Firmado digitalmente por: MEDINA PALOMINO Ricardo Eliseo FAU 20108068281 soft
Motivo: Doy V° B°
Fecha: 06/02/2025 13:08:36-0500

Firmado digitalmente por: ZAVALA MORA Clara Maria FAU 20108068281 hard
Motivo: Doy V° B°
Fecha: 06/02/2025 10:02:47-0500

DIRECTIVA DE CONSEJO DIRECTIVO

POLÍTICA DE GESTIÓN DE RIESGO OPERACIONAL

DCD Nº 01-2025

San Isidro, 30/01/2025

1. FINALIDAD

Definir los lineamientos para identificar, medir, controlar y reportar el riesgo operacional al que está expuesta la Caja de Pensiones Militar Policial (CPMP).

2. REFERENCIA LEGAL Y NORMATIVA

- Decreto Ley Nº 21021 – Ley de Creación de la Caja de Pensiones Militar-Policial y sus modificatorias
- Decreto Supremo Nº 005-75-CCFA – Reglamento del Decreto Ley Nº 21021 y sus modificatorias
- Decreto Ley Nº 19846 – Ley de Pensiones Militar Policial y sus modificatorias
- Decreto Supremo Nº 009-DE-CCFA – Reglamento de la Ley de Pensiones Militar Policial
- Decreto Legislativo Nº 1133 – Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial, y sus modificatorias
- Decreto Supremo Nº 101-2021-EF – Normas Reglamentarias y Complementarias del Decreto Legislativo Nº 1133, Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial, y sus modificatorias
- Ley Nº 26516 – Incorporan al control y supervisión de la SBS las derramas, cajas de beneficios y otros fondos que reciban recursos de sus afiliados y otorguen pensiones de cesantía, jubilación y similares, y sus modificatorias
- Ley Nº 26702 – Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y sus modificatorias
- Decreto Supremo Nº 054-97-EF – Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones y sus modificatorias
- Decreto Supremo Nº 004-98-EF – Reglamento del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones y sus modificatorias
- Resolución SBS Nº 2116-2009 – Reglamento para la Gestión de Riesgo Operacional y sus modificatorias

Firmado digitalmente por: SANTALLA HUERTA Carmen Edith FAU 20108068281 hard
Motivo: Doy V° B°
Fecha: 05/02/2025 12:22:52-0500

Firmado digitalmente por: RODRIGUEZ MARQUINA Fernando Sergio FAU 20108068281 hard
Motivo: Doy V° B°
Fecha: 05/02/2025 12:55:46-0500

Firmado digitalmente por: RIVERA PEREZ Juan Carlos FAU 20108068281 soft
Motivo: Doy V° B°
Fecha: 05/02/2025 13:44:03-0500

- Resolución SBS Nº 272-2017 – Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, y sus modificatorias
- Resolución SBS Nº 877-2020 – Reglamento para la Gestión de la Continuidad del Negocio y sus modificatorias
- Resolución SBS Nº 504-2021 – Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, y sus modificatorias
- Circular SBS Nº G-165-2012 – Informe de riesgos por nuevos productos o cambios importantes en el ambiente de negocios, operativo o informático, y sus modificatorias
- Circular SBS Nº G-191-2017– Criterios para el registro de eventos de pérdida por riesgo operacional
- Circular SBS Nº G-213-2021 – Establecen disposiciones respecto a la operatividad e información del aplicativo "Registro de Accionistas, Directores, Gerentes y Principales Funcionarios" – REDIR
- Lineamientos para la categorización y registro de los eventos de pérdida por riesgo operacional de la SBS
- Manual de Organización y Funciones de la Caja de Pensiones Militar Policial
- Directiva de Consejo Directivo Nº 13-2021 – Reglamento Interno de Consejo Directivo
- Directiva de Consejo Directivo Nº 14-2024 – Reglamento de Comité de Riesgos
- Directiva de Consejo Directivo Nº 02-2025 – Manual de Gestión de Riesgo Operacional

3. ALCANCE

Los lineamientos contenidos en la presente política se aplican en todas las unidades orgánicas de la CPMP.

4. GLOSARIO

4.1. Apetito por el riesgo: Nivel de riesgo que la empresa está dispuesta a asumir dentro de su capacidad de riesgo, para alcanzar sus objetivos.

4.2. Cambios importantes en el ambiente de negocio, operativo o informático: Modificaciones en los procesos y/o sistemas que afecten significativamente el nivel de riesgo de la CPMP.

4.3. Capacidad de riesgo: Nivel máximo de riesgo que puede asumir una empresa dados sus recursos actuales, requerimientos regulatorios y obligaciones contractuales.

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

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

4.6. 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.

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

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

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

4.10. Fraude interno: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad y discriminación) en las que se encuentra implicado, al menos, un miembro de la empresa.

4.11. Gestión de riesgos: Proceso que consiste en identificar, evaluar, tratar, reportar y monitorear los riesgos que la empresa enfrenta.

4.12. Gestor de riesgo operacional: Colaborador encargado de gestionar, al interior de cada unidad orgánica, las acciones relacionadas con la gestión de riesgo operacional, de acuerdo a lo estipulado en el presente documento. Para ello, debe tener condición de nombrado, con categoría de subgerente o jefe de departamento, o, en caso de ausencia, quien haga sus veces mediante encargatura asignada y aprobada.

4.13. Interrupción del negocio y fallos en los sistemas: Interrupción del negocio y fallos en los sistemas.

4.14. Límites de riesgo: Nivel máximo de riesgo, en función al apetito, expresado preferentemente en medidas cuantitativas por líneas de negocio, tipos de riesgo, concentraciones, u otros apropiados a la complejidad de las operaciones y servicios de la empresa y el sector al que pertenece.

4.15. Nuevo producto: Producto lanzado por primera vez por la empresa o cuando se realiza un cambio en un producto existente que modifica su perfil de riesgo.

4.16. Pérdida: Impacto negativo en los resultados de la entidad.

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

4.18. Riesgo: Posibilidad de ocurrencia de un evento que impacte negativamente a los objetivos de la CPMP.

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

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

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

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

5. LINEAMIENTOS GENERALES

5.1. Establecer una estructura organizativa conformada por el Consejo Directivo, la Gerencia General, la Unidad de Auditoría Interna, las gerencias, los gestores de riesgos operacionales y los trabajadores, con la finalidad de que la gestión de riesgo operacional se realice con líneas muy definidas de responsabilidad, evaluación y reporte.

5.2. Establecer una cultura organizacional que promueva prácticas adecuadas de gestión de riesgos, las cuales para ser efectivas deben formar parte integral de las actividades regulares de la CPMP.

5.3. Contar con la metodología de evaluación de riesgos operacionales adecuada a la naturaleza y complejidad de la CPMP, que permita identificar y mitigar los riesgos operacionales que generan los siguientes tipos de eventos: “fraude interno”, “fraude externo”, “relaciones laborales y seguridad en el puesto de trabajo,” “clientes, productos y prácticas empresariales”, “daños a activos materiales”, “interrupción del negocio y fallos en los sistemas” y “ejecución, entrega y gestión de procesos”.

5.4. Contar con una metodología de evaluación del diseño de control.

5.5. Contar con una metodología para indicadores claves de riesgo.

5.6. Contar con una base de datos para el registro de los eventos de pérdida por riesgo operacional.

5.7. Contar con una metodología para la identificación evaluación de nuevos productos o cambios importantes y subcontrataciones significativas.

5.8. Contar con una metodología para la evaluación del desempeño de los gestores para la aplicación de incentivos.

5.9. La CPMP debe contar con procesos y directivas actualizadas para que puedan ser utilizados en la evaluación de riesgos operacionales.

5.10. Contar con un sistema de gestión de seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de su información.

5.11. Contar con un sistema de gestión de continuidad del negocio.

5.12. La CPMP debe contar con un sistema de información y reporte oportuno de riesgos operacionales para la toma de decisiones de las unidades orgánicas competentes.

5.13. Ejecutar programas de capacitación sobre mecanismos de administración del riesgo operacional, con el objetivo de asegurar que el personal cuente con las habilidades y experiencia apropiadas y optimizar las actividades de gestión de riesgo operacional de la organización.

5.14. Los lineamientos establecidos en el presente documento deben ser cumplidos por todas las unidades orgánicas involucradas de la organización, y cada nivel de administración es responsable por la idoneidad y efectividad de estos dentro de su competencia.

5.15. Realizar reportes trimestrales al Comité de Riesgos sobre la gestión de riesgo operacional.

6. LINEAMIENTOS ESPECÍFICOS

6.1. Apetito de riesgo operacional

6.1.1. El apetito de riesgo operacional está compuesto por la capacidad de riesgo operacional, los límites de riesgo operacional y el apetito por riesgo operacional.

6.1.2. La capacidad de riesgo operacional debe ser estimada considerando como referencia la fórmula establecida por la SBS para el cálculo del requerimiento patrimonial por riesgo operacional (método básico).

6.1.3. Los límites de riesgo operacional deben ser calculados en función a la capacidad y a la información histórica de eventos de pérdida de la CPMP.

6.1.4. Los resultados del cálculo de la capacidad, límites y apetito por riesgo operacional deben ser reportados por la Gerencia de Riesgos y Desarrollo al Comité de Riesgos, a través de un informe.

6.1.5. La metodología señalada en los puntos anteriores se desarrolla en la directiva "Manual de Gestión de Riesgo Operacional" de la CPMP.

6.2. Autoevaluación de riesgos y controles

6.2.1. La CPMP debe contar con una base de riesgos, en función a la identificación de los riesgos operacionales de cada proceso.

6.2.2. El Departamento de Riesgos Operacionales, en coordinación con los gestores de riesgo operacional, debe desarrollar los talleres de autoevaluación para cada uno de los procesos de la CPMP. La revisión de cada proceso debe realizarse con una periodicidad anual.

6.2.3. Cada proceso debe contar con una matriz de riesgos y controles para asegurar su alineación con el apetito al riesgo.

6.2.4. El Departamento de Riesgos Operacionales debe verificar la efectividad de los controles.

6.2.5. Los procesos o sus modificaciones en el ambiente operativo y tecnológico, que requieran ser implementados, deben ser evaluados utilizando la metodología establecida para las autoevaluaciones de riesgos y sus resultados deben ser informados en Comité de Riesgos.

6.3. Base de datos y eventos de pérdida

6.3.1. La CPMP debe contar con una base de datos de eventos de pérdida por riesgo operacional, administrada por la Gerencia de Riesgos y Desarrollo, en donde se registren todos los eventos de pérdida originados en la CPMP.

6.3.2. Los eventos de pérdida mayores al umbral definido, según el apetito de riesgos, deben contar con un informe y planes de acción, en caso el nivel del riesgo operacional asociado lo requiera.

6.3.3. Todos los eventos de riesgo operacional deben ser reportados y registrados de acuerdo a los procedimientos establecidos en la directiva "Manual de Gestión de Riesgo Operacional" de la CPMP.

6.4. Nuevos productos y cambios importantes

6.4.1. Realizar la identificación y evaluación de riesgos del nuevo producto o cambio importante. Los resultados de dicha evaluación y los planes de acción definidos deben ser presentados al Comité de Riesgos.

6.4.2. La CPMP debe presentar a la Superintendencia de Banca, Seguros y AFP (SBS), copia de los informes de riesgos por nuevos productos a los diez (10) días hábiles siguientes a su lanzamiento y para cambios importantes en el ambiente de negocios, operativo o informático, dentro de los diez (10) días hábiles de presentados al Comité de Riesgos.

6.5. Subcontratación significativa

6.5.1. Realizar la evaluación de riesgos de la subcontratación significativa. Los resultados de dicha evaluación y los planes de acción definidos deben ser presentados al Comité de Riesgos.

6.5.2. Se debe gestionar los riesgos asociados a la subcontratación significativa, considerando la normativa interna relacionada a la evaluación de proveedores, mecanismos de subcontratación y procedimientos del nivel de prestación de servicio.

6.5.3. Cuando se realice un proceso a través de servicios por terceros, los contratos que se firmen con el proveedor del servicio deben ser precisos con la finalidad de que garanticen una clara asignación de responsabilidades, debiendo establecer cláusulas de riesgo operacional en dichos contratos y en los casos que corresponda.

6.6. Indicador clave de riesgo

6.6.1. Cuando se identifique un riesgo inherente con nivel de exposición alto y extremo, así como otras consideraciones precisadas en la directiva "Manual de Gestión de Riesgo Operacional" de la CPMP, dentro del proceso de autoevaluación de riesgos y controles, se debe definir, e implementar un indicador clave de riesgo, que debe ser monitoreado por un periodo de seis (6) meses, periodo que puede ser extendido en caso sea necesario.

6.6.2. Establecer procedimientos para definir, implementar, registrar, reportar y monitorear los indicadores clave de riesgos.

6.6.3. Definir planes de acción para los indicadores que no cumplen con el umbral establecido.

6.7. Sistema de incentivos

6.7.1. La CPMP debe contar con un sistema de incentivos para fortalecer la gestión de riesgo operacional.

6.7.2. La evaluación del desempeño de los gestores de riesgo operacional se realiza una (1) vez al año por el Departamento de Riesgos Operacionales, en coordinación con la Gerencia de Riesgos y Desarrollo. Los resultados son comunicados por el Departamento de Riesgos Operacionales al Departamento de Recursos Humanos.

6.7.3. Los incentivos son no monetarios: entrega de reconocimientos o premios, por haber realizado una gestión destacada durante el periodo de evaluación, lo cual está a cargo del Departamento de Recursos Humanos.

6.8. Requerimiento de información

6.8.1. La CPMP debe presentar a la SBS, informes anuales referidos a la gestión de riesgo operacional, a través del *software* IG-ROp del Portal del Supervisado, dentro del plazo establecido por la SBS.

6.8.2. La CPMP debe designar un funcionario responsable por la información a ser reportada a través del IG-ROp del portal supervisado por la SBS. El funcionario responsable debe corresponder al Gerente de Riesgos y Desarrollo o al funcionario principal, según las disposiciones de la Circular SBS Nº G-213-2021.

6.8.3. La CPMP debe tener a disposición de la SBS, toda la información de sustento de la gestión de riesgo operacional.

6.8.4. El Comité de Riesgos informa al Consejo Directivo sobre la exposición al riesgo operacional de la CPMP, en los informes periódicos que presenta a esa instancia.

6.8.5. Responsabilidad

6.8.5.1 Del Consejo Directivo

a) Aprobar la política general que guíe las actividades de la CPMP en la gestión de sus riesgos operacionales.

b) Asignar los recursos necesarios para la gestión de riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiado.

c) Establecer un sistema de incentivos que fomente la gestión de riesgo operacional y que favorezca la toma apropiada de riesgos.

d) Aprobar el apetito de riesgo operacional de la CPMP.

e) Aprobar la directiva "Manual de Gestión de Riesgo Operacional" de la CPMP, y sus modificaciones.

f) Conocer los principales riesgos operacionales afrontados por la CPMP.

g) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.

h) Tener la seguridad razonable de que la CPMP cuente con una gestión de riesgo operacional, y que los principales riesgos identificados se encuentran bajo control, dentro de los límites establecidos.

6.8.5.2 Del Comité de Riesgos

a) Proponer al Consejo Directivo las políticas y la organización para la gestión de riesgo operacional, así como las modificaciones que se realicen a los mismos.

b) Proponer al Consejo Directivo la capacidad, el apetito y los límites de riesgo operacional que la CPMP esté dispuesta a asumir en el desarrollo del negocio.

c) Aprobar los informes sobre los riesgos asociados a nuevos productos y las medidas de tratamiento propuestas o implementadas, de forma previa a su lanzamiento.

d) Aprobar los informes sobre los riesgos asociados a los cambios importantes en el ambiente de negocios, operativo o informático, de forma previa a su ejecución, así como de las medidas de tratamiento propuestas o implementadas.

e) Informar al Consejo Directivo sobre el nivel de exposición al riesgo operacional, de acuerdo a la información remitida por la Gerencia de Riesgos y Desarrollo.

f) Proponer mejoras en la gestión de riesgo operacional.

6.8.5.3 De la Gerencia General

a) Implementar la gestión de riesgo operacional conforme a las disposiciones del Consejo Directivo.

b) Informar al Consejo Directivo respecto a nuevos productos y, en general, sobre iniciativas gerenciales relevantes (cambios de sistemas, procesos, modelos de negocios, inversiones sustanciales, entre otros), que puedan tener un impacto material en el perfil de riesgo operacional de la entidad.

c) Impulsar la comunicación sobre la gestión de riesgos operacionales en toda la CPMP.

d) Velar por el cumplimiento de las políticas relacionadas a la gestión de riesgo operacional, conforme a las disposiciones del Consejo Directivo.

6.8.5.4 De las unidades orgánicas

a) Gestionar y administrar el riesgo operacional relacionado al logro de los objetivos de sus respectivas unidades.

b) Asegurar que los roles y responsabilidades que estén relacionados a la gestión de riesgo operacional sean definidos y difundidos claramente en la gerencia.

c) Definir planes de acción para tratar el riesgo operacional en caso se considere necesario.

d) Las subgerencias, gerencias y departamentos son responsables de la implementación de los cambios importantes en el ambiente operativo y tecnológico, y de la subcontratación significativa de servicios externos. Por lo tanto, deben mantener una comunicación efectiva con el Departamento de Riesgos Operacionales, en forma previa, y durante los procesos de contratación y ejecución, para gestionar los riesgos operacionales asociados.

e) Asumir, ante el Gerente General, los resultados de la gestión de riesgo operacional correspondiente a su unidad.

6.8.5.5 De la Gerencia de Riesgos y Desarrollo

a) Velar por una adecuada gestión de riesgo operacional, al promover el alineamiento de la toma de decisiones de la entidad con el apetito de riesgo operacional.

b) Verificar periódicamente que las políticas y procedimientos establecidos para la gestión de riesgo operacional estén definidos en los manuales correspondientes, y que sean consistentes con el tamaño y la complejidad de las operaciones de la CPMP.

c) Verificar periódicamente que los procesos y directivas de la CPMP se encuentren actualizados, para que puedan ser utilizados como insumos en la evaluación de riesgos operacionales.

d) Informar a la Gerencia General respecto a nuevos productos y, en general, sobre iniciativas gerenciales relevantes (cambios de sistemas, procesos, modelos de negocios, inversiones sustanciales, entre otros), que puedan tener un impacto material en el perfil de riesgo operacional de la entidad.

e) Velar por una adecuada comunicación sobre la gestión de riesgos operacionales en toda la CPMP.

f) Informar a la Gerencia General el cumplimiento de las políticas relacionadas a la gestión de riesgo operacional

g) Informar trimestralmente al Comité de Riesgos, según sea el caso, los aspectos relevantes de la gestión de riesgos para una oportuna toma de decisiones.

h) Informar al Comité de Riesgos acerca de los riesgos asociados al lanzamiento de nuevos productos, y a los cambios importantes en el ambiente de negocios, el ambiente operativo o informático, de forma previa a su lanzamiento o ejecución, así como de las medidas de tratamiento propuestas o implementadas.

6.8.5.6 Del Departamento de Riesgos Operacionales

a) Proponer y elaborar las políticas, procedimientos y metodologías apropiadas para la gestión de riesgo operacional.

b) Participar en el diseño y permanente actualización de la directiva "Manual de Gestión de Riesgo Operacional" de la CPMP.

c) Desarrollar la metodología para la gestión de riesgo operacional.

d) Apoyar y asistir a las demás unidades orgánicas para la aplicación de la metodología de gestión de riesgo operacional, al promover el alineamiento de las medidas de tratamiento de los riesgos operacionales con los niveles de apetito y tolerancia aprobadas por el Consejo Directivo.

e) Velar por el cumplimiento de las funciones y responsabilidades asignadas a los gestores de riesgo operacional, gerentes y personal de la CPMP, en relación a la gestión de riesgo operacional.

f) Identificar las necesidades de capacitación y difusión para una adecuada gestión de riesgo operacional por parte de los gestores de riesgo operacional.

g) Administrar la cartera de riesgos operacionales y la base de datos de eventos de pérdida por riesgo operacional.

h) Informar a la Gerencia de Riesgos y Desarrollo, los aspectos relevantes de la gestión de riesgos operacionales para una oportuna toma de decisiones.

i) Elaborar y enviar a través de la extranet de la SBS, el informe electrónico anual (a través del aplicativo IG-ROp) de la gestión de riesgo operacional dentro de los plazos establecidos (a más tardar el 31 de marzo del año siguiente al año del reporte, según Resolución SBS Nº 877-2020), previa aprobación de la Gerencia de Riesgos y Desarrollo.

j) Evaluar los riesgos operacionales asociados a cambios importantes en el ambiente de negocio, operativo o informático, y asociados al lanzamiento de nuevos productos, al cubrir las diferentes etapas de su desarrollo,

desde la concepción de la idea hasta culminar su implementación, sobre la base de lo reportado por el gestor de riesgo operacional.

6.8.5.7 De los gestores de riesgo operacional

a) Participar en la evaluación de los riesgos operacionales y aportar experiencia y conocimiento sobre el proceso que lidera en la valoración de impacto y frecuencia de los riesgos.

b) Definir planes de acción para mitigar los riesgos operacionales identificados, realizar el seguimiento mensual del avance de los planes y reportarlos al Departamento de Riesgos Operacionales.

c) Participar en los programas de capacitación desarrollados por la Gerencia de Riesgos y Desarrollo.

d) Comunicar las iniciativas de nuevos productos, nuevos servicios o cambios importantes en el ambiente operativo e informático, a ser desarrollados en los procesos bajo su responsabilidad, antes de su implementación. Así como enviar la información requerida por el Departamento de Riesgos Operacionales.

e) Enviar documentos de sustento sobre los servicios a contratar y verificar que se incluyan cláusulas de riesgo operacional en los contratos, según corresponda.

f) Definir indicadores clave de riesgo con el apoyo del Departamento de Riesgos Operacionales y reportarlos de forma periódica.

6.8.5.8 De todo el personal

a) Todos los trabajadores y funcionarios de la CPMP son responsables de la gestión de riesgo operacional dentro de las funciones que realizan como parte de sus labores habituales.

b) Informar a los gestores de riesgo operacional, la existencia de cualquier evento que signifique un riesgo operacional, a través de los mecanismos establecidos y de cumplir con las políticas y procedimientos que se establecen en el presente manual.

c) Participar en los programas de capacitación desarrollados por la Gerencia de Riesgos y Desarrollo.

CAJA DE PENSIONES MILITAR POLICIAL