciones, accidentes, etc.).

La combinación de líneas de negocio y clase de riesgo determina una tipología específica de riesgo operacional. En total hay 56 combinaciones posibles que permiten entender y controlar mejor el riesgo operacional cuando éste se materializa en forma de eventos. A la hora de mitigar, no es lo mismo el riesgo de fraude interno (que se controla mediante la segregación funcional y la seguridad lógica) que los desastres (que se suavizan a través de planes de contingencia).

1.2.3.3.RIESGO OPERACIONAL EN EL GOBIERNO CORPORATIVO

Según (Arcenegui Rodrigo & Vicente, 2010) Los continuos escándalos financieros ocurridos en las últimas décadas son, muchos de ellos, ejemplos clásicos de fallos operacionales en las entidades. En última instancia, los mayores perjudicados por estos escándalos han sido los accionistas de las entidades, que han pagado el precio de los mismos de una u otra forma.

El análisis de los distintos casos de escándalos nos aporta una serie de factores comunes a todos ellos:

- Falta de lealtad y responsabilidad de los administradores, accionistas mayoritarios y directivos.
- Falta de transparencia.
- Deficientes sistemas de supervisión de los controles.
- Falta de eficacia del auditor externo.
- Comportamientos poco éticos e independientes de los que componen las organizaciones.
- Lentitud o falta de eficacia de los supervisores.

En definitiva, estos factores nos muestran que las causas de los distintos escándalos financieros son deficiencias y fallos en los procesos de las entidades.

El riesgo operacional se define como aquél al que está expuesta una entidad de sufrir pérdidas como consecuencia de procesos internos, personas o sistemas inadecuados o defectuosos, o por causas externas. Por tanto, la primera aproximación a la relación existente entre el riesgo operacional y el gobierno corporativo se encuentra relacionada con la consecución de los objetivos de los accionistas, es decir, la obtención de una adecuada retribución a sus inversiones, lo que se conoce hoy en día como la creación de valor para el accionista. Una adecuada gestión del riesgo operacional en las entidades crea valor para el accionista a través de la mejora competitiva y reduciendo el nivel de pérdidas operacionales en la entidad.

Las nuevas formas de propiedad –fondos de inversión, planes de pensiones, etc.- han puesto de manifiesto la necesidad de mayor protección de los accionistas al aumentar la distancia entre el propietario inversor y el consejo de administración, así como la

necesidad de buscar soluciones para fomentar la participación de los inversores institucionales en el gobierno de las sociedades.

Por otro lado, hoy en día no se concibe a las entidades como meros entes mercantilistas, ahora ya que la sociedad entra a formar parte de ese conflicto de intereses como comunidad social en la que se integra la empresa y que puede soportar los costes de cierre de plantas o negocios auxiliares, el trabajo de otros miembros de la familia del trabajador, viviendas, estudios y el conjunto de relaciones sociales de la zona de influencia de la empresa. De esta forma se pone en manifiesto lo que se ha denominado "responsabilidad social de la empresa".

Las dos realidades descritas nos llevan a entender que todos los propietarios de recursos aportados tienen intereses por conocer cómo se invierten dentro de la empresa, dado que en función de esto obtendrán sus rentas futuras. El gobierno corporativo en términos de colectivos interesados, admitiendo que no solo los accionistas tienen derechos a cambio de su capital sino que todos los propietarios de recursos aportados (capital, mano de obra, materia prima, etc.) tienen que recibir rentas de la empresa, consiste en repartir correctamente esas cuasi-rentas de forma que se maximice el bienestar de todos los colectivos interesados.

Ahora bien, la intervención de todos los interesados en los mecanismos previstos de control no suelen ser eficientes debido a los distintos intereses encontrados y la lentitud que provocan en los procesos de toma de decisiones. Por tanto, ante la imposibilidad o suficiencia de un sistema de voz de todos los interesados en todos los órganos de gobierno, se debe acudir a la protección contractual o la regulación.

La protección contractual de los acreedores se manifiesta mediante la estipulación de un interés fijo pactado, garantías adicionales en el caso de impago, plazos anuales de

vencimiento que ofrecen la posibilidad de renovación, derechos de decisión en el caso de suspensiones de pagos o quiebras y el derecho a convertir la deuda en acciones. Todo ello constituye un conjunto de salvaguardas para los intereses de los acreedores.

En el caso de los trabajadores, su protección contractual es más teórica que real, dado que si bien disponen de un sueldo fijo y la posibilidad de abandonar la empresa con pocas restricciones, para que esto sea efectivo es necesario un mercado de trabajo perfecto en el que no haya dificultad para encontrar empleos alternativos similares.

Por último, cuando existe una gran desigualdad entre las partes, como puede ser el caso descrito de los trabajadores con los directivos o los acreedores en el caso de las empresas financieras, hay que recurrir a la intervención del poder público para evitar situaciones de abuso. Allí donde no llega el altruismo de los directivos, ni los incentivos, ni el control compartido, ni la protección contractual, debe llegar el Estado mediante la regulación y la supervisión de la toma de decisiones para asegurar razonablemente los intereses de todos los afectados.

1.2.3.3.1. ESTRATEGIA EMPRESARIAL Y LOS VALORES CORPORATIVOS

(ASBA, 2015), establece como principio general que, las entidades deben contar con una estrategia aprobada por el Directorio estableciendo principios para la identificación, medición, control, monitoreo y mitigación del riesgo operativo.

Las estrategias y políticas deberían ser implementadas por la Función de Gestión de Riesgo, responsable de identificar y gestionar todos los riesgos. La Función de Gestión de Riesgo puede incluir sub-unidades especializadas por riesgos específicos.

Las entidades deberían desarrollar su propio enfoque y metodología para la gestión de riesgos, de acuerdo con su objeto social, tamaño, naturaleza y complejidad de

operaciones y otras características. La implementación del sistema de gestión de riesgo operativo debería considerar todas las etapas de gestión de riesgo, incluyendo la identificación, evaluación, medición, monitoreo y control.

Sin objetivos no se puede gobernar una empresa, por ello es necesario tenerlos enunciados en todo momento y desarrollados en todos sus detalles. Como señala el Informe del comité de Basilea (2006), la ausencia de una estrategia empresarial y una adecuada planificación suele tener consecuencias que constituyen el origen de las mayores pérdidas empresariales hasta el extremo de condicionar la supervivencia. Adicionalmente, la comunicación de los objetivos estratégicos y los valores corporativos a todas las partes interesadas en la empresa (clientes, proveedores, empleados, directivos, supervisores, etc.) es un elemento clave para lograr su efectividad.

El riesgo asociado a la actividad descrita es un riesgo estratégico puro, excluido de la definición de riesgo operacional adoptada por Basilea II. Pero este riesgo estratégico es origen de una serie de riesgos operacionales. Así, ante la ausencia de una correcta definición de la estrategia y objetivos, las entidades se encuentran expuestas a ineficiencias en las acciones comerciales, falta de racionalización del gasto, etc.

El establecimiento de unos valores corporativos que fomenten la discusión interna franca y en tiempo de los problemas de la empresa facilita una correcta solución de los mismos. Igualmente, los valores deben dejar claro que las prácticas corruptas y los sobornos están prohibidos en las actividades de la empresa. En concreto, el consejo de administración debe asegurar que se establezcan políticas que delimiten la calidad del gobierno corporativo en relación con los valores corporativos, tales como:

a) Conflicto de interés:

b) Idéntico tratamiento para los familiares y otras partes vinculadas.

Estas operaciones deben ser conocidas por el consejo de administración y constituir el objeto de revisión por parte de los auditores internos y externos, de forma que se asegure que no se está infringiendo pérdidas a la empresa.

La ausencia de políticas adecuadas sobre valores corporativos expone a la entidad a riesgos tales como la realización de acciones no éticas amparadas bajo un vacío de normativa interna que suelen llevar aparejadas una falta de medios para poderlas sancionar de forma adecuada.

1.2.3.3.2. EL COMPORTAMIENTO ÉTICO Y UN ADECUADO SISTEMA DE CONTROL INTERNO

El buen gobierno corporativo se reduce a que propietarios, administradores y directivos mantengan una conducta adecuada e implanten un correcto sistema de control interno para hacer que el resto de la organización evite comportamientos poco éticos que conlleven fraudes, enriquecimientos de dudosa legitimidad u otras irregularidades.

El informe COSO (1997, pp. 31-2) relaciona tres razones por las que se realizan prácticas fraudulentas o cuestionables: los incentivos, las tentaciones y la ignorancia. El informe continúa indicando que la condición suficiente para implantar la ética empresarial es el ejemplo, dado que los empleados suelen imitar a sus líderes. Los códigos de conducta constituyen una herramienta básica de autorregulación para cumplir con las mejores prácticas del gobierno corporativo. Los aspectos que suelen regular los códigos éticos son los siguientes:

- Responsabilidad de los altos cargos:

- Obligación de cumplir la legalidad.
- Asunción de los valores y misiones de la entidad.
- Lealtad y buena fe.
- Mantenimiento de una conducta social y pública.

- Independencia y objetividad en el desarrollo profesional:
  - Prioridad de los intereses empresariales frente a los particulares.
  - Evitar los conflictos de intereses.
  - Discreción y secreto profesional.
  - Tratamiento adecuado de la información privilegiada.
  - Adquisiciones y ventas de propiedades, comunicación de posiciones deudoras, tratamiento ético en la prestación de servicio al cliente, no aceptación de obsequios, etc.

En resumen, en la entidad debe imperar la confianza, la integridad, el juego limpio y el respeto por los demás. No existe sustituto para la honestidad de las personas que componen una entidad. La ausencia de estas "reglas de juego" expone a la entidad a distintos riesgos operacionales cuyas características fundamentales son:

- Son riesgos de baja frecuencia, es decir, no se producen en las entidades de forma recurrente, lo que no nos debe llevar a pensar que no existen.
- Muchos de ellos suelen ser riesgos de alto impacto, es decir, una vez que se materializan producen quebrantos de importancia en el patrimonio de las entidades.
- Son riesgos de difícil cuantificación, que pueden provocar pérdidas explícitas, implícitas en otras pérdidas de la entidad o pérdidas no contables, que generen un lucro cesante para las entidades.

- Son riesgos operacionales con un alto potencial de generar otros tipos de riesgos que en ocasiones tienen mayores consecuencias, como el riesgo reputacional, es decir incrementan la percepción de incertidumbre de resultados y la percepción de la entidad por parte de la sociedad.
- Son riesgos de difícil gestión, que únicamente pueden ser abordados por la propia entidad definiendo de forma detallada los comportamientos y acciones no deseables y estableciendo las acciones correctoras cuando sean detectados a través de un sistema de control, tanto interno como externo, a lo largo de toda la organización.

1.2.3.4.CICLO DE GESTIÓN DEL RIESGO OPERACIONAL

Según (García Ribas, 2010) La gestión del riesgo operacional se basa en un ciclo de gestión que consta de cuatro fases bien diferenciadas:

a) **Identificación:** en esta fase identificamos el riesgo operacional al que estamos expuestos, utilizando para ello tanto las técnicas cualitativas como las cuantitativas. También se puede obtener información muy útil procedente de los reguladores y de las auditorías internas y externas.

b) **Cuantificación:** sirve para asignar el grado de importancia a cada factor de riesgo. Se puede hacer de varias maneras: si se tiene datos reales, el importe anual de pérdida será una buena medida, si no lo hay, se deberá estimar impacto y frecuencia anual.

c) **Mitigación:** una vez conocida la importancia de cada factor de riesgo operacional, debemos proceder a la mitigación de aquellos que pueden ser relevantes. Mitigar significa reducir o eliminar el riesgo. Para ello, es necesario crear un comité de riesgo operacional cuya misión consistirá en analizar las distintas opciones posibles,

en términos de coste/beneficio. No tendrá ningún sentido mitigar riesgos cuyos efectos costaran a la entidad menos dinero que la mitigación en sí.

d) **Seguimiento:** consiste en monitorizar la evolución del riesgo a lo largo del tiempo. El seguimiento es indispensable si se lleva a cabo algún tipo de mitigación para probar que esta se produce en los términos en que se planeó. El seguimiento debe efectuarse tanto en la parte cualitativa como en la cuantitativa.

1.2.3.5.MÉTODOS DE LA GESTIÓN DEL RIESGO OPERACIONAL

1.2.3.5.1. GESTIÓN CUALITIVA DEL RIESGO OPERACIONAL

La gestión cualitativa del riesgo operacional es aquella que se realiza sin necesidad de experimentar eventos, es decir, sin que el riesgo llegue a materializarse en la organización.

Se puede hacer de muchas maneras, sin embargo, la más extendida consiste en utilizar cuestionarios que las distintas áreas del negocio y soporte cumplimentar. Cada entidad, ya sea individualmente o con la ayuda de una consultora, debe diseñar una batería de preguntas que varían en función de la actividad cuyo objetivo es auto-evaluar de qué forma se está gestionando el riesgo operacional.

Los cuestionarios deben ser cumplimentados por expertos de las unidades, es decir, personas que conozcan a fondo los procesos que se llevan a cabo y las incidencias que se registran.

Las conclusiones que se pueden extraer son múltiples. En primer lugar se podrá conocer de forma global el nivel de exposición de la unidad revisada, además se conocerá también los factores de riesgo a los que está expuesta y, por consiguiente,

se podrán tomar medidas correctoras para mitigar el riesgo operacional sin que se hayan producido eventos.

Este último punto es especialmente importante. Si analizamos los grandes eventos ocurridos en el sector financiero en los últimos 10 años, observaremos que en la mayor parte de ellos había signos claros de debilidades de control que justamente fueron aprovechadas para meter transacciones fraudulentas en los libros.

La gestión cualitativa es, por consiguiente, muy importante. Debe de formar parte de la cultura corporativa, debe estar al alcance del mayor número posible de empleados, para que cada uno actúe como policía denunciando situaciones anómalas.

Con la gestión cualitativa se pueden identificar factores de riesgo importantísimos como, por ejemplo: la inexistencia de los planes de continuidad de sistemas, la falta de segregación funcional, las debilidades en los controles, etc. Se trata, pues, de una medida preventiva para la organización.

1.2.3.5.2. GESTIÓN CUANTITATIVA DEL RIESGO OPERACIONAL

La gestión cuantitativa está basada en la experiencia. Consiste en recoger en una base de datos todas las pérdidas que se van produciendo en nuestra organización. El análisis de los datos registrados nos proporciona información acerca del riesgo operacional y por consiguiente podemos determinar cuáles han sido las causas del mismo para poder actuar sobre ellas.

Para comprender mejor el riesgo al que se está expuesto es muy importante que las pérdidas que se recogen se clasifiquen por líneas de negocio y clases de riesgo, algo que también forma parte de las recomendaciones del Comité de Basilea.

Las bases de datos nos hablan del pasado, y solo tienen naturaleza predictiva en aquellas celdas que contienen eventos de alta recurrencia. De hecho, uno de los grandes problemas a los que se enfrentan las entidades que solo gestionan cuantitativamente es que no pueden saber su nivel de exposición a eventos de baja frecuencia como desastres o grandes fraudes, porque lo más normal es que no los hayan sufrido en el pasado.

La utilidad de una base de datos es doble, por un lado podemos gestionar mejor el riesgo operacional y por otro nos proporciona la información necesaria para calcular nuestro capital de riesgo. Sin embargo, esta información no es suficiente, porque en muchos casos los datos almacenados en las son insuficientes para calcular el capital de riesgo. Entendiendo que cada celda es la intersección de una línea de negocio con una clase de riesgo operacional, por tanto, bajo el esquema del Comité de Basilea habría 56 celdas.

Para solucionar este problema, algunas entidades han recurrido a las bases de datos externas que proporcionan datos complementarios que pueden mezclarse con los propios para determinar el CaR, Capital at Risk o capital de riesgo.

1.2.3.5.3. INTEGRACIÓN DE LOS MÉTODOS CUALITATIVO Y CUANTITATIVO

Según (Gimeno Coma, 2010), el objetivo principal en un modelo de riesgo operacional debe ser el llegar a conocer el perfil de riesgo de la entidad. Éste es el primer paso para poder gestionar su exposición al riesgo y, por supuesto, calcular el consumo de capital.

Pero, ¿qué quiere decir conocer el perfil de riesgo? Parece una pregunta simple: se considerará uno o varios indicadores de exposición y así se medirá el perfil de riesgo de una manera más o menos sofisticada en función del método seleccionado

(básico, estándar o avanzado). Pero esa pregunta esconde un concepto que debe remarcarse: el conocimiento.

En numerosas ocasiones los conceptos dato, información y conocimiento se utilizan de forma distinta pero no son lo mismo.

Dato: un dato es un registro. No nos dice nada sobre el porqué de las cosas. Los conjuntos de datos son la base para la creación de la información. En el ámbito del riesgo operacional se trabaja con diversas bases de datos: base de pérdidas, evaluaciones cualitativas y, en los modelos AMA, bases de pérdidas externas.

Información: informar es "dar forma a". La información tiene significado en sí misma. Se transforma los datos en información de muy diversas maneras: contextualizando, categorizando, calculando, corrigiendo, condensando. Así, por ejemplo, se utiliza unas categorías comunes dadas por el propio Acuerdo de Basilea: esa categorización nos permite obtener información (qué tipo de evento se materializa de forma más frecuente, qué línea de negocio ha generado más quebrantos, etc.).

Conocimiento: es una mezcla de experiencia, valores, información y "saber hacer". El conocimiento en una organización, se produce cada vez que un individuo de la misma hace uso de sus habilidades (formación previa, experiencia profesional, etc.) y de la información que tiene a su alcance para la resolución de un problema o el desarrollo de un proyecto. El conocimiento se deriva de la información mediante: comparación, consecuencias, conexiones. Así pues, para conocer el verdadero perfil de riesgo de la entidad se debe gestionar, a parte de la

infinidad de datos e información, las comparaciones, consecuencias y conexiones que se puedan dar entre ellos.

DOS VISIONES DE UNA MISMA REALIDAD

Tanto los métodos cuantitativos como los cualitativos son instrumentos para analizar una misma realidad: el riesgo operacional. Como sabemos, éste se halla latente en todas las áreas de actividad y potencialmente se puede materializar con muchas caras diferentes. A cada una de estas caras la llamaremos RO_1, RO_2,….,RO_n.

Los riesgos que más nos ocupan el día a día son aquellos que se materializan (algunos de forma reiterativa). A cada una de estas materializaciones las llamaremos sucesos y usaremos la siguiente nomenclatura para hacer referencia a ellos: S_{RO1}, S_{RO2},….,S_{ROn}.

Podemos representar estos conceptos, y sus relaciones, mediante el diagrama de Venn

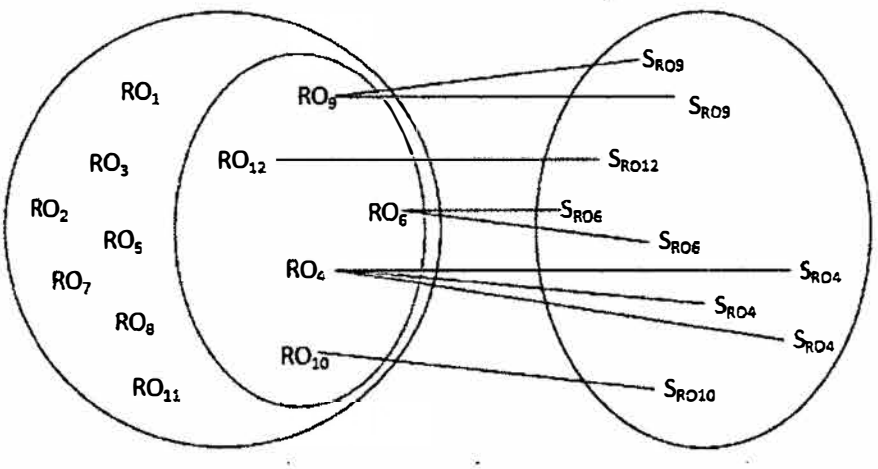


Figura 1.1: Diagrama de Venn

Fuente: La gestión del riesgo operacional: de la teoría a su aplicación. Fernández Laviada, Ana. Edit. LIMUSA Noriega Editores. Cantabria – España. Pág. 288

Así, el conjunto de los riesgos conforma el mapa de riesgos operacionales de la entidad y el conjunto de los sucesos se corresponde con nuestra base de datos de pérdidas.

Éstas son, cada una de ellas por separado, dos potentes herramientas de análisis del riesgo operacional de nuestra entidad.

Más allá de lo que pueda requerir el supervisor nacional en el proceso de validación de los diferentes modelos, la integración de los métodos cualitativo y cuantitativo nos debe permitir tener una visión única y completa de lo que el riesgo operacional supone. Una adecuada gestión de lo que puede llegar a suponer podría ser la diferencia entre subsistir o desaparecer.

1.2.3.5.4. VISIÓN CUALITATIVA

Los objetivos que debemos cumplir mediante el análisis cualitativo, lógicamente, están directamente vinculados al ciclo de gestión del riesgo operacional:

a) **Identificación:** debemos identificar de forma exhaustiva los diferentes riesgos operacionales (RO_1, RO_2,….,RO_n) que podrían llegar a materializarse y por tanto producirnos algún tipo de quebranto. Asimismo también debemos identificar los controles que se tiene establecidos para la mitigación de esos riesgos (ya sea para reducir la probabilidad de ocurrencia o para mitigar su impacto). Con toda esa información se estará en disposición de obtener el mapa de riesgos y controles de nuestra entidad. Para que este mapa de riesgos y controles pueda ser gestionado debe centrarse en los riesgos operacionales "que importan", es decir, aquellos cuya probabilidad de ocurrencia sea elevada

así como aquellos cuya materialización, aunque improbable, pudiese llegar a suponer un quebranto de elevado impacto. Se trata, pues, de identificar los riesgos potenciales.

b) **Evaluación y cuantificación:** los diferentes coordinadores de riesgo operacional deberán valorar cuál es nuestra exposición a cada uno de estos riesgos así como evaluar la fortaleza de los sistemas de control de la entidad. Estas evaluaciones permitirán efectuar pruebas de estrés y de evaluación de resultados sobre nuestro modelo.

c) **Mitigación y seguimiento:** en función de la valoración anteriormente mencionada, la entidad deberá instrumentar los planes de acción necesarios para la mitigación preventiva de las posibles materializaciones de riesgos. Deben tener un tratamiento especial, mediante la confección de planes de contingencia y de continuidad de negocio, aquellos riesgos cuya materialización pudiese suponer la desaparición de la entidad. Estos riesgos difícilmente podrán analizarse a partir de metodologías cuantitativas salvo que nos lleguen por la vía de las bases de datos externos. Dada la cantidad de datos que se gestiona, este trabajo puede resultar muy tedioso y, por lo tanto, es recomendable la implantación de herramientas informáticas especializadas. De la misma manera es recomendable la creación de una adecuada red de coordinadores que ayudarán a analizar la amplia amalgama de procesos que discurren por la entidad.

1.2.3.5.5. VISIÓN CUANTITATIVA

El análisis cuantitativo también está vinculado al ciclo de gestión del riesgo operacional.

a) **Identificación:** se deben identificar todos los sucesos operacionales que estén generando quebrantos a nuestra entidad. con ellos, una vez clasificados y estructurados, obtendremos la base de datos de pérdidas. Se trata de riesgos materializados que se han convertido en hechos contables; así la contabilidad será la principal fuente de datos.

   Un aspecto a considerar es el hecho de que cuando un riesgo se materializa no siempre lo hace con un solo efecto. En estos casos se encontrará diversos apuntes contables relacionados entre sí y que conforman un único suceso. Para ello se debe establecer una codificación (por ejemplo: centro de ocurrencia + fecha de ocurrencia + identificador de riesgo) que permita vincular todos los efectos relacionados de la forma más automatizada posible. Para asegurar que se está capturando todos los datos que se necesita, se debe hacer un análisis sistemático de las cuentas contables de los balances de todos los centros de la entidad.

b) **Evaluación y cuantificación:** los propios apuntes contables nos dan de forma directa la cuantificación de las pérdidas operacionales que sufrimos. En este caso el papel de los coordinadores será el de analizar los motivos que han hecho que se materialicen los riesgos.

c) **Mitigación y seguimiento:** en el caso de que se detectasen fallos de control significativos deberían proponerse planes de acción para evitar futuras materializaciones siempre con un previo análisis coste/beneficio. Hay que tener en cuenta que una de las opciones para la gestión de los riesgos es la contratación de pólizas de seguros. En este caso, la función de los

coordinadores de riesgo operacional será la de analizar los posibles cambios en los procesos de registro de pérdidas.

1.2.3.5.6. EL CICLO DE GESTIÓN DEL RO: LA INTEGRACIÓN

Una vez efectuados los análisis cualitativo y cuantitativo se tiene mucha información y se debe establecer la relación que existe entre los riesgos y sucesos.

Para obtener una visión integrada y completa del riesgo operacional todavía falta conocer cuáles son los riesgos operacionales que se materializan y además con qué frecuencia e impacto (relaciones entre riesgos operacionales y sucesos).

VENTAJAS

a) **Permite analizar la coherencia de las evaluaciones de los coordinadores**

La integración del mapa de riesgos y de la base de datos, nos permitirá analizar la coherencia de las evaluaciones cualitativas realizadas por los coordinadores ya que se podrán comparar con los resultados obtenidos en el análisis cuantitativo (al menos de los riesgos que se hayan materializados). Con esta comparación se obtendrá una retroalimentación entre ambos métodos.

b) **Potencia la retroalimentación del mapa de riesgos**

Si en el momento de registrar una pérdida operacional en la base de datos no se es capaz de vincular ese suceso a un riesgo de los del mapa puede ser debido a que no fuese contemplado en el análisis cualitativo. En ese caso se deberá incorporar el riesgo con su correspondiente valoración.

c) **Mejora la integridad de la base de datos de pérdidas**

Tomando en cuenta el supuesto anterior, la otra opción sería que se estuviese intentando registrar como riesgo operacional un suceso que no es de ese ámbito. Ante esa duda han de contactar con el coordinador de riesgo operacional quien clarificará el criterio a seguir.

d) Facilita y da calidad a la automatización de la captura de sucesos

El hecho de tener un inventario de riesgos nos permite tenerlos clasificados según las categorías de riesgos establecidas por BIS II y, en algunos casos, incluso por líneas de negocio. Esta clasificación previa de los riesgos hace que los sucesos, en su mayoría, queden automáticamente clasificados en el momento de su captura.

Esta clasificación, al ser centralizada, evita la dispersión de criterios de clasificación que podría darse si se realizase por parte de los contables de la entidad.

e) Permite la realización de análisis coste/beneficio más depurados

En la gestión práctica del riesgo operacional facilitará la realización del análisis coste/beneficio para evaluar la conveniencia de instaurar los planes de acción ya que tendremos vinculada, riesgo a riesgo, la valoración cualitativa a la base de datos de pérdidas.

Evidentemente, llegar a esta integración entre la visión cualitativa (mapa de riesgos) y la cuantitativa (base de datos de pérdida) puede no ser trivial. La tarea será más o menos compleja (y costosa) en función de numerosos factores propios de cada entidad: versatilidad de los sistemas transaccionales, adaptabilidad al cambio, volumen de datos a tratar, recursos disponibles, etc.

1.2.3.5.7. SISTEMA DE INDICADORES: CUADRO DE MANDO DE RIESGO OPERACIONAL

Un sistema de información es un conjunto de elementos vinculados con la finalidad de servir de soporte de ayuda a la toma de decisiones. Cuadro de mando es un concepto derivado del término francés *"tableau de bord"* que viene a significar cuadro de instrumentos o tablero de mando, con el propósito de configurar un marco de información cuya utilidad básica es el diagnóstico. Una definición más formal de Cuadro de Mando es la que realiza Ballvé (2001) que lo define como *"el conjunto de indicadores cuyo seguimiento periódico permitirá contar con un mayor conocimiento de la situación de la empresa"*. Para el caso específico del RO, la finalidad del cuadro de mando será proporcionar información sobre la posición y previsible evolución del riesgo de una entidad y servir de apoyo para la toma de decisiones del responsable de RO o de los diferentes directivos de cada área organizativa.

Su implantación en una entidad como herramienta de gestión proporciona las siguientes ventajas:

- Permite un seguimiento periódico del perfil de riesgo de la entidad.
- Contribuye a mantener un estado de alerta permanente sobre los factores de riesgo identificados como clave y reflejar sus desviaciones.
- Ayuda a implantar planes de acción para la mejora y perfeccionamiento de los procesos.
- Permite identificar las causas de las desviaciones y su incidencia en la posición de riesgo de la entidad.
- Actúa como predictor de eventos de pérdida operacional.

El objetivo del cuadro de mando basado en indicadores es poder contrastar periódicamente el perfil de riesgo, obtenido previamente con los enfoques o herramientas de tipo cualitativo de gestión de riesgo: autoevaluaciones y mapas de riesgo, básicamente, con mediciones objetivas preferentemente de carácter cuantitativo, que se obtienen directamente de los procesos. Este objetivo se concentra en el diseño y la implantación de un cuadro de mando que reúna las siguientes características:

- Tiene que estar integrado en la plataforma de herramientas que configuran la gestión de RO.
- Debe estar implantado en toda la organización y con asignación de responsabilidades en cada área.
- La definición de niveles de tolerancia debe permitir evaluar el perfil de riesgo y reducir la aparición de eventos de pérdida.
- Debe estar relacionado con las pérdidas reales acaecidas para que tenga capacidad predictiva.
- Contribuirá a la metodología de cálculo de los requerimientos de capital.

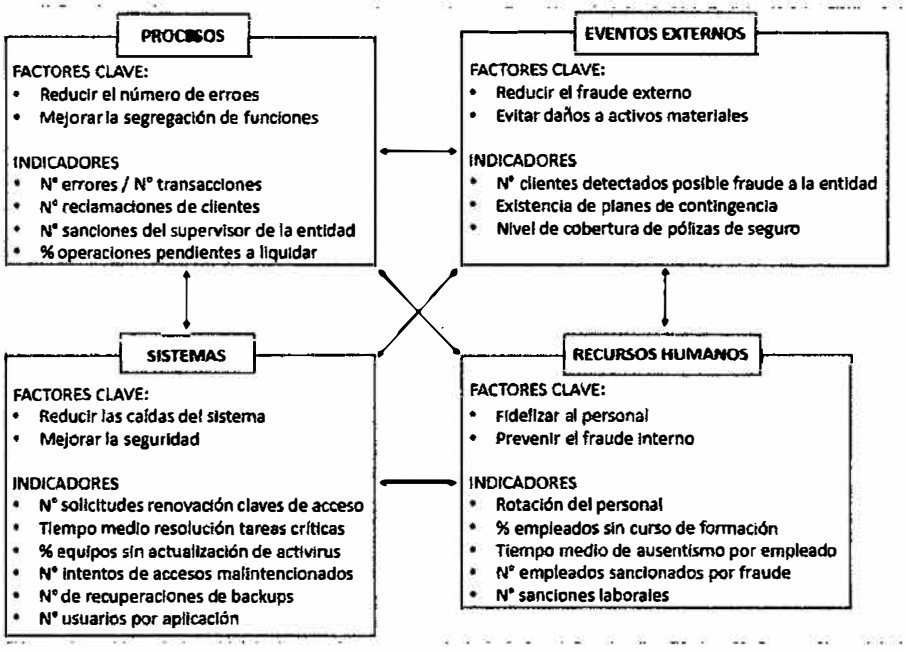


Figura 1.2: Cuadro de mando de riesgo operacional

Fuente: La gestión del riesgo operacional: de la teoría a su aplicación. Fernández Laviada, Ana. Edit. LIMUSA Noriega Editores. Cantabria – España. Pág. 348

1.2.3.6.CUESTIONARIOS DE EVALUACIÓN

Para una correcta identificación de los riesgos es necesario un sólido conocimiento de las actividades y procedimientos que se desarrollan en cada una de las áreas que se analicen. Siendo:

- *Factor de riesgo:* es cualquier circunstancia, situación, elemento, proceso, etc. al que se encuentra expuesta la entidad y que de producirse se materializa en un quebranto.
- *Controles:* son cualquier acción o política que lleva a cabo la entidad, con el fin de anular o reducir un factor de riesgo.

Las fuentes de información que se pueden utilizar en el desarrollo de los cuestionarios iniciales son:

- Documentos internos, como procedimientos escritos, presupuestos, planes de actividad, etc.
- Informes de auditores internos y/o externos.
- Procedimientos de control interno.
- Revisiones de políticas y procedimientos.
- Análisis de nuevos productos.
- Sistemas de información.

Estos cuestionarios iniciales se presentarán y completarán con entrevistas en detalle que se realizarán con cada uno de los responsables de las áreas con el objetivo de:

- Obtener información de los procesos o actividades que realizan y otra información relevante que permita adaptar los cuestionarios.
- Identificar los factores y tipos de riesgos a los que está expuesta el área.
- Identificar los mecanismos de control interno existentes para mitigar los riesgos.
- Identificar oportunidades de mejora del control interno.

En el transcurso de las entrevistas, se deberá recabar la mayor información posible y apoyarla con la documentación existente:

- Identificación y descripción de las principales tareas (procesos) realizadas.
- Existencia de manuales, normativa, procedimientos escritos, así como tratar de identificar sus carencias.
- Información manejada (datos, cifras, ratios, interna o externa).
- Errores y fallos más frecuentes.
- Motivos de pérdidas.

- Posibles indicadores de riesgo.
- Oportunidades de mejora.
- Estadísticas utilizadas, tanto de trabajos efectuados como de problemas (transacciones, errores, reclamaciones, pérdidas, cobertura objetivos, tiempo por expediente, etc.)
- Coberturas de seguro.

1.2.3.7. VALORACIÓN DEL RIESGO OPERACIONAL

Una vez identificados los riesgos asociados a los distintos procesos, es necesario establecer una metodología para medirlos, valorarlos y priorizarlos.

Existen diferentes técnicas basadas en modelos cuantitativos como el VaR, pero estos modelos cuantitativos tropiezan con un problema significativo que es la falta de disponibilidad de una profundidad de datos suficiente para que el modelo estadístico sea realmente predictivo.

Modelo cualitativo, para establecerlo a cada factor de riesgo se le asigna un valor por su importancia en el área de negocio y otro por su probabilidad de ocurrencia.

Con este esquema de valoración se clasifican los riesgos en dos vertientes:

- *Riesgo inherente*: es el riesgo intrínseco de la actividad que se analiza sin considerar la existencia de los controles existentes o que se puedan implantar para mitigarlo.
- *Riesgo residual*: es el riesgo en el que realmente está incurriendo la entidad en una actividad y momento concreto teniendo en cuenta el efecto de los controles establecidos para la reducción del riesgo identificado. El efecto de los controles puede suponer la reducción de la frecuencia de un riesgo, de su impacto o de ambos a la vez.

La calificación inicial realizada para el riesgo inherente se relativiza en función de la efectividad y grado de cobertura que ofrecen los mecanismos de control establecidos, que se califican también en una escala cualitativa:

- Total: los controles establecidos eliminan prácticamente la probabilidad de ocurrencia y/o impacto del riesgo inherente reduciéndose a Muy Bajo.
- Alta: los controles establecidos limitan significativamente la probabilidad de ocurrencia y/o impacto del riesgo inherente reduciéndose a Bajo.
- Media: los controles establecidos limitan, pero no drásticamente, la probabilidad de ocurrencia y/o impacto del riesgo inherente reduciéndose a Bajo.
- Baja: los controles establecidos muestran debilidades significativas que impiden que sean efectivos en un elevado número de ocasiones, por lo que se mantiene la calificación inicial de riesgo inherente.
- Muy baja: prácticamente se produce una inexistencia de controles o bien los existentes no son en absoluto efectivos, por lo que se mantiene la calificación inicial del riesgo inherente.

1.2.3.8. MÉTODOS DE MITIGACIÓN

LA GESTIÓN DE RECURSOS HUMANOS

Los recursos humanos constituyen la parte más importante en la gestión del riesgo operacional. Las empresas que disponen de personal cualificado, motivado y experimentado, son las que tienen las mejores bases para controlar el riesgo operacional.

Los aspectos más relevantes para minimizar el riesgo que hay que tener en cuenta en la gestión de recursos son los siguientes:

- **Formación:** es fundamental que el personal tenga el nivel de formación adecuada para la función que desempeña.
- **Dotación de plantilla:** la capacidad de los procesos depende del número de personas, su distribución a lo largo del mismo y de la capacidad de las aplicaciones informáticas que se usan. La gestión debe encaminarse a adecuar estos recursos a los volúmenes que deben ser tratados, sin sobrecargar a la unidad.
- **Gestión del conocimiento:** cada empresa tiene su propia cultura y esto es algo que solo se puede transmitir entre los propios empleados. Por consiguiente, es fundamental que el conocimiento se transmita de forma adecuada (mediante planes de entrenamiento, manuales, etc.).
- **Política retributiva:** una de las formas más habituales de pérdida de talento la constituyen las bajas voluntarias, en especial de aquellas personas que se van a la competencia. La razón principal suele ser la económica. Por tanto, es necesario que se identifique a las personas clave de la organización y se aseguren que su retribución está en consonancia con el mercado laboral, o incluso ligeramente por encima, para no propiciar estos movimientos.
- **Planes de sustitución:** consiste en prever de antemano cómo reemplazar a determinadas personas clave en caso de que causen baja.

SEGREGACIÓN FUNCIONAL

Si analizamos ciertos eventos de riesgo operacional ocurridos en los últimos años y nos fijamos especialmente en determinados fraudes y actividades no autorizadas veremos que, casi siempre, lo que ha pasado es que el defraudador tenía diversas funciones, entre las cuales se encontraban algunas que son incompatibles entre sí. Dicho en otras palabras: el empleado, a veces, es juez y parte.

Estos posibles conflictos entre funciones se solucionan con una adecuada segregación funcional que consiste en impedir que recaigan sobre la misma persona atribuciones que, de estar juntas, posibilitan la comisión del delito o de la actividad no autorizada.

EL CONTROL DUAL

El control dual es una forma de prevenir errores de alto impacto. Consiste en duplicar los controles, realizándolos dos veces, sobre determinadas transacciones que, de resultar fallidas, tendrían un coste muy alto para la organización.

PLANES DE CONTINGENCIA

Es el método más eficaz para mitigar el impacto de las pérdidas, en caso de interrupción prolongada, de los servicios prestados por cualquier empresa a causa de acontecimientos catastróficos.

Consiste en el desarrollo y mantenimiento de programas de acción para garantizar el funcionamiento de sistemas y procesos alternativos a los medios habitualmente usados para dar el soporte básico a la entidad.

PLANES DE CONTINUIDAD DE SERVICIO

El método idóneo para reducir cualquier pérdida que pueda originarse en caso de interrupción puntual de los servicios básicos de una empresa, consiste en el establecimiento de un plan de acción que contemple las medidas que deben adoptarse

en el supuesto de que se registren las circunstancias críticas contempladas en el mismo.

El plan de continuidad garantizará la calidad y correcto funcionamiento de los sistemas de soporte y los servicios básicos ofertados por la entidad en situaciones de normalidad y tendrá por objeto la utilización de los medios necesarios para alcanzar esos fines.

LA SEGURIDAD FÍSICA

La exposición a riesgos físicos y ambientales puede producir pérdidas económicas, tener repercusiones de carácter legal y ocasionar quebrantos en la imagen de la entidad.

Esta consiste en levantar barreras físicas y procedimientos de control como medidas de protección y contramedidas ante amenazas contra los activos, recursos e información confidencial provocadas por la acción humana o accidentes de la naturaleza. El sistema de seguridad física debe responder a las características del ámbito a cubrir y, por lo tanto, existirán tantos sistemas de seguridad diferentes como zonas a proteger.

LA SEGURIDAD LÓGICA

El objetivo de la seguridad lógica informática es el de mantener la integridad, disponibilidad, confidencialidad, control y autenticidad de la información procesada por los sistemas informáticos, así como la protección a la réplica, consistencia y aislamiento de la información procesada mediante la aplicación de barreras y procedimientos que impidan el acceso a los datos por parte de personas no autorizadas.

Los riesgos ocasionados por la vulneración de los sistemas de seguridad lógica pueden tener su origen en actuaciones de personas vinculadas o no con la empresa, actos realizados de forma accidental o con intención de causar daño.

1.2.3.9. MARCO DE CONTROL DEL RIESGO OPERACIONAL

Según (Fernández Madrazo, Rodríguez Navamuel, & Rosich Parte, 2010), el marco de control para la gestión del RO se compone de aquellos elementos esenciales y necesarios para crear un ambiente de gestión de los riesgos operacionales; entre ellos, los más importantes son los siguientes:

a) ***Consejo de administración y alta dirección:*** uno de los factores más importantes para alcanzar el éxito en la eficiente implantación de un sistema de gestión del RO es que tanto el consejo de administración como la alta dirección se encuentren implicados en el proceso. Los auditores internos deberán verificar si el consejo de administración aprueba una estrategia a seguir en el marco de la gestión del RO en la cual se especifique la definición tomada por la entidad para el RO, el nivel de tolerancia y las políticas específicas para gestionarlo.

   Desde el punto de vista de auditoría interna, también será importante revisar aspectos tales como los siguientes:

   - Existencia de estudios de necesidades de recursos para afrontar la gestión del RO.

- Existencia de planes de contingencia ante situaciones críticas originadas por riesgos operacionales.
- Previsión de procesos de revisión de la estrategia tomada para asegurar la inclusión en el proceso de gestión de nuevos riesgos operacionales.
- Establecimiento de circuitos de reporting tanto al consejo de administración como a la alta dirección.

b) ***Estructura organizativa:*** la eficacia en el funcionamiento de todo el sistema de gestión del RO pasa por el diseño de una estructura organizativa adecuada. Así, el auditor interno deberá hacer comprobaciones sobre aspectos como:

- Creación de un comité de RO por el que se implique la alta dirección y definición de su composición, funciones, etc.
- Existencia de una entidad operativa específica para la gestión del RO con los medios humanos y técnicos necesarios.
- Asignación de responsables de RO en cada área organizativa de la entidad y en las sociedades del grupo.
- Adecuada segregación de funciones entre las funciones de gestión y control del RO.

c) ***Manuales de políticas y procedimientos:*** el auditor interno deberá comprobar la existencia y revisar el contenido de estos manuales y su aprobación por la alta dirección, que se encuentren actualizados y que estén puestos a disposición de la plantilla. Además, habrá de verificar si la definición de los riesgos y de las diversas líneas de negocio es acorde con el NACB.

d) ***Manuales de funciones:*** en este caso es preciso realizar comprobaciones similares a las realizadas sobre los manuales de políticas y procedimientos. Además, tiene especial importancia verificar la inclusión de las funciones relacionadas con la gestión del RO a los diferentes responsables o áreas implicadas como puede ser:

- Gestor de RO.
- Comité de RO u órgano similar.
- Responsables de la gestión del RO en las diferentes áreas.
- Auditoría interna.

e) ***Factores internos de riesgo:*** los auditores internos deberán analizar los factores internos de la organización que tienen o han tenido incidencias significativas en la gestión del RO. En este sentido, deberán verificar que el gestor del RO informe periódicamente al Comité de RO de la situación de estos factores, de su evolución y de las medidas tomadas para mitigar sus efectos. Entre estos factores de riesgos se encuentran los siguientes:

- Estructuras organizativas inadecuadas que no faciliten la segregación de funciones o el seguimiento y análisis de las actividades desarrolladas en la entidad.
- Inexistencia de manuales operativos o de procedimientos de las actividades desarrolladas en la entidad.
- Inexistencia de manuales de funciones, que definan el ámbito de actuación de las diferentes áreas de la entidad.
- Carencia de un código de gobierno corporativo que influya en la toma de decisiones.

- Carencia de códigos éticos que regulen las actuaciones de la plantilla de la entidad.
- Deficiencias en la automatización de los procesos básicos de la entidad.
- Deficiencias en los procesos formativos o de selección de personal.
- Inexistencias de mecanismos efectivos de supervisión de las operaciones y de los procesos.

f) ***Factores externos de riesgo:*** existen factores externos o exógenos que influyen en la forma de afrontar la gestión del RO y a los que los auditores internos han de prestar atención, especialmente a aquellos que pueden tener una incidencia significativa en dicha gestión. Entre estos factores externos de riesgo se encuentran los siguientes:

- Obsolencia tecnológica.
- Falta de adaptación de los procedimientos de la entidad a las nuevas normas legales o inexistencia de supervisión sobre la implantación de las mismas.
- Falta de adaptación ante la aparición de nuevos mercados, productos o actividades.
- Aparición de nuevas formas de fraude que tienen o pueden tener efectos negativos sobre la entidad.
- Realización de actividades en zonas de alta peligrosidad, bien por los efectos naturales (atmosféricos o de cualquier otra naturaleza) o por actos delictivos (vandalismo u otras formas de actos antisociales).

g) ***Infraestructura tecnológica***: se trata de un aspecto fundamental en cualquier enfoque utilizado para la gestión de los riesgos, dada la complejidad de la

metodología utilizada (si bien la misma aumentará desde los modelos básicos a los avanzados). En este sentido, los auditores internos han de analizar las herramientas informáticas puestas a disposición del departamento encargado de la gestión del RO, verificando la efectividad de las mismas en su cometido y que contemplan aquellos elementos necesarios para proporcionar información relevante para incorporar en los procesos de toma de decisiones de la entidad, tales como pueden ser indicadores de riesgos, gestión de planes de acción, etc. asimismo, deberán asegurarse de la existencia de manuales operativos actualizados así como que existe un grado de seguridad informático adecuado en función de los diferentes perfiles de usuario.

h) Circuito de información: tal y como se ha señalado anteriormente, todo este esfuerzo de sistematizar la gestión del RO no tendría sentido si no se proporcionara información útil y relevante para la toma de decisiones en la entidad, pero es igual de importante que en el caso de que se genere este tipo de información ésta llegue a su destino y sea considerada adecuadamente por los órganos de decisión. Los auditores internos deberían analizar los distintos informes emitidos y las principales características de los mismos, como pueden ser:

- *Finalidad,* verificando que la información generada permite la identificación de las áreas problemáticas así como las acciones correctivas pertinentes.
- *Distribución,* comprobante si la información se dirige tanto a la alta dirección como a los responsables de las áreas organizativas de la entidad y que la misma es recibida por sus destinatarios.

- *Periodicidad.*
- *Fuente de datos.*
- *Responsable de su actualización o control.*

Asimismo, habrán de comprobar el uso que se hace de los mismos y su efectividad para la realización del seguimiento de la gestión.

i) ***Responsables para la gestión del RO en los diferentes departamentos:*** en los procedimientos diseñados por los auditores internos deberá considerarse la existencia de responsables de la gestión del RO en los propios departamentos de la organización, ya que ellos han de ser el puente entre los mismos y el departamento de RO. Se deberá comprobar que éstos hacen un seguimiento activo del RO y que reciben la formación adecuada.

j) ***Formación en RO:*** otro de los hitos fundamentales a la hora de diseñar un buen marco de control del RO es la existencia de planes de formación en esta materia. Auditoría interna deberá realizar revisiones de los mismos, verificando su impartición efectiva tanto a los directamente implicados en la gestión del RO como al resto de la plantilla.

1.2.4. EL CAMBIO CULTURAL

(García Ribas, 2010) Afirma que la gestión del riesgo operacional involucra a toda una organización, empezando por la alta dirección y terminando por los empleados de menor rango.

Y, para que esto sea posible es necesario que se produzca un cambio cultural en la organización promovido desde las altas esferas. Esta es la tarea más ardua a la que se

enfrentan las organizaciones si desean tener éxito en la implantación de los mecanismos de gestión del riesgo operacional.

En las grandes empresas multinacionales este tipo de cambios necesitan entre cinco y diez años para producirse en su totalidad. No basta con pasar un mensaje o un lema desde la alta dirección. Para que la nueva cultura cale en la organización, es necesario que esté presente en el día a día de todas y cada una de las personas que la componen. Será, por tanto, necesario realizar un gran esfuerzo en materia de comunicación interna, formación y compensación.

COMUNICACIÓN INTERNA

A través de los mecanismos clásicos de comunicación interna que la empresa utilice (memorandos, revistas, e-mail, etc.) debe notificarse a toda la plantilla que el riesgo operacional es un riesgo que se desea controlar por el bien de la entidad.

FORMACIÓN

Una vez que la entidad ha comunicado a todos sus integrantes su intención de gestionar el riesgo operacional, es necesario llevar a cabo cursos de formación en los cuales se transmita a todas las personas que gestionan procesos, los conocimientos necesarios para afrontar los ejercicios de identificación y cuantificación de los factores de riesgo operacional en sus respectivas unidades.

Normalmente, es la unidad central de riesgo operacional la que se encarga de realizar esta labor, explicando detalladamente las causas y consecuencias de eventos, las distintas clases de riesgo operacional, los mecanismos de mitigación, etc.

COMPENSACIÓN

Para garantizar que la implantación de una cultura orientada a la gestión del riesgo operacional se efectúe satisfactoriamente, es recomendable introducir recompensas económicas por ello.

Dentro del esquema de compensación se puede tener en cuenta muchos factores, por ejemplo, la calidad y cantidad de factores de riesgo encontrados, las medidas de mitigación implantadas, etc.

1.2.5. DESCRIPCIÓN GENERAL DE LA CAJA DE PENSIONES MILITAR POLICIAL

La Caja de Pensiones Militar Policial (CPMP), creada mediante el Decreto Ley N° 21021, es una persona jurídica de Derecho público interno con autonomía administrativa, económica y financiera. Sus principales funciones son:

- Administrar el régimen de pago de las pensiones y compensaciones de sus miembros, de conformidad con lo establecido en el Decreto Ley N° 19846 "Ley de Pensiones Militar - Policial" y en el Decreto Legislativo N° 1133 "Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial".
- Administrar los recursos de la CPMP con la finalidad de incrementarlos.
- Administrar otros fondos y prestar otros servicios que sean aprobados por decreto supremo, refrendado conjuntamente por los ministros de Defensa y del Interior.

Son afiliados de la CPMP, el personal militar y policial egresado de las escuelas de formación de oficiales y de personal subalterno, y aquellos que se hayan incorporado a las Fuerzas Armadas (FF AA) y Policía Nacional del Perú (PNP) a partir del 1 de enero de 1974, que perciban remuneraciones sujetas al descuento para el Fondo de Pensiones

del Decreto Ley N° 19846. También, los deudos del personal mencionado son acreedores a los beneficios que otorga la Ley de Pensiones Militar - Policial.

Además, se incluye al personal de las FF AA y la PNP que se encuentra bajo el Régimen de Pensiones del Decreto Legislativo N° 1133, por haber iniciado la carrera de oficiales o suboficiales a partir del 10 de diciembre de 2012.

El Consejo de Supervisión es el órgano superior de la CPMP, que formula y dirige la política institucional, y está constituido por el Ministro de Defensa y el Ministro del Interior.

La dirección de la CPMP se encuentra a cargo del Consejo Directivo, que está conformado de la siguiente manera:

- Un (1) director designado por los ministros de Defensa, del Interior y de Economía y Finanzas, quien lo preside.
- Dos (2) directores designados por el Ministro de Defensa.
- Dos (2) directores designados por el Ministro del Interior.
- Dos (2) directores designados por el Ministro de Economía y Finanzas.
- Dos (2) representantes de los pensionistas de la CPMP, uno (1) proveniente de la PNP y uno (1) de las FF AA.

La entidad se encuentra bajo la supervisión de la Superintendencia de Banca, Seguros y AFP (SBS) **(Anexo N° 1 y N° 2)**, y está sujeta a la acción de control de la Contraloría General de la República (CGR). Asimismo, se encuentra inscrita en el Registro de Personas Jurídicas de Lima, en la Partida N° 11013023.

Por otro lado, bajo el marco de la mejora de la calidad del servicio al pensionista, la CPMP brinda información previsional de manera ágil por los canales de atención establecidos. Estos son:

- Plataforma de atención: canal presencial ubicado en el local institucional de la CPMP, a través del que se reciben solicitudes, consultas y reclamos.
- Call center: canal telefónico que permite recibir solicitudes, consultas y reclamos.
- Buzón del afiliado: dirección de correo electrónico mediante la que se reciben consultas y reclamos.
- Portal previsional: página web de la entidad en donde se muestra información sobre los trámites y procesos previsionales.

El mantenimiento y optimización de dichos canales se realiza con la finalidad de ofrecer el mejor servicio posible, y brindar calidad, seguridad y confianza a los afiliados.

1.2.5.1.ORGANIZACIÓN

El Consejo de Supervisión es el órgano superior de la CPMP, que formula y dirige la política institucional, y está constituido por el Ministro de Defensa y el Ministro del Interior.

La dirección de la CPMP se encuentra a cargo del Consejo Directivo, que está conformado de la siguiente manera:

- Un (1) director designado por los ministros de Defensa, del Interior y de Economía y Finanzas, quien lo preside.
- Dos (2) directores designados por el Ministro de Defensa.
- Dos (2) directores designados por el Ministro del Interior.

- Dos (2) directores designados por el Ministro de Economía y Finanzas.
- Dos (2) representantes de los pensionistas de la CPMP, uno (1) proveniente de la PNP y uno (1) de las FF AA.

El organigrama de la Caja de Pensiones Militar se encuentra en el **anexo N°3.**

ÓRGANO DE SUPERVISIÓN: CONSEJO DE SUPERVISIÓN

MINISTRO DE DEFENSA: Pedro Álvaro Cateriano Bellido

MINISTRO DEL INTERIOR: Daniel Belizario Urresti Elera (periodo: desde el 24 de junio de 2014) y Walter Jorge Albán Peralta (periodo: hasta el 24 de junio de 2014).

ÓRGANO DE DIRECCIÓN: CONSEJO DIRECTIVO

PRESIDENTE: Lorena Masías Quiroga

VICEPRESIDENTE: Luis Fernando Ruiz Lecaros (representante del Ministerio de Defensa - periodo: desde el 23 de octubre de 2014).

REPRESENTANTE DEL MINISTERIO DE ECONOMÍA Y FINANZAS: Alfonso Jesús Garcés Manyari (periodo: hasta el 4 de octubre de 2014).

REPRESENTANTES DEL MINISTERIO DE DEFENSA: Roberto Luis Urrunaga Pascó-Font

REPRESENTANTES DEL MINISTERIO DEL INTERIOR: Adriana Milagros Mindreau Zelasco y Jorge Pablo Nicolás Noziglia Chávarri.

REPRESENTANTES DEL MINISTERIO DE ECONOMÍA Y FINANZAS: Edgard Eduardo Ortiz Gálvez (periodo: desde el 5 de octubre de 2014), Alfonso Jesús Garcés Manyari (periodo: hasta el 4 de octubre de 2014) y José Giancarlo Gasha Tamashiro.

REPRESENTANTES DE LOS PENSIONISTAS DE LAS FUERZAS ARMADAS: Técnico de Primera EP (R) Alejandro Córdova Depaz (periodo: desde el 21 de julio de 2014).

SECRETARIO: Roxana Olinda Argote Lozano.

ÓRGANO DE CONTROL

ÓRGANO DE CONTROL INSTITUCIONAL: NIMIA CHIN ARCE

ÓRGANO EJECUTIVO

GERENCIA GENERAL: FERNANDO KIHARA TOMITA (e)

ÓRGANO DE ASESORÍA

GERENCIA LEGAL: Clara María Zavala Mora (periodo: desde el 1 de febrero de 2014) y Claudia Livia Bayro Valenza (e) (periodo: hasta el 31 de enero de 2014).

ÓRGANO DE APOYO

GERENCIA DE INFORMÁTICA: JORGE ALEXANDER KANEKO LA ROSA

ÓRGANOS DE LÍNEA

GERENCIA DE PENSIONES: Virgilio Paz Enciso (e)

GERENCIA DE ADMINISTRACIÓN Y FINANZAS: Felipe Rigoberto Fonseca Taboada

GERENCIA DE RIESGOS Y DESARROLLO: Nicolás Zegarra Martínez

COMITÉS DE LA CPMP

A. COMITÉ DE RIESGOS E INVERSIONES

Fecha de creación: 4 de noviembre de 2004

Tiene por finalidad proponer y evaluar, tanto las políticas y procedimientos para la identificación y administración de los riesgos de operación y financieros que afronta la CPMP en el desarrollo de sus actividades y operaciones.

A fin de adecuar los procesos a las disposiciones de la SBS, este comité fue reemplazado por el Comité de Riesgos y el Comité de Inversiones; ambos creados en mayo de 2014.

B. COMITÉ DE RIESGOS

Fecha de creación: 28 de mayo de 2014

Tiene por finalidad proponer y evaluar las políticas, normas y procedimientos para la identificación y administración de los riesgos de operación y financieros que afronta la entidad en el desarrollo de sus actividades y operaciones.

Principales funciones:

a. Elaborar y/o revisar y someter a aprobación del Consejo Directivo las propuestas referidas a:
   - Los objetivos, estrategias, políticas, procedimientos y acciones de la gestión integral de riesgos y opinar sobre las modificaciones que se realicen, así como supervisar su implementación (Anexo N° 3);
   - El nivel de tolerancia y el grado de exposición al riesgo que la entidad está dispuesta a asumir en el desarrollo del negocio;

- Los procedimientos y/o normas de control interno que aseguren un adecuado manejo y solución de los conflictos de interés en las actividades relacionadas a la gestión de riesgos; y,
- Las propuestas de mejoras en la Gestión Integral de Riesgos.

b. Decidir las acciones necesarias para la implementación de las medidas correctivas requeridas, en caso existan desviaciones con respecto a los niveles de tolerancia al riesgo y a los grados de exposición asumidos.

c. Aprobar la toma de exposiciones que involucran variaciones significativas en el perfil de riesgo de la entidad o de los patrimonios administrados bajo responsabilidad de la entidad.

d. Velar por el cumplimiento de los límites de inversión internos y regulatorios, e informar inmediatamente al Consejo Directivo y al Comité de Inversiones en caso de inobservancia de estos.

e. Aprobar el procedimiento para autorizar los excesos temporales a los límites internos establecidos para los distintos tipos de riesgos de inversión.

f. Aprobar y revisar anualmente las metodologías, parámetros, modelos y escenarios de estrés a ser utilizados para identificar, medir, analizar, monitorear, limitar, controlar, informar y revelar los riesgos de inversión a los que estén expuestas las carteras administradas.

g. Aprobar los estándares y/o procedimientos para el monitoreo diario de los riesgos de inversión a los que se encuentran expuestos los recursos de las carteras administradas.

h. Evaluar y someter a consideración del Consejo Directivo las propuestas del Comité de Inversiones, referidas a:

- Los límites internos de exposición a riesgo de inversión de manera global o por tipo de riesgo;
- Los niveles de alerta temprana para el control de los riesgos de inversión;
- Las inversiones en nuevas subclases de activo y/o tipos de instrumentos u operaciones, nuevos mercados, monedas, agentes intermediarios y contrapartes, emisores, entidades de custodia, mecanismos de negociación electrónica, entre otros; y,
- Las subclases de activo y/o tipos de instrumentos u operaciones de inversión que se sujetarán al proceso de autorización por parte de la Superintendencia de Banca, Seguros y AFP, de conformidad con lo indicado en el capítulo XVIII del Compendio de Normas Reglamentarias del Sistema Privado de Pensiones.

i. Realizar el seguimiento a las recomendaciones realizadas por el Departamento de Evaluación de Riesgos al Gerente General y al Comité de Inversiones.

j. Vigilar y monitorear el cumplimiento de los procedimientos referidos a los criterios de valorización de los diferentes instrumentos u operaciones de inversión.

C. COMITÉ DE INVERSIONES

Tiene por finalidad el desarrollo de acciones necesarias para alcanzar los objetivos planteados en el marco de las políticas de inversión de la CPMP.

D. COMITÉ DE CONTROL INTERNO

Fecha de creación: 2 de abril de 2009

Tiene por finalidad poner en marcha las acciones necesarias para la adecuada implementación del Sistema de Control Interno en la gestión de la entidad, y su eficaz funcionamiento por medio de la mejora continua.

Principales funciones:

a. Proponer al Presidente del Consejo Directivo la capacitación del personal de la entidad sobre el marco conceptual y normativo del control interno, con el propósito de facilitar el desarrollo de las acciones necesarias para la implementación del Sistema de Control Interno.

b. Recopilar información, estudiar y analizar el sistema de control interno existente en la entidad.

c. Formular el diagnóstico sobre el actual Sistema de Control Interno de la entidad.

d. Formular el Plan de Trabajo para la implementación del Sistema de Control Interno en la entidad, concordante con la normativa técnica de control vigente sobre el particular y conforme a la naturaleza de la CPMP.

e. Coordinar las acciones para el proceso de implementación del Sistema de Control Interno en todos los niveles de la organización.

f. Efectuar el seguimiento e informar al Presidente del Consejo Directivo sobre los resultados y avances del proceso de implementación del Sistema de Control Interno de la entidad.

E. COMITÉ DE GERENTES

Tiene por finalidad actuar como mecanismo de participación, información y toma de decisiones de las actividades ejecutadas en la CPMP.

Principales funciones:

a. Proponer las políticas, normas, objetivos y estrategias de la CPMP.

b. Discutir, analizar y proponer los planes estratégicos y operativos, así como las necesidades de recursos humanos, físicos y financieros necesarios para cumplir con dicha planificación.

c. Proponer el Manual de Organización y Funciones, así como los manuales de Descripción de Cargos, para la aprobación del Consejo Directivo.

d. Cumplir los acuerdos establecidos en las sesiones del Comité. Hacer planteamientos de las acciones correctivas y preventivas, cuando estas se requieran, respecto de la ejecución de los planes estratégicos y operativos.

e. Otras que, por su naturaleza, son de competencia del Comité.

1.2.5.2.POLÍTICAS DE LA CAJA DE PENSIONES MILITAR POLICIAL

El 2 de octubre de 2013, el Consejo de Supervisión solicitó que el planeamiento estratégico de la CPMP contenga acciones conducentes a:

- Proponer las modificatorias o ampliaciones al marco normativo, reglamentario y legal necesarios para optimizar la operatividad de la CPMP.
- Lograr una administración de los fondos de manera transparente y eficiente, recomendando los mecanismos objetivos que garanticen un adecuado proceso de rendimiento al Consejo de Supervisión.
- Desarrollar un plan de mejora de la calidad del servicio ofrecido a los afiliados, así como las acciones de austeridad necesarias, entre otros.
- Proponer el tratamiento futuro de los activos que respaldan el Régimen de Pensiones del Decreto Ley N° 19846, con el fin de optimizar y hacer más transparente la adecuada administración y rentabilización de las cuentas de depósitos, el portafolio de títulos y la cartera de créditos.

- Identificar y proponer con detalle las acciones conducentes a que las llamadas "Unidades de Negocio" se constituyan, definitivamente, en mecanismos de generación de renta a favor de los afiliados a la CPMP, buscando la recuperación de los recursos que hubieran sido asignados a las mismas en el tiempo y garantizando la absoluta transparencia de dichas acciones y sus respectivos resultados.
- Diseñar los mecanismos y naturaleza que contendrían las evaluaciones periódicas que permitan identificar la sostenibilidad financiera del Fondo de Garantía Pensionario Militar y Policial.
- Proponer las acciones necesarias a fin que la SBS disponga de los elementos legales necesarios y plenos para poder supervisar las acciones que se puedan tomar en la CPMP, tanto desde el punto de vista directriz como de gestión.

1.2.5.3.FILOSOFÍA DE LA CPMP

MISIÓN: "Garantizar el pago oportuno y sostenido de las prestaciones a los afiliados, brindando un servicio previsional de calidad".

VISIÓN: "Ser una entidad previsional cuya imagen, solvencia y calidad de servicio brinden plena seguridad y confianza a sus afiliados".

VALORES Y PRINCIPIOS INSTITUCIONALES:

Responsabilidad: Obligación moral de asumir, adecuada y eficientemente, las funciones y atribuciones asignadas.

Identidad: Compromiso de las personas al logro de los objetivos institucionales.

Productividad: Hábito de las personas a favor de la búsqueda permanente de formas más eficaces para lograr más resultados con los mismos o menos recursos.

Buen trato natural: Práctica constante de la empatía y de la cordialidad con las personas.

Honradez: Virtud de las personas reflejada en el respeto a los bienes ajenos.

Trabajo en equipo: Condición de trabajo en la que un conjunto de personas realiza actividades de manera organizada para alcanzar un objetivo común.

1.2.5.4.SISTEMA DE PENSIONES DEL PERSONAL MILITAR Y POLICIAL

El Régimen de Pensiones se creó el 26 de diciembre de 1972 por el Decreto Ley N° 19846, que unificó el Régimen de Pensiones del Personal Militar y Policial por los servicios prestados al Estado y los derechos que corresponden a sus deudos.

Las pensiones que se otorgan por medio de este régimen son: disponibilidad o cesación temporal, retiro o cesación definitiva e invalidez o incapacidad. Para los deudos, se otorga la pensión de sobrevivientes. Este régimen fue declarado cerrado con el Decreto Legislativo N° 1133, por lo que no admite nuevas incorporaciones o reincorporaciones.

Asimismo, el Decreto Legislativo N° 1133 creó el nuevo Régimen de Pensiones del Personal Militar y Policial, al que pertenece el personal que inicia la carrera de oficiales o suboficiales a partir del 10 de diciembre del año 2012. Su administración está a cargo de la CPMP.

Las pensiones a las que se pueden acceder con el presente régimen son: retiro, disponibilidad e invalidez o incapacidad; y para los deudos, la pensión de sobrevivientes.

Por otro lado, mediante el Decreto Ley N° 22595, a partir del 1 de julio de 1979 se actualizaron los porcentajes de aportes destinados al fondo de pensiones de los servidores públicos sujetos a los regímenes de los Decretos Leyes N° 19846, 20530 y 22303. El aporte para las pensiones de los trabajadores del sector público, comprendidos en los regímenes referidos, es equivalente al 12% del monto de las remuneraciones pensionables: 6% es descontado al trabajador y 6%, a cargo del Estado.

Cabe señalar que hasta el año 2017, el aporte del personal que se encuentre bajo el Régimen de Pensiones del Decreto Legislativo N° 1133 será equivalente al 12% de la remuneración pensionable: 6% a cargo del personal militar y policial, y 6% a cargo del Estado. Sin embargo, a partir del año 2018, el aporte de las personas que inicien la carrera de oficiales o suboficiales bajo este decreto legislativo, será equivalente al 19% de la remuneración pensionable: 13% a cargo del personal de las FF AA y de la PNP, y 6% a cargo del Estado.

Asimismo, la segunda disposición complementaria final del Decreto Legislativo N° 1133 dispuso conceder a los pensionistas del Régimen de Pensiones, regulado por el Decreto Ley N° 19846, un monto adicional a la pensión y los beneficios que perciben, equivalente al incremento de la remuneración otorgada al personal militar y policial en actividad. Las sumas que corresponden a este incremento, según el grado del personal, fueron establecidas en el Decreto Supremo N° 246-2012-EF.

Por otro lado, la undécima disposición complementaria final del Decreto Legislativo N° 1132 estableció el pago del subsidio póstumo y por invalidez para los actuales pensionistas del Decreto Ley N° 19846. Por ello, obtienen el derecho a pensión en casos de invalidez o fallecimiento del titular (viudez) de las FF AA y PNP, acaecido en acción de armas, acto de servicio, consecuencia del servicio o con ocasión del servicio.

Además, se establecieron nuevos tratamientos para el caso de los pensionistas del Decreto Ley N° 19846 que reinician actividades laborales a favor del Estado; presentándose dos (2) situaciones que dependen del momento en el que el pensionista adquiere dicha calidad. La primera corresponde al personal que pasó a ser pensionista antes de la fecha de entrada en vigencia del Decreto Legislativo N° 1133, quien percibe una pensión promedio equivalente a 1,505 nuevos soles; y la segunda, al personal que pasa a ser pensionista luego de la entrada en vigencia de dicho decreto, quien percibe una pensión promedio equivalente a 2,984 nuevos soles.

Finalmente, el marco legal aplicado a la CPMP es el siguiente:

- Decreto Ley N° 21021 de fecha 17 de diciembre de 1974 - "Ley de Creación de la Caja de Pensiones Militar Policial"
- Decreto Supremo N° 005-75-CCFA de fecha 22 de agosto de 1975 - "Reglamento de la Ley de Creación de la Caja de Pensiones Militar Policial"
- Decreto Ley N° 22595 de fecha 1 de julio de 1976 - "Se actualizaron los porcentajes de aportes destinados al Fondo de Pensiones de los servidores públicos sujetos a los regímenes de los Decretos Leyes N° 19846, 20530 y 22303"
- Decreto Ley N° 19846 de fecha 26 de diciembre de 1972 - "Ley de Pensiones Militar - Policial".
- Decreto Supremo N° 009-DE-CCFA de fecha 17 de diciembre de 1987 - "Reglamento de la Ley de Pensiones Militar - Policial".
- Decreto Legislativo N° 1133 de fecha 8 de diciembre de 2012 - "Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial".

1.3. MARCO CONCEPTUAL

Control: Son las medidas tomadas para disminuir la probabilidad de ocurrencia o impacto en caso que el riesgo se materialice.

Clientes: Factor de riesgo que corresponde a fallas negligentes o involuntarias de las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos físicos: Pérdidas derivadas de daños o perjuicios a activos físicos de la compañía.

Evento: Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

Eventos de pérdida: Son aquellos incidentes que generan pérdidas por riesgo operativo a las compañías.

Factores de riesgo: Se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo. La Superintendencia

de Banca, Seguros y AFP los clasifica en: internos (recurso humano, procesos, tecnología e infraestructura) y factores externos.

Impacto: Pérdida potencial que se puede generar en caso de ocurrencia del evento de riesgo operativo.

Indicador de riesgo: Un indicador de riesgo es un elemento empírico de naturaleza generalmente cuantitativa, aunque puede ser también de tipo cualitativo, cuyos valores son por lo general calculados con base en datos históricos que permiten representar la dimensión teórica o específica de un factor de riesgo considerado clave.

Dada la heterogeneidad de los factores que la componen, se puede estudiar realizando una división o clasificación de los factores de riesgo en otros tipos de riesgo que, teniendo la misma base conceptual, difieren significativamente en la naturaleza o las causas que lo originan. Esta clasificación puede facilitar el estudio del comportamiento de cada factor y la identificación del conjunto de indicadores de riesgo asociados a cada uno de ellos.

La vinculación del factor clave e indicador/es de riesgo se puede sintetizar del siguiente modo: factor clave es lo que es necesario medir e indicador de riesgo es cómo se mide el factor de riesgo.

La utilidad de los indicadores radica en la posibilidad de establecer un valor óptimo u objetivo para cada uno de ellos, y a partir de éste fijar intervalos de variación aceptables o niveles de criticidad. Los valores objetivos se determinan en función del grado de tolerancia establecido por la entidad, los objetivos estratégicos o los planes de negocio. En función del intervalo de variación establecido, la entidad puede definir planes de acción o medidas correctoras según el grado de desviación de los indicadores.

Pérdidas: Cuantificación económica de la ocurrencia de un evento de riesgo operativo, así como los gastos derivados de su atención.

Perfil de Riesgo: Resultado consolidado de la medición de los riesgos a los que se ve expuesta una empresa.

Políticas: Son los lineamientos generales que las compañías deben adoptar en relación con la GRO.

Procedimientos: Son la secuencia de actividades relacionadas entre sí que especifican su forma de ejecución para llevar a la práctica dentro de un proceso.

Procesos: Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

Relaciones laborales: Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y, en general, la legislación vigente sobre la materia.

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

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

Gestión del Riesgo Operacional (GRO): Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de

información y capacitación, mediante los cuales las compañías vigiladas identifican, miden, controlan y monitorean el riesgo operativo.

Unidad de Riesgo Operativo: Se entiende por el Departamento de Evaluación de Riesgos, el área o cargo, designada por la empresa, de acuerdo a las normativas de la Superintendencia de Banca, Seguros y AFP.

CAPÍTULO II

HIPÓTESIS Y VARIABLES

2.1. FORMULACIÓN DE HIPÓTESIS

2.1.1. HIPÓTESIS GENERAL

Existe un alto grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014.

2.1.2. HIPÓTESIS ESPECÍFICAS

H.E.1: Las categorías del riesgo operacional se relacionan significativamente en el nivel de gestión de la Caja de Pensiones Militar Policial.

H.E.2: Los componentes del marco que gestión de la Caja de Pensiones Militar Policial son organización, herramientas y reporting.

2.2. VARIABLES Y DEFINICIÓN OPERACIONAL DE VARIABLES

VARIABLES	DIMENSIONES	INDICADORES	INDICES
VARIABLE 1 RIESGO OPERACIONAL	CATEGORIAS DEL RIESGO OPERACIONAL	FRAUDE INTERNO	• ACTIVIDADES NO AUTORIZADAS
			• HURTO Y FRAUDE
		FRAUDE EXTERNO	• HURTO Y FRAUDE
			• SEGURIDAD DE SISTEMAS
		RELACIONES LABORALES Y SEGURIDAD EN EL PUESTO DE TRABAJO	• RELACIONES LABORALES
			• SALUD Y SEGURIDAD EN EL PUESTO
			• DIVERSIDAD Y DISCRIMINACIÓN
		PRÁCTICAS CON CLIENTES, PRODUCTOS Y NEGOCIOS	• ADECUACIÓN, DIVULGACIÓN DE INFORMACIÓN DE CONFIANZA
			• PRÁCTICAS INADECUADAS DE NEGOCIOS O MERCADO
		DAÑOS A ACTIVOS MATERIALES	• DESASTRES Y OTROS ACONTECIMIENTOS
		INTERRUPCIÓN DEL NEGOCIO Y FALLAS EN LOS SISTEMAS	• SISTEMAS
		EJECUCIÓN, ENTREGA Y GESTIÓN DE PROCESOS	• OPERACIONES
			• COMUNICACIÓN DE INFORMES
			• CLIENTES Y DOCUMENTACIÓN
			• CUENTAS DE CLIENTES
VARIABLE 2: GESTION	MARCO DE GESTION	ORGANIZACIÓN	• ESTRUCTURA • RESPONSABLE DE GRO • DOCUMENTOS DE GESTIÓN
		HERRAMIENTAS	• INDICADORES Y ALERTAS • AUTOEVALUACIONES • BASES DE DATOS
		REPORTING	• INFORMACIÓN EMITIDA • INFORMACIÓN RECIBIDA

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. TIPO Y NIVEL DE INVESTIGACIÓN

3.1.1. TIPO DE INVESTIGACIÓN

El tipo de investigación es "básica, conocida también como pura o fundamental, está destinada a aportar un cuerpo organizado de conocimientos científicos (...). Se preocupa de recoger información de la realidad para enriquecer el conocimiento teórico científico" (Valderrama Mendoza, 2005, pág. 28).

Con la presente investigación se pretendió aportar al conocimiento científico sobre el riesgo operacional.

3.1.2. NIVEL DE INVESTIGACIÓN

En este trabajo de investigación se utilizó el nivel de investigación correlacional, cuyo propósito es conocer la relación o grado de asociación que existe entre las variables en un contexto en particular (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010).

3.2. MÉTODO Y DISEÑO DE INVESTIGACIÓN

3.2.1. MÉTODO

El método empleado en el presente trabajo de investigación es el deductivo; que consiste en el razonamiento mental que permite descubrir nuevos conocimientos de lo general para llegar a lo particular y permite extender los conocimientos que se tienen

sobre la clase determinada de fenómenos a otro cualquiera que pertenezca a esa misma clase, (Bernal Torres, 2006, pág. 56).

3.2.2. DISEÑO

Diseño no experimental, transeccional, que según (Hernández Sampieri, Fernández Collado, & Baptista Lucio, Metodología de la Investigación, 2010) es un estudio que se realiza sin la manipulación deliberada de variables y en los que solo se observan los fenómenos en su ambiente natural para después analizarlos, recolectan datos en un solo momento y cuyo propósito es describir variables y analizar su incidencia y relación en un momento dado.

3.3. POBLACIÓN

3.3.1. CARACTERÍSTICAS Y DELIMITACIÓN

El presente proyecto de investigación tiene como población de estudio a los 116 colaboradores de la Caja de Pensiones Militar Policial.

3.3.2. UBICACIÓN ESPACIO - TEMPORAL

El estudio se realizó en las instalaciones de la Caja de Pensiones Militar Policial ubicada en Av. Jorge Basadre N° 950, Distrito de San Isidro – Lima.

3.4. MUESTRA

Para definir el tamaño de la muestra se ha utilizado el tipo de muestreo probabilístico, ya que según (Hernández Sampieri, Fernández Collado, & Baptista Lucio, Metodología de la Investigación, 2010), estas muestras son esenciales en los diseños de investigación transeccionales… donde se pretende hacer estimaciones y donde todos los elementos de la población tienen una misma probabilidad de ser elegidos.

3.4.1. TAMAÑO Y CÁLCULO DE LA MUESTRA

Para determinar el tamaño de la muestra de los colaboradores de la Caja de Pensiones Militar Policial se realizó la siguiente operación:

$$n = \frac{Z^2 \times p \times q \times N}{e^2 (N-1) + Z^2 \times p \times q}$$

Dónde:

n : Es el tamaño de la muestra que se va a tomar en cuenta para el trabajo de campo. Es la variable que se desea determinar.

p y q : Representan la probabilidad de la población de estar o no incluidas en la muestra. De acuerdo a la doctrina, cuando no se conoce esta probabilidad por estudios estadísticos, se asume que p y q tienen el valor de 0.5 cada uno.

Z : Representa las unidades de desviación estándar que en la curva normal definen una probabilidad de error= 0.05, lo que equivale a un intervalo de confianza del 95 % en la estimación de la muestra, por tanto el valor Z = 1.96.

N : El total de la población. Este caso 116 personas.

e : Representa el error estándar de la estimación. En este caso se ha tomado 5%

SUSTITUYENDO

$$n = \frac{(0.5 \times 0.5) \times 1.96^2 \times 116}{(0.05)^2 \ (116-1) + (0.5 \times 0.5) \times 1.96^2}$$

n = 89

Tamaño de la muestra: 89 trabajadores de la Caja de Pensiones Militar Policial.

Tabla 1: Distribución de la muestra

	POBLACIÓN		
DEPENDENCIA	Trabajadores	Porcentaje	**MUESTRA**
Consejo Directivo	**2**	**2.00%**	**2**
Gerencia General	**4**	**4.00%**	**3**
Gerencia Legal	**2**	**2.00%**	**2**
Departamento de Asesoría Corporativa	**3**	**3.00%**	**3**
Departamento de Asuntos Judiciales	**3**	**3.00%**	**3**
Gerencia de Informática	**14**	**10.00%**	**9**
Gerencia de Pensiones	**12**	**9.00%**	**8**
Departamento de Atención al afiliado	**16**	**13.00%**	**11**
Departamento de Recaudación y Liquidaciones	**11**	**9.00%**	**8**
Gerencia de Administración y Finanzas	**3**	**3.00%**	**3**
Departamento de Recursos Humanos	**4**	**4.00%**	**3**
Departamento de Logística	**15**	**11.00%**	**10**
Departamento de Contabilidad y Presupuesto	**6**	**6.00%**	**5**
Departamento de Tesorería	**3**	**3.00%**	**3**
Departamento de Inversiones Financieras	**3**	**3.00%**	**3**
Órgano de Control Institucional	**7**	**7.00%**	**5**
Gerencia de Riesgos y Desarrollo	**2**	**2.00%**	**2**
Departamento de Evaluación y Riesgos	**3**	**3.00%**	**3**
Departamento de Planeamiento y Organización	**3**	**3.00%**	**3**
TOTAL	116	100%	89

Fuente: Elaboración propia

3.5. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Las técnicas de recopilación de datos que se utilizaron en la investigación fueron las siguientes:

Encuesta – Cuestionario: técnica e instrumento que consiste en recopilar información sobre una parte de la población denominada muestra. Se elabora en función a las

variables e indicadores del trabajo de investigación. La construcción del cuestionario presupone seguir una metodología sustentada en: los objetivos, cuerpo de teorías, hipótesis, variables e indicadores"; se aplicó a los trabajadores de la Caja de Pensiones Militar Policial, que laboran en el Consejo Directivo, Gerencia General, Gerencia Legal, Gerencia de Informática, Gerencia de Pensiones, Gerencia de Administración y Finanzas, Órgano de Control Institucional y Gerencia de Riesgos y Desarrollo.

Análisis documental: se utilizó para evaluar la relevancia de la información que se considerará para el trabajo de investigación, relacionada a teorías relacionadas a riesgo operacional y gestión.

Escalamiento tipo Likert: "desarrollado por Rensis Likert en 1932.... Consiste en un conjunto de items presentados en forma de afirmaciones y juicios, ante los cuales se pide la reacción de los participantes. Es decir, se presenta cada afirmación y se solicita al sujeto que externe su reacción eligiendo uno de los cinco puntos o categorías de la escala. A cada punto se le asigna un valor numérico..." (Hernández Sampieri, Fernández Collado, & Baptista Lucio, Metodología de la Investigación, 2010)

Fichas bibliográficas: se utilizaron para tomar anotaciones de los libros, textos, revistas, normas y de todas las fuentes de información correspondientes a riesgo operacional y gestión.

3.6. PROCESAMIENTO Y ANÁLISIS DE DATOS

El procesamiento y análisis de los datos obtenidos del trabajo de campo se realizó mediante:

Ordenamiento y clasificación: se aplicó para tratar la información cualitativa y cuantitativa.

Registro manual: se aplicó para digitar la información de las diferentes fuentes.

Proceso computarizado con Excel: para determinar diversos cálculos matemáticos y estadísticos.

Statistical Package for the Social Sciences – SPSS: (paquete Estadístico para las Ciencias Sociales) desarrollado en la Universidad de Chicago; se utilizó para digitar, procesar y analizar datos y determinar indicadores promedios (sirve para estimar parámetros y probar hipótesis).

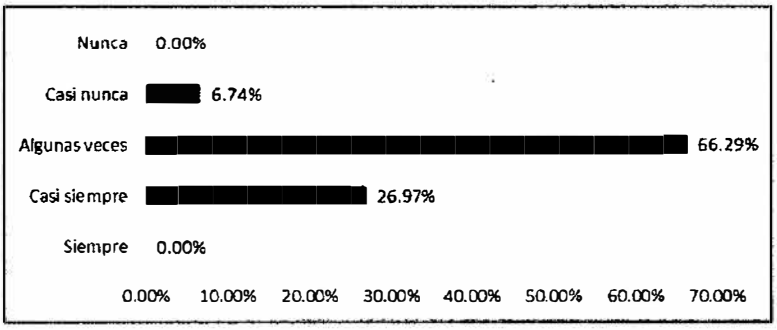
CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

CATEGORIAS DEL RIESGO OPERACIONAL

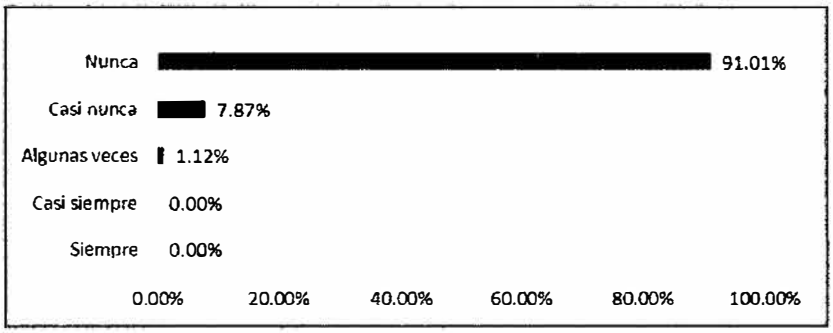
Gráfico 4.1: Las actividades de los colaboradores de la Caja de Pensiones Militar Policial, según autorización y/o supervisión del jefe inmediato, Lima, 2014



Fuente: Elaboración propia con base en las encuestas, 2014

Como se puede observar En el gráfico 4.1, el 66.29% de los encuestados, colaboradores de la Caja de Pensiones Militar Policial, declara que algunas veces sus actividades son autorizadas y/o supervisadas por su jefe inmediato y un 26.97% declara que casi siempre las actividades que realizan son supervisados y/o autorizados por sus jefes inmediatos.

Gráfico 4.2: Presentación de documentos falsos por parte de los miembros de la Caja de Pensiones de Pensiones Militar Policial, Lima, 2014



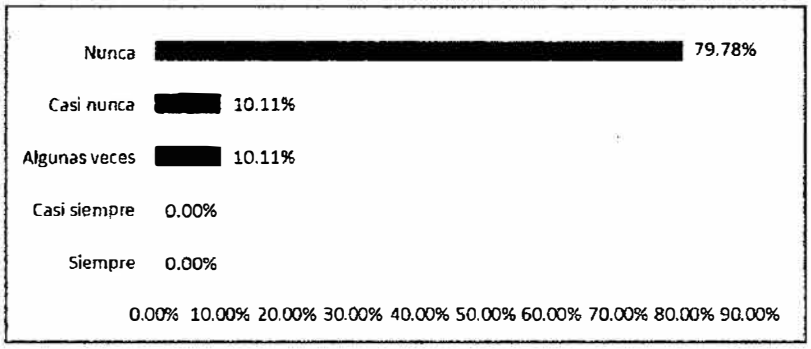
Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.2 se puede observar que sólo un 1.12% de los colaboradores de la Caja de Pensiones Militar Policial indicaron que alguna vez se pudo detectar documentación falsa presentado por un miembro de la entidad, tomando este resultado como general se puede inferir que en la entidad no se aprecia un nivel significativo de fraude interno.

Según (Arcenegui Rodrigo & Vicente, 2010) los propietarios, administradores y directivos deben mantener una conducta adecuada y deben implantar un correcto sistema de control interno para hacer que el resto de la organización evite comportamientos poco éticos que conlleven fraudes, enriquecimientos de dudosa legitimidad u otras irregularidades, ya que son riesgos de difícil gestión, que únicamente pueden ser abordados por la propia entidad definiendo de forma detallada los comportamientos y acciones no deseables y estableciendo las acciones correctoras cuando sean detectados a través de un sistema de control, tanto interno como externo, a lo largo de toda la organización.

Teniendo en cuenta el marco teórico se podría definir que la CPMP monitorea en gran medida las actividades de sus colaboradores evitando así el fraude interno.

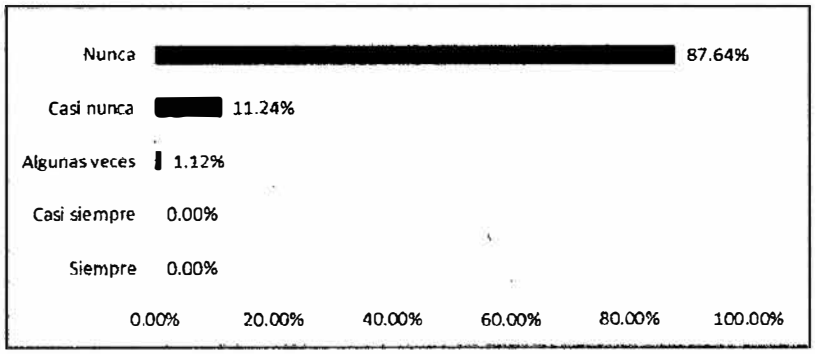
Gráfico 4.3: Documentos falsos presentados por personas ajenas en la Caja de Pensiones Militar Policial, Lima, 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

Se observa en la Gráfico 4.3, que en Caja de Pensiones Militar Policial, los colaboradores indican que en algunas ocasiones, el 10.11%, se ha podido detectar documentación falsa presentada por personas ajenas a la entidad.

Gráfico 4.4: Ataques informáticos y/o robo de información en la Caja de Pensiones Militar Policial, Lima, 2014



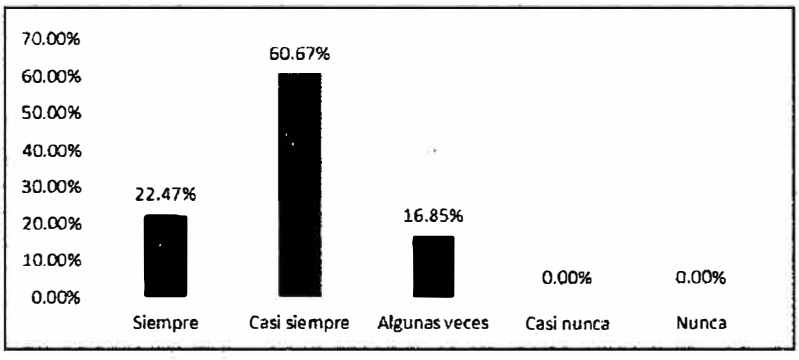
Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico N° 4.4 se aprecia que en menor porcentaje (1.12%) algunas veces los colaboradores de la Caja de Pensiones Militar Policial, fueron víctimas de ataques informáticos y/o robo de información en la entidad.

Según (García Ribas, 2010) dentro del grupo de controles deficientes dentro de una entidad se tiene, la seguridad lógica: es el control a los accesos a los sistemas, ya sea la que protege los aplicativos como la referente a accesos por internet y los documentos: toda la operativa que se realiza debe quedar documentada (firma de contratos de descuentos) y comunicaciones a los clientes. Si esa documentación no se ajusta a derecho, la entidad pierde protección jurídica y por consiguiente puede dar lugar a pérdidas operacionales.

En el caso de la CPMP se puede inferir que ha establecido controles que le permiten reducir este tipo de riesgos.

Gráfico 4.5: Las relaciones laborales y el normal desarrollo de las funciones de los colaboradores de la Caja de Pensiones Militar Policial, Lima, 2014

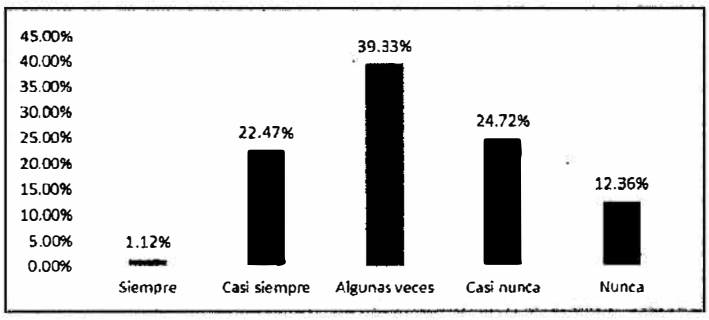


Fuente: Elaboración propia con base en las encuestas realizadas, 2014

Como se puede observar en el gráfico 4.5, el 60.67% de los encuestados de la Caja de Pensiones Militar Policial, declara que casi siempre las relaciones laborales se relacionan con el normal desarrollo de las funciones, mientras que el 22.47% acepta que las relaciones laborales siempre se relacionan con el normal desarrollo de las funciones de los colaboradores de la Caja de Pensiones Militar Policial.

Resultado que permite corroborar los expuestos por (Fernández Laviada & Martínez García, 2010), que concluyen que la introducción de forma generalizada el RO en la cultura de las organizaciones que a la vez ésta influirá en las relaciones laborales, siendo el principal reto al que deberán enfrentarse las entidades que quieran implantar con éxito un marco completo de gestión del RO. Sin embargo, la gestión correcta y completa de este riesgo no sólo les servirá para cumplir con la normativa y regulación vigente sino que les permitirá, además, reducir las pérdidas por fallos operacionales, los riesgos de control y mejorar la calidad de los servicios.

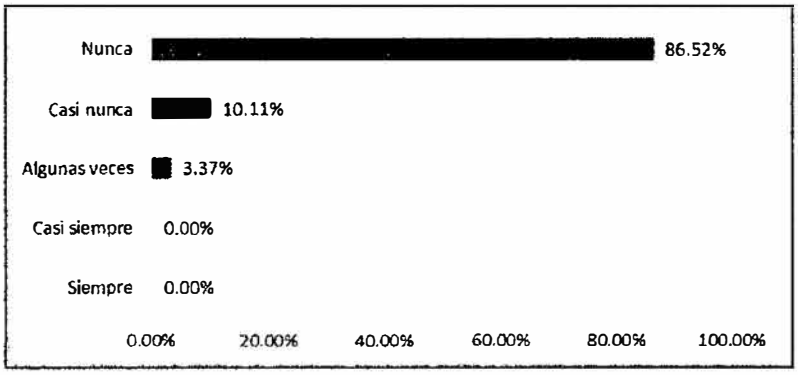
Gráfico 4.6: Las condiciones óptimas remunerativas y contractuales y el desempeño de sus funciones en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.6 se observa que un 39.33% de los encuestados considera que algunas veces existen condiciones óptimas remunerativas y contractuales frente a un 24.72% de los colaboradores de la Caja de Pensiones Militar Policial, que considera que casi nunca existe estas condiciones; dado estos resultados se podría considerar que estas condiciones podrían pasar a ser aspectos de riesgo operacional que la entidad debería considerar; que para poder difuminarlo se deberá tener en cuenta el informe COSO (1997, pp. 31-2) que relaciona tres razones por las que se realizan prácticas fraudulentas o cuestionables: los incentivos, las tentaciones y la ignorancia. El informe continúa indicando que la condición suficiente para implantar la ética empresarial es el ejemplo, dado que los empleados suelen imitar a sus líderes.

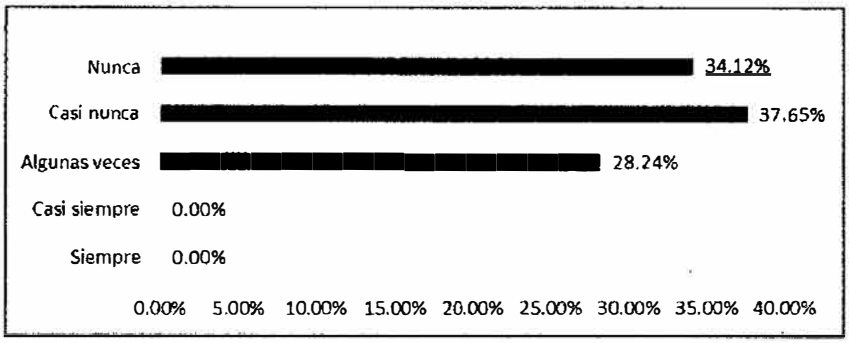
Gráfico 4.7: Actos de discriminación e intolerancia a la diversidad en la Caja de Pensiones Militar Policial, Lima, 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.7 evidencia que en la Caja de Pensiones Militar Policial, algunas veces (3.37%) o casi nunca (10.11%) se han presentado casos de discriminación e intolerancia a la diversidad pero a pesar de ello se podría deducir que en la entidad impera el respeto a los demás.

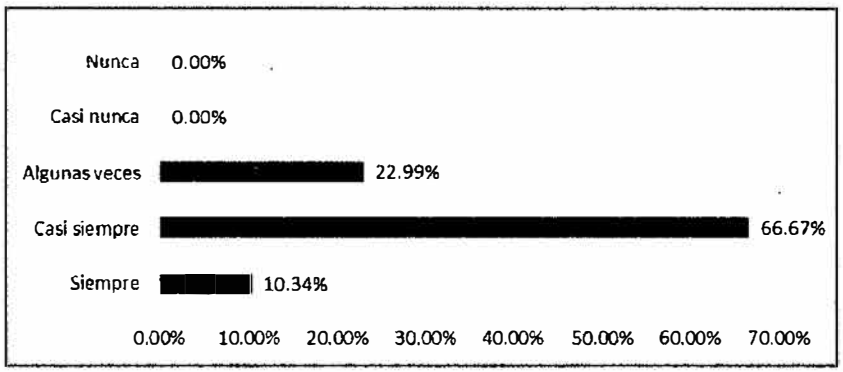
Gráfico 4.8: Actos de violación de privacidad al brindar información al usuario interno o externo en la Caja de Pensiones Militar Policial, Lima, 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.8, los colaboradores de la CPMP indican que casi nunca (37.65%) han cometido actos de violación a la privacidad, confusión de cuentas y/o uso de información confidencial.

Gráfico 4.9: Identificación correcta de las personas que solicitan información en la Caja de Pensiones Militar Policial, Lima, 2014

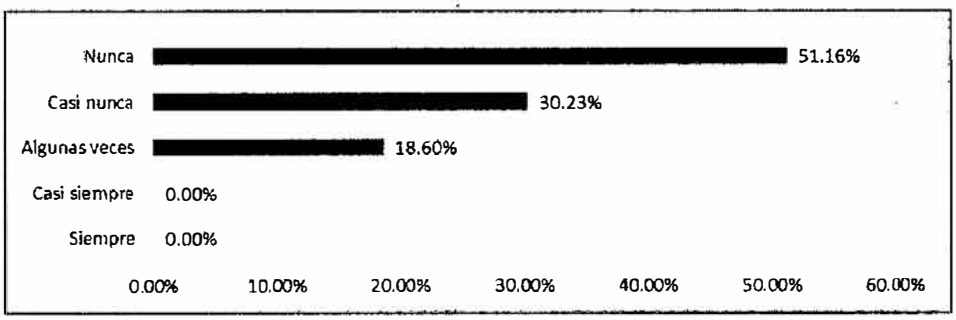


Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.9, el 66.67% de las personas que solicitan información se identifican correctamente o portan la debida autorización para hacer consultas.

Lo que evidencia que el RRHH de la CPMP se encuentra bien capacitado para realizar sus actividades diarias, esto en contraste con lo que afirma (García Ribas, 2010) que el recurso más importante es el RRHH, ya que sin una adecuada política de gestión de RRHH no se puede pensar en gestionar correctamente el riesgo operacional.

Gráfico 4.10: Paralización de actividades debido a fallas en el sistema informático y/o incidentes en suministros causados por factores externos en la Caja de Pensiones Militar Policial, Lima, 2014

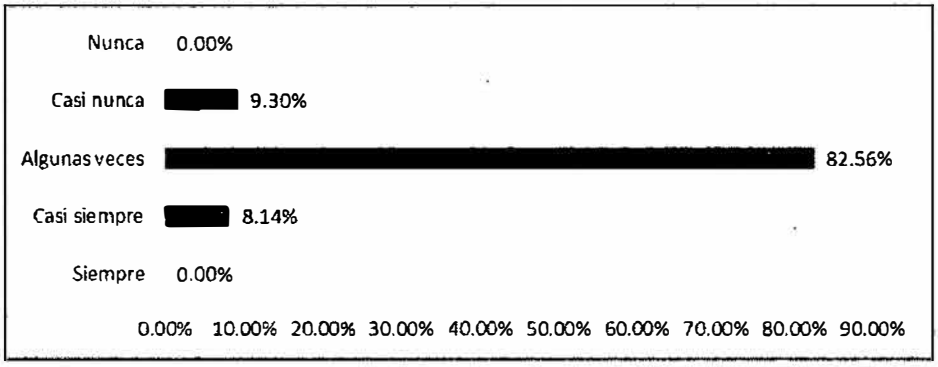


Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.10, el 82.56% los colaboradores de la Caja de Pensiones Militar Policial, indicaron que tuvieron que paralizar algunas veces sus actividades debido a fallas en el sistema informático, telecomunicaciones y/o incidentes en suministros causados por factores externos. Según (García Ribas, 2010) dentro de los recursos tecnológicos es conveniente segregar este grupo que engloba el hardware (computadores, cableado, servidores, etc.) y el software

(conjunto de programas que rigen los aplicativos) los factores externos no pueden ser controlados por la entidad.

Gráfico 4.11: Errores de introducción de datos, incumplimiento de plazos y/o responsabilidades en la Caja de Pensiones Militar Policial, Lima 2014

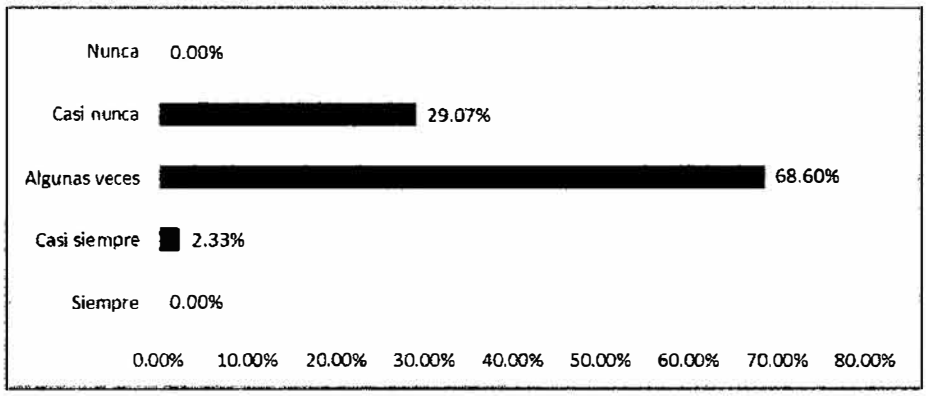


Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.11, se puede apreciar que el 82.56% de los encuestados indica que ha cometido errores de introducción de datos, incumplimiento de plazos y/o responsabilidades.

Según (García Ribas, 2010) en muchos casos los aplicativos no incorporan los elementos de filtrado necesarios para mitigar el riesgo operacional o no cumplen los objetivos para los que fueron diseñados, esto acompañado de segregación funcional que se da cuando un mismo individuo puede ejecutar dos o más funciones incompatibles entre sí, se genera un riesgo evidente de fraude.

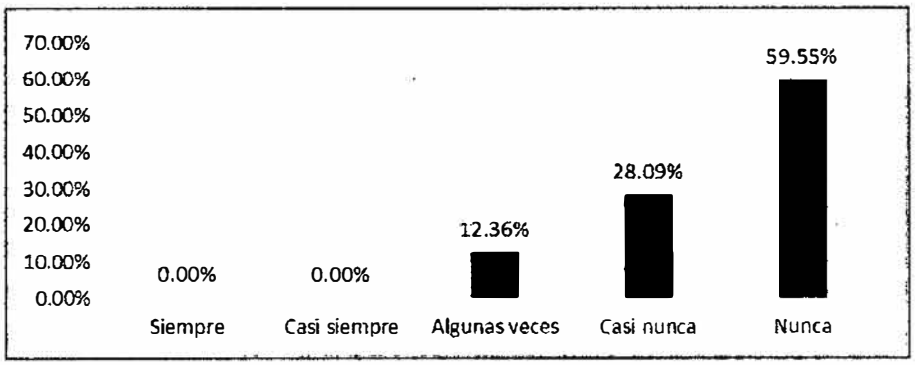
Gráfico 4.12: Información inexacta y/o incumplimiento de esta obligación con el cliente interno o externo en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.12, el 68.60% de los colaboradores de la Caja de Pensiones Militar Policial, manifiestan haber brindado información inexacta y/o haber incumplido con esta obligación con el cliente tanto interno como externo que solicita información.

Gráfico 4.13: Acceso no autorizado a cuentas de usuarios y/o información confidencial en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

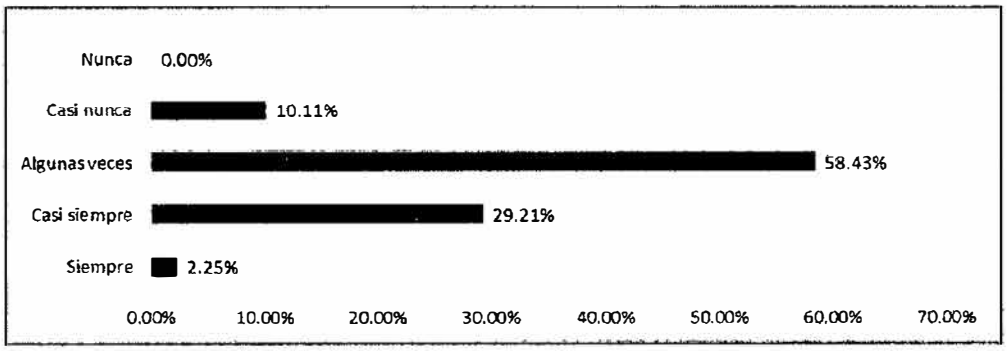
En el gráfico 4.13, solo el 12.36% de los colaboradores de la Caja de Pensiones Militar Policial, algunas veces ha tenido acceso no autorizado a cuentas de usuarios, registro de clientes y/o

información confidencial frente a un 59.55% de los encuestados nunca ha tenido acceso no autorizado a cuentas de usuarios, registro de clientes y/o información confidencial.

Según (Arranz Álamo & Rodríguez López, 2010) estos tipos de incidentes corresponden a pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

MARCO DE GESTIÓN

Gráfico 4.14: La estructura organizativa de la Caja de Pensiones Militar Policial y la gestión y cumplimiento de la misión organizacional



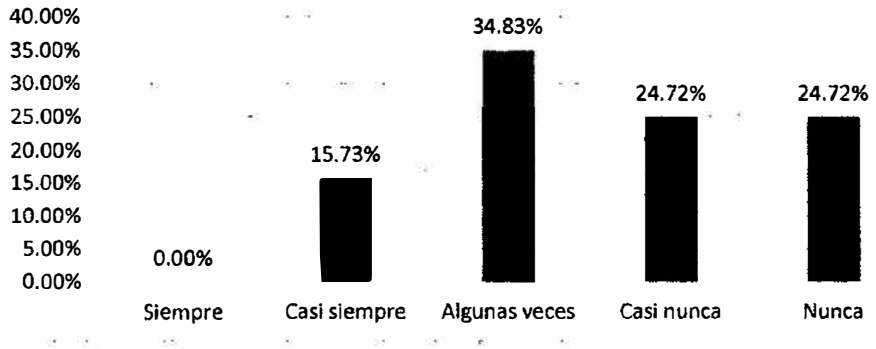
Fuente: Elaboración propia con base en las encuestas realizadas, 2014

Del gráfico 4.14, se puede apreciar que el 58.43% de los encuestados considera que algunas veces, la estructura organizativa de la Caja de Pensiones Militar Policial permite una adecuada gestión y cumplimiento de la misión organizacional y un 29.21% considera que casi siempre la estructura que maneja la CPMP permite una adecuada gestión de la misma y por ende permite el cumplimiento de la misión organizacional.

(Fernández Madrazo, Rodríguez Navamuel, & Rosich Parte, 2010) señalan que la estructura organizativa permite lograr la eficacia en el funcionamiento de todo el sistema de gestión del RO si se tiene una estructura organizativa adecuada que incluye la creación de un comité de RO por el que se implique la alta dirección y definición de su composición, funciones, etc., la existencia de una entidad operativa específica para la gestión del RO con los medios humanos y técnicos necesarios; la asignación de responsables de RO en cada área organizativa de la entidad y en las sociedades del grupo y la adecuada segregación de funciones entre las funciones de gestión y control del RO

Al contrastar la literatura con el organigrama de la CPMP se puede decir que se encuentra en proceso de adecuación organizativa con miras a mejorar la gestión del riesgo operacional.

Gráfico 4.15: Manual de procedimiento de las actividades que se desarrolla en la Caja de Pensiones Militar Policial, Lima 2014

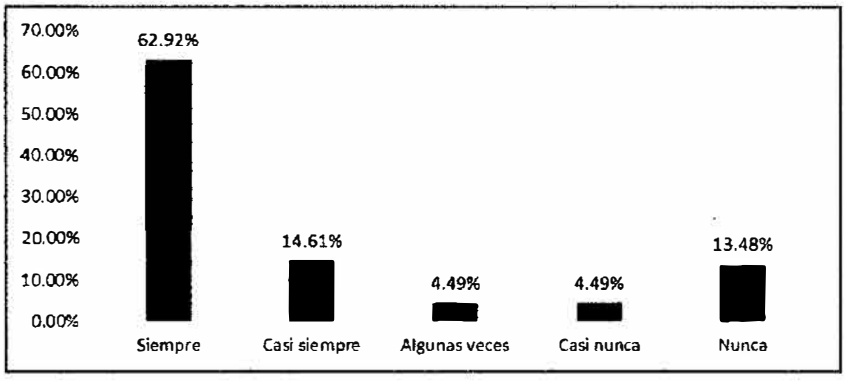


Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.15, se puede apreciar que solo algunas veces (34.83%) los colaboradores de la Caja de Pensiones Militar Policial indican que contaron con manuales de procedimientos para la realización de sus actividades en el área donde laboran, frente a un 24.72% que manifiesta que casi nunca o nunca tuvieron un manual de procedimientos; lo que evidencia que estos

aspectos pueden pasar a constituirse como factores de riesgo operacional ya que según (Fernández Madrazo, Rodríguez Navamuel, & Rosich Parte, 2010) la inexistencia de manuales operativos o de procedimientos de las actividades desarrolladas en la entidad o la inexistencia de manuales de funciones, que definan el ámbito de actuación de las diferentes áreas de la entidad constituyen factores internos de riesgo operacional.

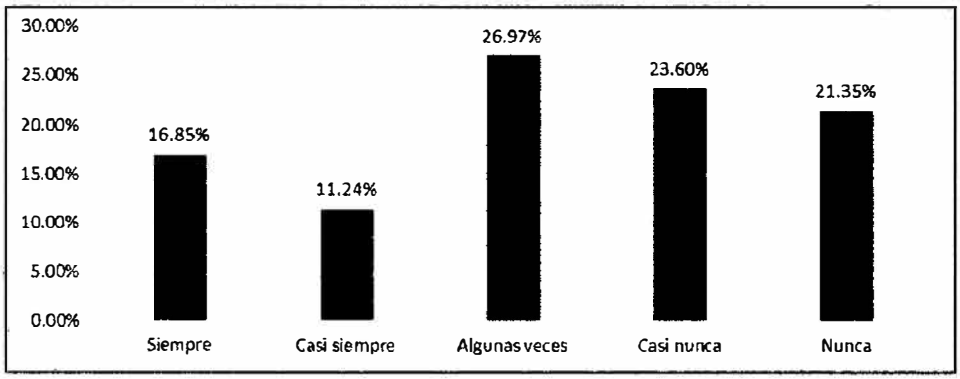
Gráfico 4.16: Acceso a documentos de gestión en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.16, se observa que el 62.92% de los colaboradores de la Caja de Pensiones Militar Policial, indican que siempre tienen acceso a los documentos de gestión, como el MOF, Plan Estratégico y otros.

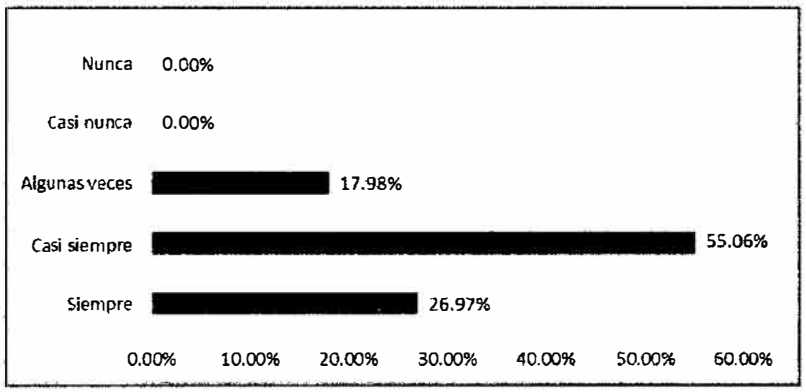
Gráfico 4.17: Revisión de los documentos de gestión en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

Se observa en el gráfico 4.17) que solo un 26.97% de los encuestados de la Caja de Pensiones Militar Policial, alguna vez ha revisado los documentos de gestión, de lo que se puede inferir que los colaboradores de la CPMP no se encuentran identificados con la parte filosófica de la entidad.

Gráfico 4.18: Actividades de autoevaluación de la gestión institucional en la Caja de Pensiones Militar Policial, Lima 2014

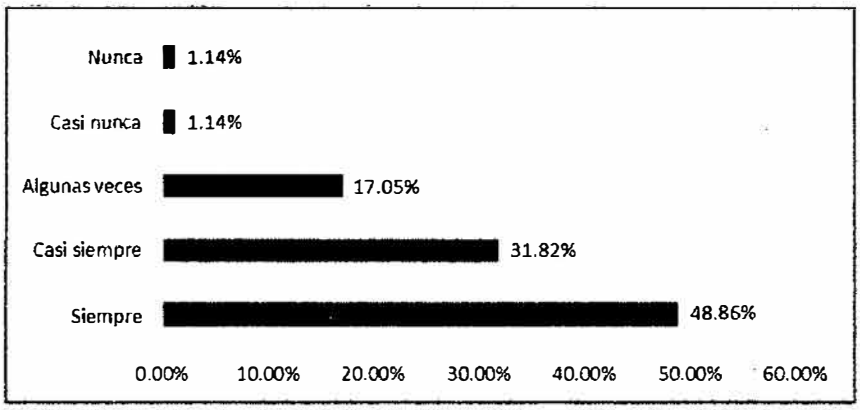


Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.18, se puede apreciar que un 55.06% de los encuestados de la Caja de Pensiones Militar Policial, manifiesta que casi siempre la entidad realiza actividades de autoevaluación de la gestión institucional.

Según (Fernández Madrazo, Rodríguez Navamuel, & Rosich Parte, 2010) este tipo de autoevaluaciones puede darse de mejor manera mediante auditoría externa siempre en cuanto se tenga en consideración los siguientes: el alcance de los trabajos de auditoría externa realizados, el grado de importancia de las recomendaciones efectuadas, el grado de implementación de las mismas, así como su previsión para finalizarlas, la existencia o no de limitaciones al alcance o salvedades en el informe, causas que las han originado y plazo de corrección estimados.

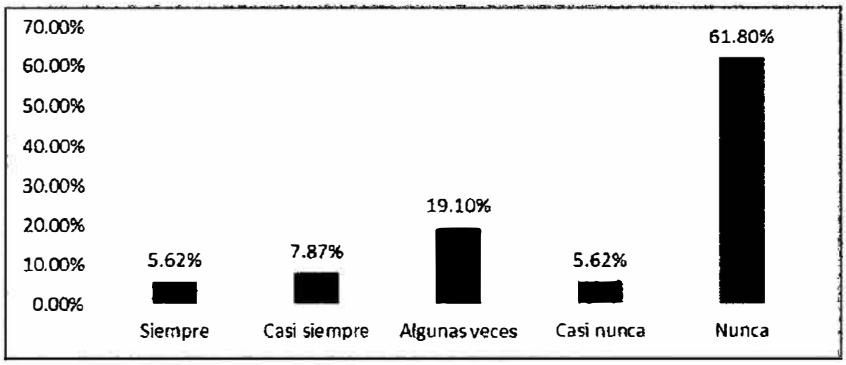
Gráfico 4.19: Base de datos en las áreas de la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

Se observa en el gráfico 4.19 que los colaboradores de la Caja de Pensiones Militar Policial indicaron que el 48.86% de las áreas cuentan con su propia base de datos.

Gráfico 4.20: Reportes de información sobre riesgo operacional en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Elaboración propia con base en las encuestas realizadas, 2014

En el gráfico 4.20 se puede observar que los encuestados de la Caja de Pensiones Militar Policial indican que nunca (61.80%) han contado con un reporte de información emitida y/o recibida sobre riesgo operacional; lo que evidencia el desconocimiento de los integrantes de la mayoría de las áreas que las bases de datos que ellos manejan son una fuente de información útil y relevante para la toma de decisiones en la entidad, ya que esta información permitirá la identificación de las áreas problemáticas así como las acciones correctivas pertinentes, también evidencia que el circuito de la información no se está llevando de manera satisfactoria, no se eleva a la alta dirección y esta no está devolviendo la información procesada a las áreas pertinentes para el posterior control de un posible riesgo organizacional tal como lo manifestó (Fernández Madrazo, Rodríguez Navamuel, & Rosich Parte, 2010).

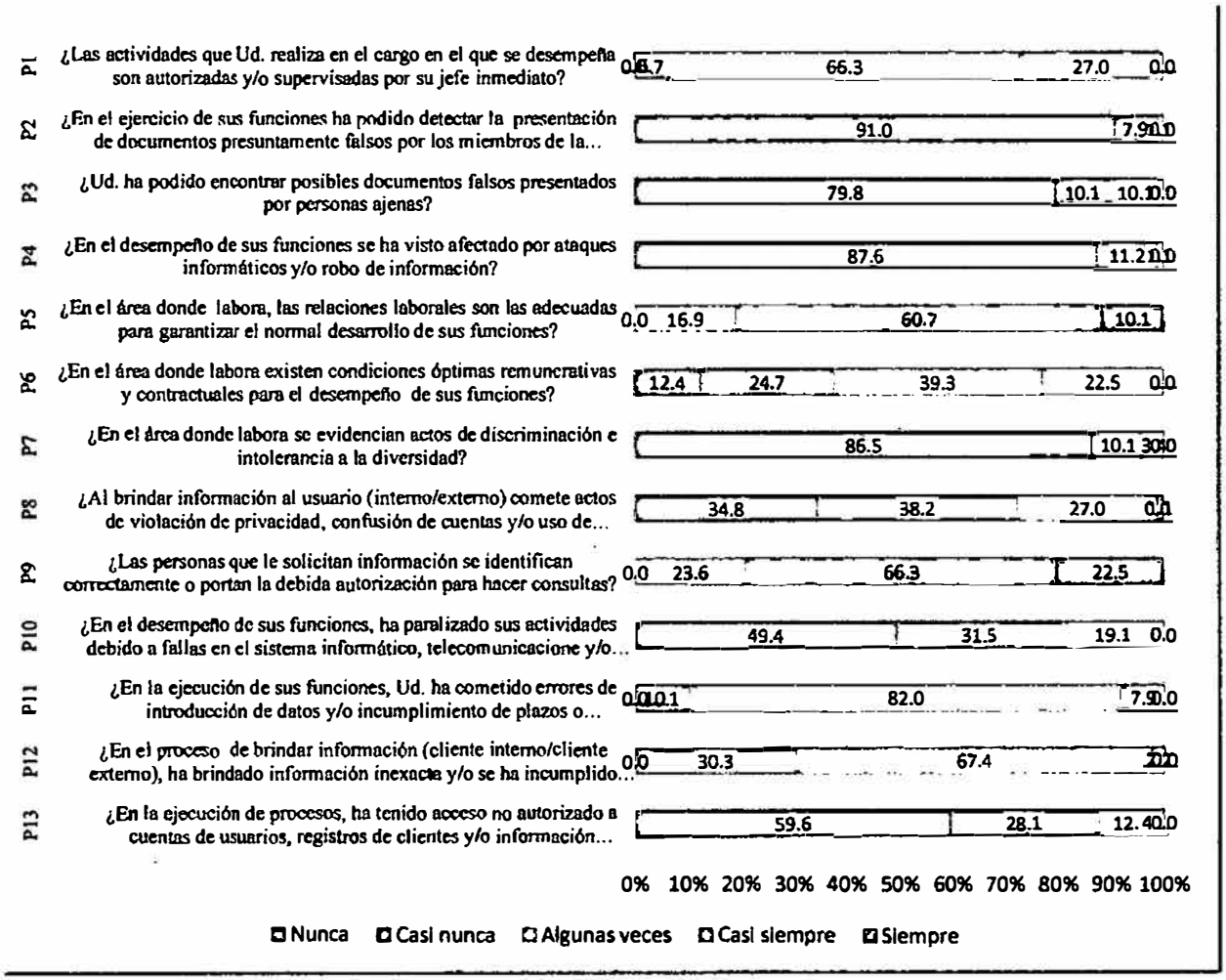
4.1.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DEL RIESGO OPERACIONAL Y EL NIVEL DE GESTIÓN DE LA CAJA DE PENSIONES MILITAR POLICIAL

Tabla 2: Categorías del riesgo operacional

N°	COMPONENTES	Nunca		Casi nunca		Algunas veces		Casi siempre		Siempre	
		n	%	n	%	n	%	n	%	n	%
P1	¿Las actividades que Ud. realiza en el cargo en el que se desempeña son autorizadas y/o supervisadas por su jefe inmediato?	0	0.0	6	6.7	59	66.3	24	27.0	0	0.0
P2	¿En el ejercicio de sus funciones ha podido detectar la presentación de documentos presuntamente falsos por los miembros de la entidad?	81	91.0	7	7.9	1	1.1	0	0.0	0	0.0
P3	¿Ud. ha podido encontrar posibles documentos falsos presentados por personas ajenas?	71	79.8	9	10.1	9	10.1	0	0.0	0	0.0
P4	¿En el desempeño de sus funciones se ha visto afectado por ataques informáticos y/o robo de información?	78	87.6	10	11.2	1	1.1	0	0.0	0	0.0
P5	¿En el área donde labora, las relaciones laborales son las adecuadas para garantizar el normal desarrollo de sus funciones?	0	0.0	0	0.0	15	16.9	54	60.7	20	22.5
P6	¿En el área donde labora existen condiciones óptimas remunerativas y contractuales para el desempeño de sus funciones?	11	12.4	22	24.7	35	39.3	20	22.5	1	1.1
P7	¿En el área donde labora se evidencian actos de discriminación e intolerancia a la diversidad?	77	86.5	9	10.1	3	3.4	0	0.0	0	0.0
P8	¿Al brindar información al usuario (interno/externo) comete actos de violación de privacidad, confusión de cuentas y/o uso de información confidencial?	31	34.8	34	38.2	24	27.0	0	0.0	0	0.0
P9	¿Las personas que le solicitan información se identifican correctamente o portan la debida autorización para hacer consultas?	0	0.0	0	0.0	21	23.6	59	66.3	9	10.1
P10	¿En el desempeño de sus funciones, ha paralizado sus actividades debido a fallas en el sistema informático, telecomunicaciones y/o incidentes en suministros causados por factores externos?	44	49.4	28	31.5	17	19.1	0	0.0	0	0.0
P11	¿En la ejecución de sus funciones, Ud. ha cometido errores de introducción de datos y/o incumplimiento de plazos o responsabilidades?	0	0.0	9	10.1	73	82.0	7	7.9	0	0.0
P12	¿En el proceso de brindar información (cliente interno/cliente externo), ha brindado información inexacta y/o se ha incumplido con esta obligación?	0	0.0	27	30.3	60	67.4	2	2.2	0	0.0
P13	¿En la ejecución de procesos, ha tenido acceso no autorizado a cuentas de usuarios, registros de clientes y/o información confidencial?	53	59.6	25	28.1	11	12.4	0	0.0	0	0.0

Fuente: Elaboración propia con base en las encuestas realizadas,-2014

Gráfico 4.21: Categorías del Riesgo Operacional en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Elaboración propia con base en las encuestas realizadas 2014

Partiendo de la definición del riesgo operacional planteada por el Comité de Basilea, en la que establece que "el riesgo operacional se define como el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos".

Los resultados obtenidos de la investigación de campo, reflejados en la Tabla 4.1 y Gráfico 4.21 ; muestran que el indicador Categorías de riesgo debería de atenderse mejor, ya que se

observa que solo algunas veces las actividades que realiza el colaborador es supervisado y/o supervisado por su jefe inmediato (66.3%) lo que origina que un 83% comete errores en la introducción de datos y/o incumplimiento de plazos o responsabilidades (pregunta N° 11) y como resultado en el proceso de brindar información al cliente interno y/o cliente externo se le transmita información inexacta y/o se ha incumpla con esta obligación ya que los datos que se tienen no son fiables.

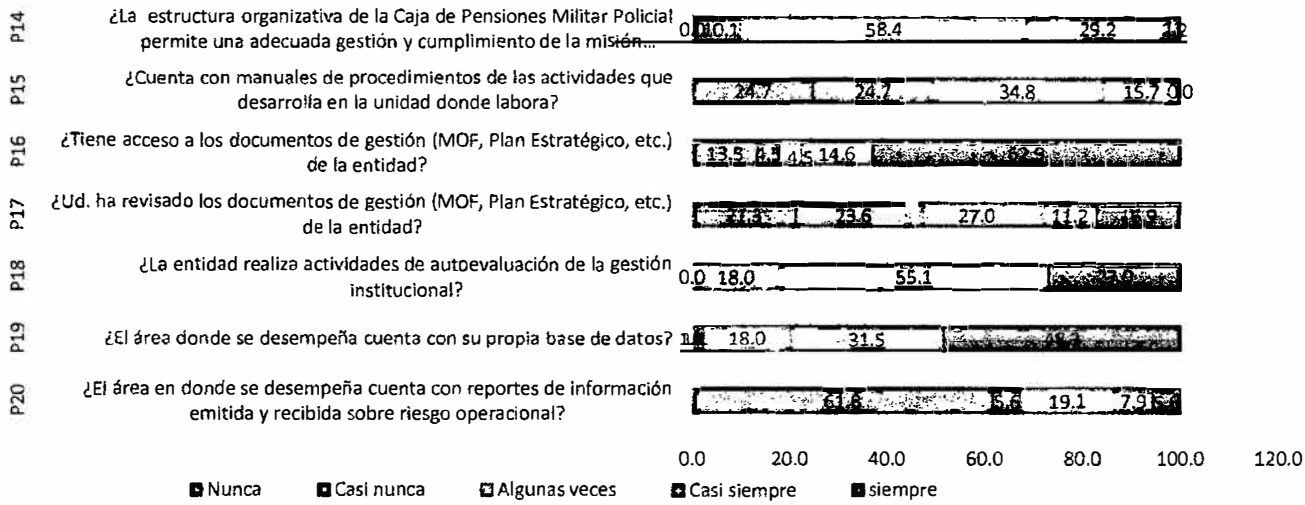
Por otro lado, si bien las relaciones laborales que mantienen los colaboradores es catalogado como adecuado casi siempre por el 60.7% de los encuestados, permitiéndoles el normal desarrollo de sus funciones; estos consideran que la parte remunerativa y contractual solo algunas veces es óptimo (39.3), evidenciando un ligero descontento puesto que un 24.7% considera que casi nunca es óptimo.

Tabla 3: Marco de Control

N°	COMPONENTES	Nunca		Casi nunca		Algunas veces		Casi siempre		siempre	
		N	%	N	%	N	%	N	%	N	%
P14	¿La estructura organizativa de la Caja de Pensiones Militar Policial permite una adecuada gestión y cumplimiento de la misión organizacional?	0	0.0	9	10.1	52	58.4	26	29.2	2	2.2
P15	¿Cuenta con manuales de procedimientos de las actividades que desarrolla en la unidad donde labora?	22	24.7	22	24.7	31	34.8	14	15.7	0	0.0
P16	¿Tiene acceso a los documentos de gestión (MOF, Plan Estratégico, etc.) de la entidad?	12	13.5	4	4.5	4	4.5	13	14.6	56	62.9
P17	¿Ud. ha revisado los documentos de gestión (MOF, Plan Estratégico, etc.) de la entidad?	19	21.3	21	23.6	24	27.0	10	11.2	15	16.9
P18	¿La entidad realiza actividades de autoevaluación de la gestión institucional?	0	0.0	0	0.0	16	18.0	49	55.1	24	27.0
P19	¿El área donde se desempeña cuenta con su propia base de datos?	1	1.1	1	1.1	16	18.0	28	31.5	43	48.3
P20	¿El área en donde se desempeña cuenta con reportes de información emitida y recibida sobre riesgo operacional?	55	61.8	5	5.6	17	19.1	7	7.9	5	5.6

Fuente: Encuestas realizadas a los colaboradores de la CPMP-2014

Gráfico 4.22: Marco de gestión en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Encuestas realizadas a los colaboradores de la CPMP-2014

El marco de control para la gestión del riesgo operacional (RO) se compone de aquellos elementos esenciales y necesarios para crear un ambiente de gestión de los riesgos operacionales; uno de los aspectos importantes de ello es el de establecer una estructura organizativa que permita una adecuada gestión y el logro de la misión de la CPMP, sin embargo de acuerdo a la percepción de los colaboradores de la Caja de Pensiones Militar Policial, la estructura que se tiene solo es adecuada algunas veces (58.4%); esto aunado a que solo algunas veces cuentas con un manual de procedimientos (34.8%). El 62.9% de los encuestados tiene acceso a los documentos de gestión de la entidad, pero solo algunas veces han sido revisados por estos (27%). Cada área siempre maneja su propia base de datos (48.3%) de los trabajos que realiza pero estos datos obtenidos nunca han sido sintetizados en un reporting de riesgo operacional (61.8%).

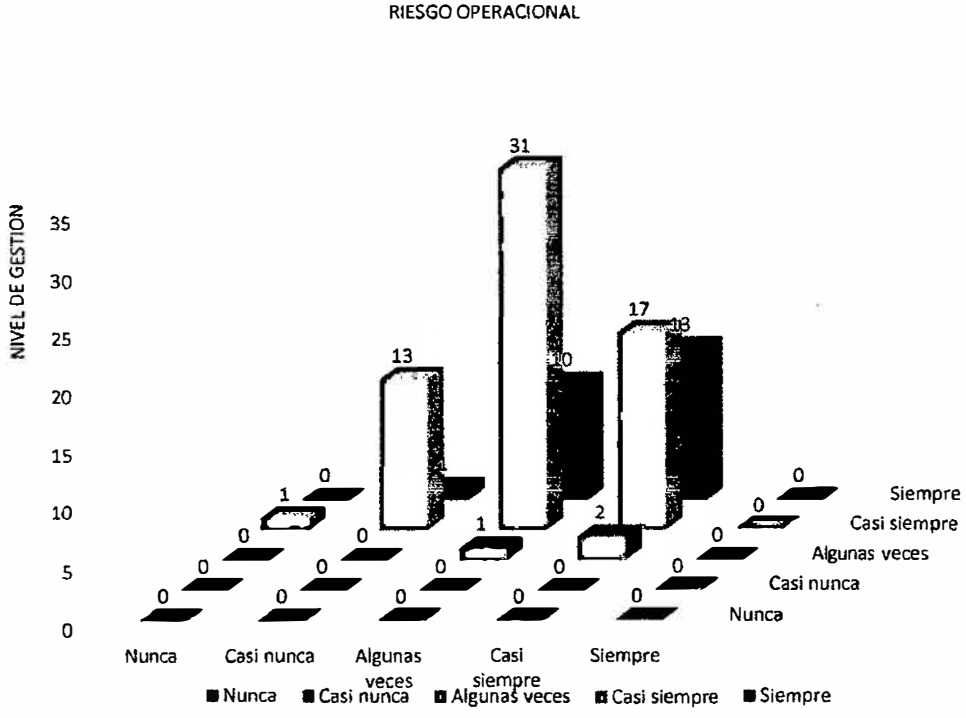
4.2. DISCUSIÓN

Tabla 4: Relación entre el riesgo operacional y el nivel de gestión en la Caja de Pensiones Militar Policial, Lima 2014

VARIABLES		RIESGO OPERACIONAL											
		Nunca		Casi nunca		Algunas veces		Casi siempre		Siempre		Total	
		N	%	N	%	N	%	N	%	N	%	N	%
GESTIÓN	Nunca	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
	Casi nunca	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
	Algunas veces	0	0.0	0	0.0	1	1.1	2	2.2	0	0.0	3	3.4
	Casi siempre	1	1.1	13	14.6	31	34.8	17	19.1	0	0.0	62	69.7
	Siempre	0	0.0	1	1.1	10	11.2	13	14.6	0	0.0	24	27.0
	Total	1	1.1	14	15.7	42	47.2	32	36.0	0	0.0	89	100.0

Fuente: Encuestas realizadas a los colaboradores de la CPMP-2014

Gráfico 4.23: Riesgo operacional y nivel de gestión en la Caja de Pensiones Militar Policial, Lima 2014



Fuente: Encuestas realizadas a los colaboradores de la CPMP-2014

INTERPRETACIÓN: El riesgo operacional tiene como objetivo promover una cultura de gestión de riesgo que incremente el entendimiento y acción de las personas e incluya promoción de la eficiencia y control efectivo; en este sentido la entidad para gestionar eficientemente este riesgo necesita mejorar su marco de gestión, desde su estructura implementando unidades específicas de riesgo operacional, dotando a los colaboradores de manuales de procedimientos para la realización de sus actividades y adecuando sus documentos de gestión al riesgo operacional pero sobre todo mejorando los canales de comunicación para que cada uno de los colaboradores esté al tanto de lo que significa gestionar el riesgo operacional (herramientas y reporting).

4.3. CONTRASTACIÓN DE HIPÓTESIS

Para iniciar la contrastación de las hipótesis, un primer aspecto es tener en cuenta dos tipos de hipótesis, la hipótesis principal o alternativa y la hipótesis nula.

La hipótesis alternativa es aquella que defiende y busca contrastar la investigadora. La hipótesis nula es aquella que sirve para dar objetividad a la investigación. En estadística, en investigación, una hipótesis nula es una hipótesis construida para anular o refutar, con el objetivo de apoyar una hipótesis alternativa. Cuando se utiliza, la hipótesis nula se presume verdadera hasta que la contrastación estadística en la forma de una prueba empírica de la hipótesis indique lo contrario, cuyo procedimiento se presenta a continuación.

Las hipótesis secundarias han sido contrastadas adecuadamente y sus resultados constan en los papeles de trabajo.

Para fines prácticos se presenta la contrastación de la hipótesis principal del trabajo de investigación.

HIPÓTESIS GENERAL O ALTERNATIVA:

H_1: Existe un alto grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial.

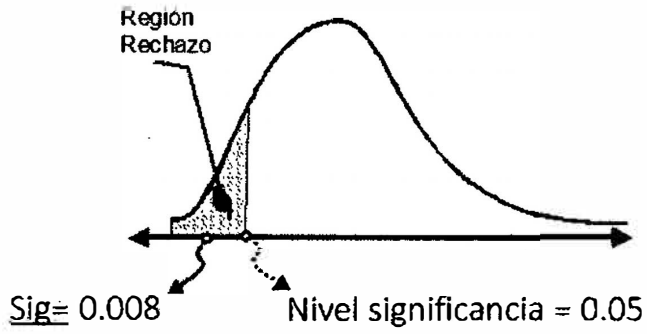
HIPÓTESIS NULA

H_0: No existe un alto grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial.

Tabla 5: Prueba de Chi-cuadrada de Pearson relación entre el riesgo operacional y el nivel de gestión en la Caja de Pensiones Militar Policial.

		Riesgo operacional
Gestión	Chi cuadrado	8,667
	Gl	6
	Sig.	,008[a,b]

Fuente: Elaboración propia



Se observa que la prueba de Chi cuadrada de Pearson se deduce como el valor "sig. Asintot" es 0,008 menor a 0,05 nivel de significancia; entonces se rechaza la hipótesis nula; por lo que podemos afirmar que **"Existe un alto grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial."**, razón por la que la hipótesis general se acepta.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Primera: Existe un alto grado de relación entre el riesgo operacional y el nivel de gestión en la Caja de Pensiones Militar Policial. El riesgo operacional en la Caja de Pensiones Militar Policial está condicionado a sus diferentes categorías como fraude interno, fraude externo, relaciones laborales y seguridad en el puesto de trabajo, prácticas con clientes, productos y negocios, daños a activos materiales, interrupción del negocio y fallas en los sistemas, ejecución, entrega y gestión de procesos.

Segunda: La Caja de Pensiones Militar Policial se ve vulnerada en sus actividades, debido a fallas en el sistema informático y/o incidentes en los suministros causados por factores externos; condiciones contractuales, remunerativas, desempeño de funciones, errores de ingresos de datos, incumplimiento de plazos y/o responsabilidades; información brindada inexacta y/o incumplimiento de la obligación de dar información, tanto al cliente interno como externo. Por lo tanto, las categorías del riesgo operacional que se relacionan con el nivel de gestión de la Caja de Pensiones Militar Policial son: las prácticas con los clientes, procesos y negocios; interrupción del negocio y fallas en el sistema; ejecución, entrega y gestión de procesos; y relaciones laborales y seguridad en el puesto de trabajo.

Tercera: La gestión de la Caja de Pensiones Militar Policial está enmarcada en una institución que cuenta con una estructura organizativa; documentos de gestión; base de datos; autoevaluaciones y cuenta con información emitida y recibida

sobre riesgo operacional, aunque en menor medida. Por tanto, los componentes del marco de gestión de la Caja de Pensiones Militar Policial son organización, herramientas y reporting.

5.2. RECOMENDACIONES

Primera: Se recomienda que la Caja de Pensiones Militar Policial tenga un mejor control de las categorías del riesgo operacional que permita mejorar el nivel de gestión, de esa manera poder mejorar la relación entre el riesgo operacional y el marco de gestión de la Caja de Pensiones Militar Policial.

Segunda: Las categorías de riesgo operacional que la Caja de Pensiones Militar Policial debe controlar en mayor medida son las relacionadas a la exactitud de la información que se brinda al cliente interno y externo; al cumplimiento de las obligaciones de los colaboradores; control en los procesos de introducción de datos, cumplimiento de plazos, desarrollo de actividades deducidas de las fallas en el sistema informático y/o incidentes en los suministros causados por factores externos y la mejora de las condiciones remunerativas y contractuales para el buen desempeño de los colaboradores.

Tercera: La Caja de Pensiones Militar Policial debe mejorar su organización mediante acciones de sensibilización en los trabajadores sobre la importancia de los conocimientos y usos de los documentos de gestión; implementar una adecuada base de datos en todas las áreas de la entidad sobre riesgo operacional y rediseñar su estructura organizacional para una adecuada gestión del riesgo operacional.

BIBLIOGRAFÍA

Anduig Aldea, M., & López Álvarez, A. (2010). Tipología y codificación de los eventos de riesgo operacional. En A. Fernández Laviada, *La gestión del riesgo operacional: de la teoría a su aplicación* (págs. 230 - 246). Cantabria, Laredo, España: LIMUSA - Noriega Editores.

Arcenegui Rodrigo, J., & Vicente, O. C. (2010). El riesgo operacional en el gobierno corporativo. En A. Fernández laviada, *La gestión del riesgo operacional: de la teoría a su aplicación* (págs. 137 - 153). Cantabria, Laredo, España: LIMUSA - Noriega Editores.

Arranz Álamo, J., & Rodríguez López, M. (2010). Mapa de riesgos: herramienta de identificación y gestión de riesgos. En A. Fernández Laviada, *La gestión del riesgo operacional: de la teoría a su aplicación* (págs. 371 - 380). Cantabria, Laredo, España: LIMUSA - Noriega Editores.

ASBA. (01 de febrero de 2015). *Riesgo Operativo.* Obtenido de www.asbaweb.org/.../Reporte%20Final%20ASBA%20-%20WG2%20-%...

Ávalos Ruiz, C. (2012). *Análisis, diseño e implementación del sistema de riesgo operacional para entidades financieras SIRO.* Lima: Pontificia Universidad Católica del Perú.

Bernal Torres, C. A. (2006). Metodología de la Investigación para administración, economía, humanidades y ciencias sociales. Naucalpan, México: Pearson Educación.

Comité de Basilea de Supervisión Bancaria. (2004). *Sanas prácticas para la gestión y supervisión del riesgo operativo.*

Comité de Supervisión Bancaria de Basilea. (2004). *Convergencia internacional de medidas y normas de capital.*

Diario El Peruano. (03 de Abril de 2009). Resolución SBS 2116-2009. *Reglamento de la Gestión de Riesgo Operacional.*

Fernández Laviada, A., & Martínez García, F. J. (2006). *El riesgo opercional como desafío para las entidades financieras. Estudio empírico del caso español.*

Fernández Laviada, A., & Martínez García, J. (2010). *El riesgo operacional como desafío para las entidades financiera. Estudio empírico del caso español.* Universidad de Cantabria.

Fernández Laviada, A., & Martínez, F. (2010). *La gestión del riesgo operacional: de la teoría a su aplicación.* Cantabria, Laredo, España: LIMUSA - Noriega Editores.

Fernández Madrazo, J., Rodríguez Navamuel, G., & Rosich Parte, J. (2010). La visión del auditor interno sobre riesgo operacional. En A. Fernández Laviada, *La gestión del riesgo operacional: de la teoría a su aplicación* (págs. 544 - 546). Cantabria, Laredo, España: LIMUSA - Noriega Editores.

García Ribas, J. (2010). Marco de gestión del riesgo operacional. En A. Fernández Laviada, *La gestión del riesgo operacional: de la teoría a su aplicación* (págs. 183 - 198). Cantabria, Laredo, España: LIMUSA - Noriega Editores.

Gimeno Coma, X. (2010). Integración de los métodos cuantitativo y cualitativo. En A. Fernández Laviada, *La gestión del riesgo operacional: de la teoría a su aplicación* (págs. 287 - 295). Cantabria, Laredo, España: LIMUSA - Noriega Editores.

Hanson García, J., & Salazar Noriega, P. (2005). *http://www.tesis.uchile.cl/.* Obtenido de http://www.tesis.uchile.cl/tesis/uchile/2005/garcia_j2/sources/garcia_j2.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). *Metodología de la Investigación* (Quinta ed.). México D. F.: McGraw-Hill.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). *Metodología de la Investigación* (Quinta ed.). México D. F.: McGraw-Hill.

Valderrama Mendoza, S. (2005). Pasos para elaborar proyectos y tesis de investigación científica. Lima, Perú: Editorial San Marcos.

Vázquez Alonso, P. (2010). La importancia de las herramientas en la gestión práctica del riesgo operativo. En A. Fernández Laviada, *La gestión del riesgo operacional: de la teoría a su aplicación* (págs. 305 - 319). Cantabria, Laredo, España: LIMUSA - Noriega Editores.

ANEXOS

MATRIZ DE CONSISTENCIA

RIESGO OPERACIONAL Y NIVEL DE GESTION DE LA CAJA DE PENSIONES MILITAR POLICIAL, 2014

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	ÍNDICES	METODOLOGÍA
PROBLEMA GENERAL ¿Cuál es el grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014? **PROBLEMAS ESPECÍFICOS** • ¿Cómo las categorías del riesgo operacional se relacionan con el nivel de gestión de la Caja de Pensiones Militar Policial? • ¿Qué componentes se consideran en el marco de gestión de la Caja de Pensiones Militar Policial?	**OBJETIVO GENERAL** Determinar el grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014 **OBJETIVOS ESPECÍFICOS** • Explicar las categorías del riesgo operacional y su relación con el nivel de gestión de la Caja de Pensiones Militar Policial • Determinar los componentes del marco de gestión de la Caja de Pensiones Militar Policial	**HIPÓTESIS GENERAL** Existe un alto grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial, 2014. **HIPÓTESIS ESPECÍFICAS** • Las categorías del riesgo operacional se relacionan significativamente en el nivel de gestión de la Caja de Pensiones Militar Policial • Los componentes del marco que gestión de la Caja de Pensiones Militar Policial son organización, herramientas y reporting	**VARIABLE 1: RIESGO OPERACIONAL**	**CATEGORIAS DEL RIESGO OPERACIONAL**	Fraude interno	• Actividades no autorizadas • Hurto y fraude	**Tipo** Investigación básica **Nivel** correlacional **Método** Deductivo **Diseño** No experimental - transeccional **Población** 116 trabajadores de la Caja de Pensiones Militar Policial **Muestra** 89 trabajadores de la Caja de Pensiones Militar Policial **Técnicas de recolección de información** Encuestas **Instrumentos de recolección de información** Cuestionario de encuesta
					Fraude externo	• Hurto y fraude • Seguridad de sistemas	
					Relaciones laborales y seguridad en el puesto de trabajo	• Relaciones laborales • Salud y seguridad en el puesto • Diversidad y discriminación	
					Prácticas con clientes, productos y negocios	• Adecuación, divulgación de información y confianza • Prácticas inadecuadas de negocios o mercado	
					Daños a activos materiales	• Desastres y otros acontecimientos	
					Interrupción del negocio y fallas en los sistemas	• Sistemas	
					Ejecución, entrega y gestión de procesos	• Operaciones • Comunicación de informes • Clientes y documentación • Cuentas de clientes	
			VARIABLE 2: GESTIÓN	**MARCO DE GESTIÓN**	Organización	• Estructura • Documentos de gestión.	
					Herramientas	• Indicadores y alertas • Autoevaluaciones • Bases de datos	

Fuente: MOF – CPMP

RELACIÓN DE PERSONAL DE LA CPMP - SEPTIEMBRE 2014

Nro.	Apellidos y Nombres	Cargo	Condición
	CONSEJO DIRECTIVO		
1	SILVA BERENGUEL MARÍA PATRICIA	ASISTENTE PRESIDENCIA CONSEJO DIRECTIVO	Permanente
2	ARGOTE LOZANO ROXANA OLINDA	SECRETARIO DEL CONSEJO DIRECTIVO	Permanente
	GERENCIA GENERAL		
3	KIJIARA TOMITA FERNANDO	GERENTE GENERAL (C)	Permanente
4	ROSSI VALDEZ KATIA MARÍA	ASISTENTE DE GERENCIA	Permanente
5	LÁZARO SABINO REYES EMILIANO	AUXILIAR ADMINISTRATIVO (CONSERJE)	Permanente
6	ESCUDERO AMADO MARÍA ELENA	COORDINADOR DE GERENCIA GENERAL	Permanente
	GERENCIA LEGAL		
7	ZAVALA MORA CLARA MARIA	GERENTE LEGAL	Permanente
8	ALMANDOZ LÓPEZ ROSA LAEL PEGGY	ASISTENTE DE GERENCIA	Permanente
	Dpto. de Asesoría Corporativa		
9	INGA JAIME SANDY MARIBEL	JEFE DEL DEPARTAMENTO DE ASESORÍA CORPORATIVA	Permanente
10	AGUIRRE JUSTINIANI GLORIA	ABOGADO	Contratado
11	CALOMINO ARELLANO FIORELLA SOLANGE	ABOGADO	Contratado
	Dpto. de Asuntos Judiciales		
12	GARCIA SANCHEZ LIZELI DIANA	JEFE DEL DEPARTAMENTO DE ASUNTOS JUDICIALES	Permanente
13	BRENIS MONTEZA LOURDES MILAGROS	ABOGADO (ASUNTOS JUDICIALES)	Contratado
14	GIANINO BUSTINZA ANGELA MARIA	ABOGADO (ASUNTOS JUDICIALES)	Contratado
	GERENCIA DE INFORMÁTICA		
15	KANEKO LA ROSA JORGE ALEXANDER	GERENTE DE INFORMÁTICA	Permanente
16	IPARRAGUIRRE EPIQUEN EDILBERTO EDUVIGS	ESPECIALISTA EN DIRECCIÓN DE PROYECTOS DE SISTEMAS DE INFORMACIÓN	Contratado
17	TORRES GUIZADO CHARITO SOLEDAD	ANALISTA FUNCIONAL	Permanente
18	NAUPAY MORALES JULIO MARTIN	ANALISTA FUNCIONAL	Contratado
19	CHÁVEZ CELACIO CARMEN ROSA	ANALISTA PROGRAMADOR	Permanente
20	GUERRERO LADERO LILIANA ROSA	ASISTENTE DE GERENCIA	Permanente
21	CAMPOS ALVARADO JULIO CESAR	ESPECIALISTA EN DIRECCIÓN DE OPERACIONES DE TECNOLOGÍAS DE LA INFORMACIÓN	Permanente
22	GOVEA LUZÓN JANET IVONNE	ANALISTA PROGRAMADOR	Permanente
23	LA ROSA GUERRERO BENJYIN ADRAIAN	ASISTENTE DE SOPORTE TÉCNICO	Permanente
24	LOO SEGURA SUSI MOYLAN	ANALISTA PROGRAMADOR	Contratado
25	HUAPAYA NAVARRO JUAN JOSE	ANALISTA PROGRAMADOR	Contratado
26	SHUAN BRINGAS CHRISTIAN HERNANDO	ANALISTA PROGRAMADOR	Contratado
27	TOMA OSORES SILVIA KYOKO	ANALISTA PROGRAMADOR	Contratado
28	DAMAZO MEJIA SAUL ENRRIQUE	ANALISTA PROGRAMADOR	Contratado
	GERENCIA PENSIONES		
29	PAZ INGOSO VIRGILIO	GERENTE DE PENSIONES (E)	Permanente
30	RATTO CORNELIO MARÍA DEL CARMEN	COORDINADOR DE RECUPERACIONES	Permanente
31	SAAVEDRA PRATTO MARÍA ROSA	COORDINADOR DE CONTROL DE CALIDAD	Permanente
32	DE MARZO ARATA MARÍA DEL CARMEN	ASISTENTE DE GERENCIA	Permanente
33	CARDENAS VELASQUEZ WALTER AUGUSTO	ASISTENTE DE CONTROL DE CALIDAD	Permanente
34	VARA FRANCO MAXIMO FELIPE	ASISTENTE LEGAL	Contratado
35	SÁNCHEZ HERRERA VÍCTOR	AUXILIAR DE CONTROL DE CALIDAD	Contratado
36	ALTAMIRANO PINEDO JULIETA JINETH	AUXILIAR DE RECUPERACIONES	Contratado
37	ZAVALA TOYKIN ROSA PATRICIA	ASISTENTE LEGAL	Contratado
38	FLORES SOTO MARTHA ROCIO	AUXILIAR DE RECUPERACIONES	Permanente
39	ELIAS AGUILAR SABRINA	AUXILIAR DE CONTROL DE CALIDAD	
40	SANTA CRUZ LOPEZ MIGUELANGEL	AUXILIAR DE RECUPERACIONES	Contratado
	Dpto. de Atención al Afiliado		

Nro.	Apellidos y Nombres	Cargo	Condición
	Dpto. de Recaudación y Liquidaciones		
57	GARCIA CUPE MARÍA DE LOS MILAGROS	ASISTENTE DE PENSIONES (LIQUIDACIONES)	Permanente
58	PAJARES QUISPE CARLOS ENRIQUE	ASISTENTE DE PENSIONES (RECAUDACIÓN)	Permanente
59	CALDERÓN MONCADA OLGA MARINA	ANALISTA DE SEGUIMIENTO Y COMUNICACIÓN	Permanente
60	CABALLERO ROJAS PEDY LEE	JEFE DE DEPARTAMENTO DE RECAUDACIÓN Y LIQUIDACIONES (E)	Permanente
61	VILLACREZ MENDOZA VÍCTOR ALEJANDRO	AUXILIAR DE PENSIONES (LIQUIDACIONES)	Permanente
62	GONZALES ARROYO FIORELLA SILVETTA	AUXILIAR DE PENSIONES (GESTIÓN DE DOCUMENTOS)	Contratado
63	CALONGE SAAVEDRA GISELA ROXANA	AUXILIAR DE PENSIONES (RECAUDACIÓN)	Contratado
64	TAPARA SOSA ANA MARÍA	AUXILIAR DE PENSIONES (LIQUIDACIONES)	Contratado
65	HUAMANI FLORES ANA	AUXILIAR DE PENSIONES (LIQUIDACIONES)	Contratado
66	VERGARA VARGAS JHONNY	AUXILIAR DE PENSIONES (LIQUIDACIONES)	Contratado
67	GUTIERREZ LEYVA ANDREA LUCIA	AUXILIAR DE PENSIONES (LIQUIDACIONES)	Contratado
	Gerencia de Administración y Finanzas		
68	FONSECA TADOMA FELIPE RIGOBERTO	GERENTE DE ADMINISTRACIÓN Y FINANZAS	Permanente
69	MILLENDEZ CASTILLO BRENDA VIVIAN	ESPECIALISTA EN FINANZAS	Permanente
70	RIOJA ARANA CAROLA PATRICIA	ASISTENTE DE GERENCIA	Permanente
	Dpto. de Recursos Humanos		
71	MORENO SUAREZ CRISTINA ZUSSET	JEFE DEL DEPARTAMENTO DE RECURSOS HUMANOS	Permanente
72	CATTER VERGARA GIANUIR MARIETTA	ASISTENTE DE DESARROLLO HUMANO	Permanente
73	RUBASTO TORRES ISABEL MARLENI	ASISTENTE ADMINISTRATIVO (REMUNERACIONES Y BENEFICIOS)	Permanente
74	SÁNCHEZ CHÁVEZ YUMA LILIANA	ASISTENTA SOCIAL	Permanente
	Dpto. de Logística		
75	SOLÍS TORRES VÍCTOR FÉLIX	JEFE DEL DEPARTAMENTO DE LOGÍSTICA	Permanente
76	HUAMANI OJEDA MARIA JANET	ASISTENTE ADMINISTRATIVO (ADQUISICIONES)	Permanente
77	QUEVEDO SILVA MANUEL FRANCISCO	ASISTENTE ADMINISTRATIVO (SERVICIOS GENERALES Y ALMACÉN)	Permanente
78	LIMA RAMOS ENRIQUE ANÍBAL	AUXILIAR ADMINISTRATIVO (CHOFER)	Permanente
79	LLÓN GONZALES MAX LUIS	AUXILIAR ADMINISTRATIVO (MANTENIMIENTO)	Permanente
80	GÓMEZ QUIÑONES ULISES MANUEL	AUXILIAR ADMINISTRATIVO (MANTENIMIENTO)	Permanente
81	TRUJILLO LAGUNA MARCIAL	AUXILIAR ADMINISTRATIVO (CHOFER)	Permanente
82	CARDEÑO BALLADARES HÉCTOR GERMAN	ASISTENTE ADMINISTRATIVO (CONTROL DE ACTIVOS, TRANSPORTES Y SEGUROS)	Permanente
83	REDREGAL RAMIREZ RICARDO LUIS	AUXILIAR ADMINISTRATIVO (SEGURIDAD)	Permanente
84	QUISPE VÁSQUEZ ARTURO	AUXILIAR ADMINISTRATIVO (SEGURIDAD)	Permanente
85	OLIVA VARA OSWALDO RONALD	ASISTENTE ADMINISTRATIVO (ARCHIVO CENTRAL)	Permanente
86	FÉLIX OLA JUAN CARLOS	AUXILIAR ADMINISTRATIVO (ARCHIVO PROVISIONAL)	Permanente
87	RIMARACHIN SALDAÑA WILLY ROY	AUXILIAR ADMINISTRATIVO (RECEPCIONISTA DE SEGURIDAD Y TRAMITE DOCUMENTARIO)	Contratado
88	PERALTA PÉREZ PERI THORATON	AUXILIAR ADMINISTRATIVO (ARCHIVO CENTRAL)	Contratado
89	AGUIRRE MARTINEZ ALFONSO VÍCTOR	AUXILIAR ADMINISTRATIVO (ARCHIVO CENTRAL)	Contratado
	Dpto. de Contabilidad y Presupuesto		
90	CORREA MARTÍNEZ FERNANDO	JEFE DEL DPTO. DE CONTABILIDAD Y PRESUPUESTO (CONTADOR GENERAL)	Permanente
91	RAZALAR RUIZ RONALD YVAN	ANALISTA DE CONTABILIDAD (IMPUESTOS Y CONTRIBUCIONES)	Permanente
92	HERRERA VELAZCO DANIEL WILFREDO	ESPECIALISTA EN CONTABILIDAD	Permanente
93	SEVILLA GOMEZ TERESA	ASISTENTE DE CONTABILIDAD (INFORMACION FINANCIERA INVERSIONES)	Permanente
94	RUELAS PEREZ YENNI AURELIA	ESPECIALISTA EN PRESUPUESTO	Permanente

	Dpto. de Tesorería		
96	JANAMA CHOTA VICENTE	JEFE DEL DEPARTAMENTO DE TESORERÍA	Permanente
97	[illegible]	[illegible]	Contratado
98	[illegible]	ASISTENTE DEL DEPARTAMENTO DE TESORERÍA	Contratado
	Dpto. de Inversiones Financieras		
99	SEBASTIAN CALVO VILMA ESTHER	JEFE DEL DEPARTAMENTO DE INVERSIONES FINANCIERAS	Permanente
100	PALMI PADILLA MANUEL FRANCISCO	ASISTENTE DE INVERSIONES FINANCIERAS	
101	RAMIDA QUILICHE BERNARDO JACS	ASISTENTE DE INVERSIONES FINANCIERAS	Contratado
	ÓRGANO DE CONTROL INSTITUCIONAL		
102	[illegible]	[illegible]	Permanente
103	INGUA CECERRA ROCIO	AUDITOR	Permanente
104	EDQUEN CABANILLAS CLAUDIA VANESSA	AUDITOR	Permanente
105	ZUÑIGA TAPIA HANS	AUDITOR	Permanente
106	MONTOYA FERNANDEZ SANDRA ISABEL	AUDITOR	Contratado
107	CASTRO HUERTAS LILLEN PATRICIA	AUDITOR	Contratado
108	ASCUE PINEDO ANTHONY BRAYAN	AUDITOR	Contratado
	GERENCIA DE RIESGOS Y DESARROLLO		
109	[illegible]	[illegible]	Permanente
110	RAMIREZ CABALLERO MARTHA ROSARIO	ASISTENTE DE GERENCIA	
	Dpto. de Evaluación y Riesgos		
111	ARCE RAMIREZ OSCAR FÉLIX	ESPECIALISTA EN RIESGOS OPERATIVOS	Permanente
112	MERINO CARRATAL BALDEMARO FERNANDO	JEFE DEL DPTO. DE EVALUACIÓN DE RIESGOS	Permanente
113	ASTUHUAMAN JENNIFER CARINA	ASISTENTE DE EVALUACIÓN DE RIESGOS	Contratado
	Dpto. de Planeamiento y Organización		
114	SANTALLA HUERTA CARMEN EDITH	JEFE DEL DPTO. DE PLANEAMIENTO Y ORGANIZACIÓN	Permanente
115	[illegible]	ASISTENTE EN ORGANIZACIÓN Y MÉTODOS	Permanente
116	MEZARINA MUÑOZ JIMENA	ASISTENTE EN ORGANIZACIÓN Y MÉTODOS	Contratado

UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC
FACULTAD DE ADMINISTRACIÓN
ESCUELA ACADÉMICO PROFESIONAL DE ADMINISTRACIÓN

Sr. (Sra.) trabajador de la Caja de Pensiones Militar Policial, esperamos su colaboración, respondiendo con sinceridad la presente encuesta.

El objetivo de la presente encuesta es determinar el grado de relación entre el riesgo operacional y el nivel de gestión de la Caja de Pensiones Militar Policial.

Instrucciones: Lea con atención y conteste a las preguntas marcando con "X" en una sola alternativa.

1. ¿Las actividades que Ud. realiza en el cargo en el que se desempeña son autorizadas y/o supervisadas por su jefe inmediato?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

2. ¿En el ejercicio de sus funciones ha podido detectar la presentación de documentos presuntamente falsos por miembros de la entidad?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

3. ¿Ud. ha podido encontrar posibles documentos falsos presentados por personas ajenas a la entidad?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

4. ¿En el desempeño de sus funciones se ha visto afectado por ataques informáticos y/o robo de información?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

5. ¿En el área donde labora, las relaciones laborales son las adecuadas para garantizar el normal desarrollo de sus funciones?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

6. ¿En el área donde laboral existentes condiciones óptimas remunerativas y contractuales para el desempeño de sus funciones?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

7. ¿En el área donde labora se evidencian actos de discriminación e intolerancia a la diversidad?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

8. ¿Al brindar información al usuario (interno/externo) comete actos de violación de privacidad, confusión de cuentas y/o uso de información confidencial?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

9. ¿Las personas que le solicitan información se identifican correctamente o portan la debida autorización para hacer consultas?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

10. ¿En el desempeño de sus funciones, se ha paralizado las actividades debido a fallas en los sistemas informáticos, telecomunicaciones y/o incidentes en suministros causados por factores externos?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

11. ¿En la ejecución de funciones, Ud. ha cometido errores de introducción de datos y/o, incumplimiento de plazos y/o responsabilidades?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

12. ¿En el proceso de brindar información (cliente interno/cliente externo) se ha brindado información inexacta y/o se ha incumplido con esta obligación?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

13. ¿En la ejecución de procesos, ha tenido acceso no autorizado a cuentas, registros de clientes y/o información confidencial?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

14. ¿La estructura organizativa de la Caja de Pensiones Militar Policial permite una adecuada gestión y cumplimiento de la misión organizacional?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

15. ¿Cuenta con manuales de procedimientos de las actividades que desarrolla en la unidad donde labora?
   A. Muy frecuentemente
   B. Frecuentemente
   C. Ocasionalmente
   D. Casi nunca
   E. Nunca

16. ¿Tiene acceso a los documentos de gestión (MOF, Plan Estratégico, etc.) de la entidad?
    A. Muy frecuentemente
    B. Frecuentemente
    C. Ocasionalmente
    D. Casi nunca
    E. Nunca

17. ¿Ud. ha revisado los documentos de gestión (MOF, Plan Estratégico, etc.) de la entidad?
    A. Muy frecuentemente
    B. Frecuentemente
    C. Ocasionalmente
    D. Casi nunca
    E. Nunca

18. ¿La entidad realiza actividades de autoevaluación de la gestión institucional?
    A. Muy frecuentemente
    B. Frecuentemente
    C. Ocasionalmente
    D. Casi nunca
    E. Nunca

19. ¿El área donde se desempeña cuenta con su propia base de datos?
    A. Muy frecuentemente
    B. Frecuentemente
    C. Ocasionalmente
    D. Casi nunca
    E. Nunca

20. ¿La entidad cuenta con reportes de información emitida y recibida sobre riesgo operacional?
    A. Muy frecuentemente
    B. Frecuentemente
    C. Ocasionalmente
    D. Casi nunca
    E. Nunca

Agradecemos su colaboración.