Firmado digitalmente por:
ZAVALA MORA Clara Maria
FAU 20108068281 hard
Motivo: Doy V° B°
Fecha: 06/02/2025 10:04:43-0500

Firmado digitalmente por:
MEDINA PALOMINO Ricardo
Eliseo FAU 20108068281 soft
Motivo: Doy V° B°
Fecha: 06/02/2025 13:10:05-0500

## Caja de Pensiones Militar Policial

### Directiva de Consejo Directivo

### DCD Nº 02-2025

# MANUAL DE GESTIÓN DE RIESGO OPERACIONAL

**APROBADO MEDIANTE EL ACUERDO DEL CONSEJO DIRECTIVO N° 02-02-2025**
**ADOPTADO EL 30.01.2025**

**(Deja sin vigencia el manual aprobado con el Acuerdo del Consejo Directivo Nº 04-18-2023)**

Firmado digitalmente por:
SANTALLA HUERTA Carmen
Edith FAU 20108068281 hard
Motivo: Doy V° B°
Fecha: 05/02/2025 12:23:19-0500

Firmado digitalmente por:
RODRIGUEZ MARQUINA
Fernando Sergio FAU 20108068281
hard
Motivo: Doy V° B°
Fecha: 05/02/2025 13:00:01-0500

Firmado digitalmente por:
RIVERA PEREZ Juan Carlos
FAU 20108068281 soft
Motivo: Doy V° B°
Fecha: 05/02/2025 13:42:10-0500

**ÍNDICE**

# CAPÍTULO I: GENERALIDADES

## 1. OBJETIVO

Establecer los procedimientos para identificar, medir, controlar y reportar el riesgo operacional al que está expuesta la Caja de Pensiones Militar Policial (CPMP), dentro del marco del Sistema de Gestión Integral de Riesgos.

## 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 de la Ley de Creación de la Caja de Pensiones Militar Policial 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 26702 – Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros 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
- Resolución SBS Nº 2116-2009 – Reglamento para la Gestión de Riesgo Operacional y sus modificatorias
- 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
- 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 Normas para el 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 01-2025 – Política de Gestión de Riesgo Operacional.

## 3. ALCANCE

El presente documento se aplica en todas las unidades orgánicas de la CPMP.

## 4. GLOSARIO

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

**4.2.** Aceptación de riesgo: Es una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

**4.3.** Cambios importantes en el ambiente de negocio, operativo o informático: Son las modificaciones en los procesos y/o sistemas que afecten significativamente el nivel de riesgo de la CPMP.

**4.4.** Capacidad de riesgo: Es el nivel máximo de riesgo que puede asumir una empresa dados sus recursos actuales, requerimientos regulatorios y obligaciones contractuales

**4.5.** Evento: Es un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

**4.6.** Evento de pérdida por riesgo operacional: Es el evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.

**4.7.** Frecuencia anual: Es el número de sucesos de riesgo que se producen anualmente. Con el objetivo de facilitar la medición de la frecuencia, éste debe calcularse en función al número de sucesos y periodicidad.

**4.8.** Gestión de riesgos: Es el proceso que consiste en identificar, evaluar, tratar, reportar y monitorear los riesgos que la empresa enfrenta.

**4.9.** Gestor de riesgo operacional: Es el trabajador 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. Y para tal fin, debe tener condición de nombrado con categoría de subgerente o jefe de departamento, y en caso de ausencia, quien haga sus veces mediante encargatura asignada y aprobada.

**4.10.** Información: Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

**4.11.** Impacto medio inherente: Es el importe promedio de cada uno de los sucesos de riesgos que pueden producirse en el futuro con un horizonte de un año. Dependiendo de la casuística a evaluar, podrían presentarse casos en los cuales se mida respecto al importe más alto del posible suceso.

**4.12.** Límites de riesgo: Es el 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.

**4.13.** 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.

**4.14.** Número de sucesos: Es el número de veces que se estima que la ocurrencia del evento producirá pérdidas operacionales directas en un periodo de tiempo concreto.

**4.15.** Pérdida: Es un impacto negativo en los resultados de la entidad.

**4.16.** Periodicidad: Es el horizonte temporal al que hace referencia el número de sucesos (diario, semanal, mensual, trimestral, semestral, anual, década, siglo).

**4.17.** Riesgo: Es la posibilidad de ocurrencia de un evento que impacte negativamente a los objetivos de la CPMP.

**4.18.** Riesgo legal: Es la 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.

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

**4.20.** Servicios significativos: Los servicios significativos provistos por terceros son aquellos que, en caso de falla o suspensión, pueden poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, continuidad operativa o reputación. En caso de que algún bien y/o servicio significativo sea provisto por un tercero bajo la modalidad de subcontratación, la subcontratación se considera significativa.

**4.21.** Subcontratación: Es la 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: Es 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.

# CAPÍTULO II: METODOLOGÍA

## 1. GENERALIDADES

**1.1.** La metodología de administración de riesgos operacionales que la CPMP emplea ha tomado como referencia las recomendaciones y principios básicos contenidos en la ISO 31000 *Risk Management*, el Acuerdo de Capital – Basilea III y las normativas de la SBS.

**1.2.** Los factores que originan el riesgo operacional son:

**1.2.1.** Procesos internos: Es el factor que origina riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de estos.

**1.2.2.** Persona: Es el factor que origina riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros.

**1.2.3.** Tecnología de información: Es el factor que origina riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de estos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

**1.2.4.** Eventos externos: Es el factor que origina riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

**1.3.** Los tipos de eventos de pérdida por riesgo operacional son:

**1.3.1.** Fraude interno: Son las 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 implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.

**1.3.2.** Fraude externo: Son las pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

**1.3.3.** Relaciones laborales y seguridad en el puesto de trabajo: Son las pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

**1.3.4.** Clientes, productos y prácticas empresariales: Son las 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.

**1.3.5.** Daños a activos materiales: Son las pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

**1.3.6.** Interrupción del negocio y fallos en los sistemas: Son las pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

**1.3.7.** Ejecución, entrega y gestión de procesos: Son 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.

## 2. APETITO DE RIESGO OPERACIONAL

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

**2.2.** La capacidad de riesgo operacional, es estimada considerando como referencia la fórmula establecida por la SBS para el cálculo del requerimiento patrimonial por riesgo operacional (método básico), el cual es equivalente al promedio de los saldos anualizados de los márgenes operacionales brutos de la empresa, considerando los últimos tres (3) años, multiplicado por un factor fijo (15%). Si el margen operacional bruto correspondiente a alguno de los tres (3) últimos años es cero (0) o es un número negativo, dichos años no deben ser considerados en el cálculo del promedio, en cuyo caso se calcula sobre la base del número de años cuyo margen operacional bruto sea positivo [1].

[1] Resolución S.B.S Nº 2115-2009 – Reglamento para el requerimiento de patrimonio efectivo por riesgo Operacional

**2.3.** Para el Régimen Decreto Ley Nº 19846, se considera como supuesto que la CPMP recibe como ingreso el 3% de los aportes.

**2.4.** El apetito de riesgo operacional es el nivel de riesgo que la CPMP está dispuesta a asumir para alcanzar sus objetivos.

**2.5.** La capacidad y el nivel de apetito por riesgo operacional es calculado por cada una de las líneas de negocio definidas por la CPMP para los regímenes del Decreto Ley Nº 19846 y Decreto Legislativo Nº 1133.

**2.6.** Los límites de riesgo operacional son calculados en función a la capacidad y a la información histórica de eventos de pérdida de la CPMP. Los resultados del cálculo de la capacidad, límites y apetito por riesgo operacional son reportados por la Gerencia de Riesgos y Desarrollo a través de un informe.

**2.7.** La Gerencia de Riesgos y Desarrollo actualiza el apetito de riesgo operacional e informa los resultados al Comité de Riesgos.

# 3. AUTOEVALUACIÓN DE RIESGOS Y CONTROLES

La metodología de autoevaluación de riesgos operacionales, que se realiza con el apoyo del Departamento de Riesgos Operacionales, comprende las siguientes etapas:

### 3.1. Establecimiento del contexto

En esta etapa se establece el contexto estratégico, organizacional y de administración del riesgo en el cual el resto del proceso toma lugar. En primer término, se establece y explica a los gestores de riesgo operacional, los criterios sobre los cuales se evalúan los riesgos.

### 3.2. Entendimiento del proceso

**3.2.1.** Se revisa el proceso, actividad o sistema en el cual se realiza la evaluación de riesgos operativos, con la finalidad de conocer sus objetivos y metas.

**3.2.2.** En esta etapa se identifica la siguiente información:

**3.2.2.1.** Objetivos del proceso.

**3.2.2.2.** Sistemas que soportan el proceso.

**3.2.2.3.** Personal involucrado.

**3.2.2.4.** Documentación interna.

**3.2.2.5.** Documentación externa.

### 3.3. Identificación de riesgos

**3.3.1.** La identificación de los riegos operacionales inicia con el cuestionamiento de lo que puede fallar a causa de los procesos internos, de la tecnología de la información, por eventos externos o por las personas que ejecutan una actividad y cuáles son las consecuencias de la falla.

**3.3.2.** Las fuentes de información para la identificación de riesgos incluyen:

**3.3.2.1.** Revisiones de terceros (auditoría interna y externa, consultorías, entre otros).

**3.3.2.2.** Análisis de datos.

**3.3.2.3.** Análisis de procesos internos.

**3.3.2.4.** Análisis de directivas internas.

**3.3.2.5.** Comparaciones de objetivos, metas y planes por unidades orgánicas.

**3.3.2.6.** Análisis de cambios propuestos en los procesos, sistemas u organización.

**3.3.2.7.** Reportes o informes de avances en los proyectos.

**3.3.2.8.** Análisis de factores externos.

**3.3.2.9.** Base de datos de pérdidas.

**3.3.3.** En caso se identifique que los procesos y/o directivas no recogen las actividades que se realizan en la actualidad, según lo relevado por el gestor, se recomienda la actualización de dichos documentos.

### 3.4. Análisis de riesgos

Considera las fuentes de riesgos para determinar su frecuencia de ocurrencia e impacto de estas. Asimismo, el enfoque a utilizar es de tipo cuantitativo, con evaluaciones basadas en riesgo inherente, entorno de control y riesgo residual. Paralelamente, se realiza una evaluación cualitativa de impacto reputacional e impacto regulatorio.

### 3.4.1. Medición del riesgo inherente

Se mide el riesgo inherente como el cálculo de dos variables independientes:

| Riesgo Inherente = Frecuencia anual x Impacto Medio Inherente |
|---|

Así, el riesgo inherente se calcula como producto de la frecuencia anual (es decir, el número de casos ocurridos durante el año) por el impacto medio inherente.

### 3.4.2. Evaluación de controles

Si existe control, se identifica y evalúa los controles que ayudan a mitigar el riesgo, teniendo en cuenta si estos mitigan frecuencia o impacto.

**3.4.2.1.** Si el control mitiga frecuencia: Se evalúa la calificación del diseño.

**a)** Calificación del diseño y ejecución del control: Se realiza en base al cumplimiento de una serie de condiciones, para las cuales se han definido alternativas que tienen asignado un peso ponderado y su sumatoria es la calificación del diseño.

En la Tabla Nº 1 se presenta el formato para calificar el diseño del control y en la Tabla Nº 2 se presenta el formato para calificar la ejecución del control.

**Tabla Nº 1: Calificación del diseño de control**

| **Calificación del diseño de control** | | | |
|---|---|---|---|
| **Atributo** | **Opciones** | **¿El control puede ser automatizado?** | |
| | | **Sí** | **No** |
| Funcionalidad | Manual | **6 %** | **30 %** |
| | Semiautomático | **15 %** | **-** |
| | Automático | **30 %** | **-** |
| Persona que realiza el control | La misma persona encargada de la operación o proceso. | **0 %** | **0 %** |
| | Es una persona diferente, pero de la misma unidad orgánica | **2 %** | **2 %** |

| Calificación del diseño de control | | | |
|---|---|---|---|
| **Atributo** | **Opciones** | **¿El control puede ser automatizado?** | |
| | | **Sí** | **No** |
| | Es una persona de una unidad orgánica distinta | **8 %** | **8 %** |
| Alcance del control | Se revisa una muestra | **2 %** | **2 %** |
| | Se revisa todas las operaciones /transacciones / documentos | **6 %** | **6 %** |
| Documentación del control (directivas) | No documentado | **0 %** | **0 %** |
| | Documento interno del área (no oficial) | **2 %** | **2 %** |
| | Documento formal | **6 %** | **6 %** |
| Tipo | Detectivo | **4 %** | **4 %** |
| | Preventivo | **10 %** | **10 %** |
| Evidencia | No deja evidencia | **0 %** | **0 %** |
| | Deja evidencia | **18 %** | **18 %** |
| Frecuencia | El control no se ejecuta cada vez que se realiza la actividad de riesgo | **1 %** | **1 %** |
| | El control se ejecuta cada vez que se realiza la actividad de riesgo | **4 %** | **4 %** |
| Idoneidad técnica | Persona que realiza el control no es idónea | **0 %** | **0 %** |
| | Persona que realiza el control es idónea | **4 %** | **4 %** |
| Rotación de personal | Cantidad de veces que ha sido cubierta la posición en el año con personal nuevo: **Más de una (1)** vez | **0 %** | **0 %** |
| | Cantidad de veces que ha sido cubierta la posición en el año con personal nuevo: **una (1)** vez | **1 %** | **1 %** |
| | Cantidad de veces que ha sido cubierta la posición en el año con personal nuevo: **cero (0)** veces | **4 %** | **4 %** |
| **Total** | **90%** | | |

(*) Para cada condición se debe seleccionar una alternativa
(**) La máxima calificación del diseño es del 90%

En aquellos casos donde el riesgo tenga asociado más de un control para mitigar la frecuencia, se considera el promedio simple de dichos controles.

La sumatoria de la calificación del diseño del control más la calificación de la ejecución del control es lo que se entiende como el entorno de control de dicho riesgo.

| % de Entorno de Control para mitigar frecuencia = % Diseño del control |
|---|

El porcentaje que da como resultante final de la fórmula (entorno de control) es aquel que se aplica sobre la frecuencia declarada del riesgo inherente en la evaluación.

El control o la sumatoria de los controles para mitigar la frecuencia tendrá un valor máximo del 90%, dado que, por definición, un control no mitiga en un 100% el riesgo.

**3.4.2.2.** Si el control mitiga impacto: se evalúa el nivel de efectividad mitigante.

**a)** Efectividad mitigante: Para determinar la efectividad del mitigante se han establecido tres (3) niveles, según se muestra en la Tabla Nº 2, donde cada una de ellas tiene asignado un porcentaje ponderado.

Se debe seleccionar el nivel de efectividad que tiene el mitigador sobre el impacto inherente.

**Tabla Nº 2: Calificación de la ejecución de control**

| Nivel | Descripción | Efectividad |
|---|---|---|
| Bajo | Su grado de mitigación es menor al 40%. | **10 %** |
| Medio | Su grado de mitigación fluctúa entre el 40 y 60 %. | **50 %** |
| Alto | Su grado de mitigación es mayor al 60 % | **90 %** |

En aquellos casos donde el riesgo tenga asociado más de un mitigante para minimizar el impacto, se considera el promedio simple de dichos mitigantes.

| % de Entorno de Control para mitigar impacto = % de Efectividad del control |
|---|

El porcentaje que da como resultante final de la fórmula (entorno de control) es aquel que se aplica sobre el

impacto declarado del riesgo inherente en la evaluación.

El mitigante o la sumatoria de los mitigantes para minimizar el impacto tendrá un valor máximo del 90%, dado que, por definición, un control no mitiga en un 100% el riesgo.

Cada uno de los controles y/o mitigantes declarados son evaluados para determinar el grado de mitigación de los riesgos inherentes, lo que conforma el nivel de riesgo remanente, es decir, riesgo residual.

### 3.4.3. Medición del riesgo residual

Al igual que el riesgo inherente, el riesgo residual se calcula a partir de dos variables independientes: frecuencia anual e impacto medio residual.

| Riesgo residual = Frecuencia anual x Impacto medio residual |
|---|

Así, el riesgo residual se calcula como producto de la frecuencia anual (es decir, el número de casos ocurridos durante el año) por el impacto medio residual. Para el cálculo del riesgo residual, la utilización de datos históricos es un elemento relevante, pero no determinante, ya que el ejercicio de autoevaluación pretende identificar el riesgo futuro (en el próximo año) y, puede haber condicionantes que modifiquen las eventuales pérdidas de manera material.

## 3.5. Clasificación de los riesgos

Los riesgos se han clasificado en cuatro (4) niveles, y se definen por línea de negocio en las siguientes tablas:

**Tabla Nº 3: Clasificación de riesgos – Previsional D. L. Nº 19846**

| NIVEL RIESGO | Rango de exposición a riesgos (Nuevos Soles) |
|---|---|
| EXTREMO | Mayor a 67,000 |
| ALTO | <49,000; 67,000] |
| MODERADO | <14,000; 49,000] |
| BAJO | <0; 14,000] |

**Tabla Nº 4: Clasificación de riesgos – G. Inmobiliaria D. L. Nº 19846**

| NIVEL RIESGO | Rango de exposición a riesgos (Nuevos Soles) |
|---|---|
| EXTREMO | Mayor a 60,950 |
| ALTO | <44,570; 60,950] |
| MODERADO | <12,740; 44,570] |
| BAJO | <0; 12,740] |

**Tabla Nº 5: Clasificación de riesgos – Inversiones D. L. Nº 19846**

| NIVEL RIESGO | Rango de exposición a riesgos (Nuevos Soles) |
|---|---|
| EXTREMO | Mayor a 68,580 |
| ALTO | <50,150; 68,580] |
| MODERADO | <14,330; 50,150] |
| BAJO | <0; 14,330] |

**Tabla Nº 6: Clasificación de riesgos – Descuentos a Pensionistas D. L. Nº 19846**

| NIVEL RIESGO | Rango de exposición a riesgos (Nuevos Soles) |
|---|---|
| EXTREMO | Mayor a 12,240 |
| ALTO | <8,950; 12,240] |
| MODERADO | <2,560; 8,950] |
| BAJO | <0; 2,560] |

**Tabla Nº 7: Clasificación de riesgos – Inversiones D. L. Nº 1133**

| NIVEL RIESGO | Rango de exposición a riesgos (Nuevos Soles) |
|---|---|
| EXTREMO | Mayor a 67,000 |
| ALTO | <49,000; 67,000] |
| MODERADO | <14,000; 49,000] |
| BAJO | <0; 14,000] |

**Tabla Nº 8: Clasificación de riesgos – Procesos de ambos regímenes**

| NIVEL RIESGO | Rango de exposición a riesgos (Nuevos Soles) |
|---|---|
| EXTREMO | Mayor a 67,000 |
| ALTO | <49,000; 67,000] |
| MODERADO | <14,000; 49,000] |
| BAJO | <0; 14,000] |

### 3.6. Tratamiento de riesgos

Es el tratamiento que se le da a cada uno de los riesgos y se decide en base a las siguientes alternativas:

**3.6.1.** Evitar el riesgo: Es el retiro de actividades causantes del riesgo, en las cuales su tratamiento adicional no es efectivo en costo y el retorno no es atractivo en relación al riesgo involucrado.

**3.6.2.** Reducir el riesgo: Es mediante la aplicación de técnicas o procedimientos destinados a reducir su probabilidad de ocurrencia o su impacto.

**3.6.2.1.** Reducir su probabilidad de ocurrencia, considerando controles técnicos, controles a procesos, mantenimientos preventivos, entre otros.

**3.6.2.2.** Reducir las consecuencias, por ejemplo, considerando planes de recuperación de desastres, separación o reubicación de activos, planes de contingencia, condiciones contractuales.

**3.6.3.** Transferir el riesgo: Son actividades y medidas con tendencia a compartir con un tercero la responsabilidad por el manejo de riesgos y transferir la obligación por las consecuencias financieras del riesgo, en caso de ocurrencia.

**3.6.4.** Aceptar el riesgo: Es aceptar el riesgo donde los retornos potenciales son atractivos en relación con los riesgos involucrados. En este caso, el riesgo se puede administrar mediante procedimientos rutinarios.

Los riesgos evaluados de acuerdo a su nivel de riesgo son reportados a diferentes instancias para la adopción de las medidas de tratamiento según se indica en la Tabla Nº 9, donde se definen las políticas para la toma de acciones y el tiempo máximo de atención, según el nivel de riesgo o monto máximo de exposición.

**Tabla Nº 9: Políticas para la toma de acciones y tiempo máximo de atención**

| Nivel de riesgo | Tiempo máximo de atención | Aplica implementación de acción inmediata |
|---|---|---|
| **EXTREMO** | 1 mes | Si |
| **ALTO** | 3 meses | Si |
| **MODERADO** | 6 meses | No |

Para aquellos casos en los cuales el plan de acción, de acuerdo a su complejidad, requiera ser implementado en el plazo máximo de atención, desde que es definido, es necesario ejecutar una acción inmediata que permita tener controlado el riesgo mientras no sea implementado el plan de acción.

Los resultados correspondientes al análisis, clasificación y tratamiento de los riesgos se registran en la matriz de riesgos operacionales.

Los procesos o sus modificaciones en el ambiente operativo y tecnológico, deben ser evaluados utilizando la metodología establecida para las autoevaluaciones de riesgos y los resultados deben ser presentados al Comité de Riesgos.

### 3.7. Monitoreo continuo de los riesgos

**3.7.1.** Monitoreo: Consiste en hacer una revisión del flujo del proceso, actividad o sistema, con el fin de identificar nuevos riesgos.

**3.7.2.** Revisar la acción de mitigación de riesgos: Consiste en revisar el cumplimiento de los planes de acción adoptados en la fase de tratamiento de riesgos. Si el plan de acción ha sido desarrollado, se debe verificar su implementación.

Asimismo, de presentarse la necesidad, el gestor de riesgo operacional puede solicitar la reprogramación de fecha de implementación de un plan de acción, siempre y cuando se encuentre debidamente sustentado, y aprobado por su gerencia. Además, solo se acepta una reprogramación por plan de acción. De no implementarse el plan de acción en el plazo acordado, debe ser informado a la Gerencia General.

**3.7.3.** Monitoreo de riesgos residuales y revisión de controles: El nivel de riesgo residual se debe hallar en función a la evaluación del control. Dicha evaluación es producto de la revisión bajo la metodología establecida en el punto 3.4.2 “Evaluación de Controles”.

**3.7.4.** Revisar y actualizar las medidas de tratamiento: De acuerdo al resultado de los riesgos residuales se definen las nuevas medidas de tratamiento.

**3.7.5.** Desestimar los riesgos: Los riesgos pueden ser desestimados cuando la actividad que dio origen al riesgo ya no se ejecuta, debiendo contar con la documentación de sustento.

### 3.8. Comunicar y consultar

En esta etapa se genera y transmite la información apropiada y oportuna al Consejo Directivo, a la gerencia, al personal, así como a interesados externos tales como supervisores y reguladores (ver Tabla Nº 10).

**Tabla Nº 10: Políticas para la toma de acciones y tiempo máximo de atención**

| Informe | Dirigido a | Periodicidad |
|---|---|---|
| Informe de gestión del riesgo operacional (IG-ROP) | SBS | Anual |
| Resumen de la gestión del riesgo operacional | Memorial anual | Anual |
| Informe trimestral de gestión del riesgo operacional | Comité de Riesgos | Trimestral |
| Informe de nuevos productos, cambios importantes y subcontrataciones | Gerente responsable de iniciativa | Cuando amerite |
| | Comité de Riesgos | |
| | SBS | |

## 4. INDICADOR CLAVE DE RIESGO

La metodología comprende las etapas de definición y monitoreo del indicador clave de riesgo.

### 4.1. Definición del indicador clave de riesgo

**4.1.1.** Un indicador clave de riesgos se debe definir e implementar cuando se presente alguna de las siguientes situaciones:

**4.1.1.1.** Riesgos con nivel inherente alto y extremo.

**4.1.1.2.** Riesgos que mantienen un nivel residual moderado posterior a la implementación de planes de acción.

**4.1.1.3.** Riesgos con nivel residual moderado con una frecuencia igual o mayor a seis (6) veces al año.

El indicador clave de riesgo debe ser monitoreado por un periodo de seis (6) meses, periodo que puede ser extendido en caso sea necesario.

**4.1.2.** El gestor de riesgo operacional diseña el indicador clave de riesgo con el apoyo del Departamento de Riesgos Operacionales en la aplicación de la metodología para definir el indicador clave de riesgo.

**4.1.3.** El gestor de riesgo operacional debe completar la siguiente información básica que forma parte de la ficha del indicador clave de riesgo:

**4.1.3.1** Riesgo residual cuyo nivel de exposición es alto.

**4.1.3.2** Periodo de la Autoevaluación de Riesgos y Controles en la que se identificó el riesgo residual cuyo nivel de exposición es alto.

**4.1.3.3** Proceso en la que se identificó el riesgo residual cuyo nivel de exposición es alto.

**4.1.3.4** Nombre del indicador clave de riesgo.

**4.1.3.5** Descripción del indicador clave de riesgo.

**4.1.3.6** Método de cálculo para la medición del indicador clave de riesgo.

**4.1.3.7** Unidad de medida del indicador clave de riesgo.

**4.1.3.8** Periodicidad de reporte del indicador clave de riesgo.

**4.1.3.9** Umbrales para el indicador clave de riesgo.

**4.1.3.10** Responsable del cálculo del indicador clave de riesgo.

**4.2. Monitoreo del indicador clave de riesgo**

**4.2.1.** El gestor de riesgo operacional debe calcular y reportar en la periodicidad definida en el numeral 4.1.3.8, lo siguiente:

**4.2.1.1.** Valor del indicador clave de riesgo.

**4.2.1.2.** Sustento de la información utilizada para el cálculo del indicador.

**4.2.2.** El gestor de riesgo operacional es responsable de custodiar la documentación de soporte necesaria que permita a auditoría interna o externa la validación del cálculo y registro del indicador clave de riesgo en caso de ser auditados.

**4.2.3.** El Departamento de Riesgos Operacionales revisa que los valores reportados por el gestor de riesgo operacional cumplan con los criterios definidos en la ficha del indicador de riesgo operacional.

**4.2.4.** El gestor de riesgo operacional monitorea que el comportamiento de los valores del indicador clave de riesgo se encuentre dentro de los umbrales de riesgos definidos. En caso se supere el umbral establecido, debe definir planes de acción para mitigar el riesgo.

**4.2.5.** El Departamento de Riesgos Operacionales realiza el seguimiento a la implementación de los planes de acción para la mitigación del riesgo.

# 5. BASE DE DATOS DE EVENTOS DE PÉRDIDA (BDEP)

Con la finalidad de administrar las pérdidas operacionales de la CPMP e implementar planes de acción para el control y mitigación de los riesgos asociados a las pérdidas presentadas, se desarrolla la base de datos de eventos de pérdida por riesgo operacional.

## 5.1. Recolección de datos internos de eventos de pérdida

### 5.1.1. Criterios generales

**5.1.1.1.** La CPMP identifica eventos que generan impacto en la contabilidad.

**5.1.1.2.** La unidad orgánica en la cual se genere el evento de pérdida, debe contar con el sustento de cada evento de pérdida por riesgo operacional.

**5.1.1.3.** Los eventos que conducen a costos de oportunidad o ganancias no realizadas no serán registrados en la BDEP.

**5.1.1.4.** Los eventos de pérdida son asignados a la línea del negocio definido por la CPMP, según el impacto que generen en estas.

**5.1.1.5.** Si la actividad presta apoyo a más de una línea de negocio, el evento de pérdida es distribuido entre las líneas de negocio, de manera proporcional al apoyo que presta, considerando la política interna de distribución de gastos.

**5.1.1.6.** El registro en la base de datos de eventos de pérdida solo se lleva a cabo cuando la pérdida se refleje en las cuentas contables.

**5.1.1.7.** Para los eventos de pérdida que superen el umbral definido de acuerdo al apetito de riesgos, se debe elaborar un informe, el cual debe contener como mínimo la causa del evento, una descripción del modo en que se produjo el

evento, la unidad orgánica que originó la pérdida, el riesgo asociado y las acciones adoptadas para mitigar la ocurrencia de eventos similares a futuro.

**5.1.2. Clasificación de eventos de pérdida**

**5.1.2.1.** La clasificación se realiza considerando la clasificación establecida por la Superintendencia de Banca, Seguros y AFP (Anexo 1).

**5.1.2.2.** Para la asignación de los eventos de pérdidas se considera el árbol de decisiones (Anexo 2).

**5.1.3. Valoración de los eventos de pérdida**

**5.1.3.1.** El monto bruto de pérdida asociada a un evento de pérdida por riesgo operacional incluye los siguientes aspectos, según sean aplicables:

**a)** Impacto directo en los estados financieros, incluyendo gastos, disminución del valor de los activos, entre otros.

**b)** Gastos de reparación o reemplazo para restablecer la situación existente antes de la ocurrencia del evento, incluyendo el pago de deducibles asociados a los seguros contratados.

**c)** Provisiones reconocidas en los estados financieros asociadas con eventos de pérdida por riesgo operacional.

**5.1.3.2.** Los siguientes aspectos no son considerados en la determinación del monto bruto de pérdida:

**a)** Recuperaciones posteriores a la ocurrencia del evento de pérdida.

**b)** Gastos provenientes de contratos generales de mantenimiento de equipos o locales.

**c)** Gastos asociados con mejoras realizadas luego del evento de pérdida.

**d)** Primas de seguros.

**5.1.3.3.** Las pérdidas asociadas a daños en activos fijos que los inhabilitan son registradas en la BDEP, según las siguientes disposiciones:

**a)** Si se reemplaza el activo dañado, debe registrarse como pérdida el costo de adquisición.

**b)** Si no se reemplaza el activo dañado, debe registrarse como pérdida el precio estimado de mercado de dicho activo o, en caso este no se conozca, debe registrarse el costo histórico de adquisición.

**c)** En caso se reemplace el activo de manera posterior, se debe modificar el monto de pérdida registrado en la BDEP siguiendo lo indicado en el literal a.

**5.1.3.4.** En los casos en que un evento produce simultáneamente pérdidas y ganancias para la entidad, con un saldo neto negativo, dicho saldo es considerado para el cálculo del monto de pérdida y su registro en la BDEP.

**5.1.3.5.** Los eventos de pérdida asociados a reclamos presentados por los usuarios son incorporados en la BDEP.

**5.1.4. Recuperaciones**

Toda recuperación asociada al evento es registrada en la BDEP de manera separada al monto bruto de pérdida, pero relacionada al evento. Se considera una recuperación siempre que esta se produzca de manera independiente y posterior a la ocurrencia del evento de pérdida original. En el anexo 3 se incluye una relación no limitativa de recuperaciones.

**5.1.5. Provisiones**

**5.1.5.1.** Las provisiones reconocidas en los estados financieros asociadas a eventos de pérdida por riesgo operacional son registradas en la BDEP, incluyendo entre otras, las relacionadas a controversias judiciales, procesos arbitrales y procedimientos administrativos.

**5.1.5.2.** El monto de la provisión registrado en la BDEP es actualizado tantas veces como la provisión sea modificada. En el momento que se conozca con certeza el monto de pérdida definitivo asociado al evento, se reemplaza el monto de la provisión registrada por el importe definitivo.

**5.1.5.3.** Las provisiones registradas en la BDEP son identificadas, de forma que puedan distinguirse de otros impactos asociados al evento.

### 5.1.6. Evento con pérdidas múltiples

**5.1.6.1.** En caso de presentarse diversas pérdidas causadas por un evento en común, estas se agrupan en un mismo evento. Sin embargo, el registro en la base de datos se realiza en forma separada.

**5.1.6.2.** Los errores múltiples originados por una misma persona a través de un determinado periodo de tiempo son tratados como eventos independientes, por lo cual no deben ser agrupados en la BDEP.

**5.1.6.3.** En el Anexo 4 se incluye una lista no limitativa de eventos con pérdidas múltiples.

### 5.1.7. Evento con pérdidas por riesgo operacional asociadas a otros riesgos

**5.1.7.1.** Eventos de pérdida asociados al riesgo legal: Todo evento de pérdida atribuible al riesgo legal se registra en la BDEP, como el riesgo de cumplimiento, u otras que incluyan el riesgo legal o partes de este.

**5.1.7.2.** Eventos de pérdida asociados a actividades que generan riesgo de crédito: Los eventos de pérdida por riesgo operacional asociados al riesgo de crédito son registrados en la BDEP.

**5.1.7.3.** Eventos de pérdida asociados a actividades que generan riesgo de mercado: Los eventos de pérdida por riesgo operacional asociados a actividades que generan riesgo de mercado son registrados en la BDEP.

**5.1.7.4.** Eventos de pérdida asociados al riesgo estratégico: Las pérdidas originadas por el riesgo estratégico no son registrados en la BDEP.

**5.1.7.5.** Eventos de pérdida asociados al riesgo de reputación: Los eventos de pérdida por riesgo operacional asociados a la afectación de la reputación o la imagen de la entidad son registrados en la BDEP, así como todo gasto no regular o planificado asociado a la corrección de dichos efectos.

**5.1.8. Eventos de pérdida asociados a productos de seguros**

**5.1.8.1.** Los eventos de pérdida por riesgo operacional asociados a los productos de seguros son registrados en la BDEP se deben identificar en la relación en la BDEP.

**5.1.8.2.** No se registran en la BDEP las pérdidas asociadas al funcionamiento de modelos de riesgos de seguros por causas distintas a las operacionales, por ejemplo, debido a la incertidumbre propia de los modelos, que fueron debidamente estudiadas en su oportunidad y aceptadas como parte de un proceso formal de toma de decisiones.

**5.2. Estructura de la base de datos de eventos de pérdida**

**5.2.1.** Código de evento

**5.2.2.** Tipo de evento de pérdida nivel 1.

**5.2.3.** Tipo de evento de pérdida nivel 2.

**5.2.4.** Línea de negocio de la CPMP.

**5.2.5.** Descripción corta del evento.

**5.2.6.** Descripción larga del evento.

**5.2.7.** Fecha de ocurrencia o inicio del evento.

**5.2.8.** Fecha de descubrimiento del evento.

**5.2.9.** Fecha de registro contable del evento.

**5.2.10.** Monto bruto de la pérdida.

**5.2.11.** Moneda (bruto).

**5.2.12.** Tipo de cambio (bruto).

**5.2.13.** Monto recuperado.

**5.2.14.** Tipo de cambio (recuperado).

**5.2.15.** Monto total recuperado.

**5.2.16.** Moneda (total recuperado).

**5.2.17.** Cuenta de provisión.

**5.2.18.** Tipo de cambio (total recuperado).

**5.2.19.** Cuenta contable.

**5.2.20.** Monto neto de perdida.

**5.2.21.** Código de documento sustentatorio.

**5.2.22.** Descripción de proceso.

**5.2.23.** Relación con otros riesgos.

**5.3. Dinámicas contables para la gestión de eventos de pérdida**

**5.3.1.** Toda unidad orgánica reporta al quinto día útil del mes siguiente sus eventos de pérdida y provisiones asociadas al riesgo operacional al Departamento de Riesgos Operacionales. En caso, la unidad orgánica no registre eventos de pérdida o provisiones asociadas al riesgo operacional en el mes, debe confirmarlo al Departamento de Riesgos Operacionales.

**5.3.2.** El Departamento de Contabilidad informa mensualmente al Departamento de Riesgos Operacionales los gastos generados y registrados en las cuentas contables que correspondan a eventos de pérdida y provisiones por riesgo operacional.

**5.3.3.** La Subgerencia de Logística informa al Departamento de Riesgos Operacionales la utilización de algún seguro para reducir el impacto de un evento de pérdida por riesgo operacional.

**5.3.4.** El Departamento de Riesgos Operacionales realiza el registro en la base de datos eventos de pérdida, en función a la información registrada y reportada por el Departamento de Contabilidad y los gestores de riesgo operacional.

**5.3.5.** Las pérdidas por riesgo operacional son puestas en conocimiento al Comité de Riesgos por el Departamento de Riesgos Operacionales.

**5.3.6.** Se detallan las cuentas contables para el registro de los eventos de pérdida por riesgo operacional:

**5.3.6.1.** Contingencias Civiles (9043010602).

**5.3.6.2.** Contingencias Tributarias (9043010601).

**5.3.6.3.** Indemnizaciones Judiciales (904505010416).

**5.3.6.4.** Multas (904504010105).

**5.3.6.5.** Otros Reclamos M.N (1517010102).

**5.3.6.6.** Otros Gastos (90650109).

**5.3.6.7.** Otros Gastos Judiciales (904505010415).

**5.3.6.8.** Provisión de Contingencias Civiles (2802010102).

**5.3.6.9.** Otros gastos de gestión (904505010909).

**5.3.6.10.** Otros (5701010505).

## 6. NUEVOS PRODUCTOS O CAMBIOS IMPORTANTES EN EL AMBIENTE DE NEGOCIO, OPERATIVO O INFORMÁTICO

**6.1.** La CPMP gestiona los riesgos operacionales previamente al lanzamiento de un nuevo producto o cambios importantes en el ambiente de negocios, operativos o informático.

**6.2.** Los niveles de riesgo utilizados en la evaluación son los aprobados en el presente manual. Se considera como cambio importante, según la Resolución SBS Nº 2116 – Reglamento para la Gestión de Riesgo Operacional, lo siguiente:

**6.2.1.** Cambios en la forma en la que se conducen los negocios y operaciones, originados por modificaciones en las condiciones económicas, políticas o legales.

**6.2.2.** Subcontrataciones significativas.

**6.2.3.** Alianzas, contratos asociativos, participación en negocios conjuntos.

**6.2.4.** Reorganizaciones empresariales.

**6.2.5.** Proyectos cuya falla pueda generar pérdidas significativas.

**6.2.6.** Implementación de un nuevo canal de atención. En este caso, se considera como cambio importante la implementación por primera vez del nuevo canal de atención y/o modificaciones importantes a su funcionamiento.

**6.2.7.** Cambio de la infraestructura tecnológica que soporta los principales productos y/o servicios de la empresa.

**6.2.8.** Traslado de la oficina principal de la empresa.

**6.3.** Remitir a la SBS la copia de los informes de riesgos de los nuevos productos dentro de los diez (10) días hábiles siguientes a su lanzamiento y para cambios importantes en el ambiente operativo o informático dentro de los diez (10) días hábiles, luego de presentados al Comité de Riesgos.

**6.4.** Etapas del proceso de evaluación de riesgos operacionales

**6.4.1.** Las unidades orgánicas, a través de sus gestores de riesgos, informan al Departamento de Riesgos Operacionales cada una de las propuestas que tienen para lanzar un nuevo producto o realizar un cambio planificado en el ambiente de negocio, operativo o informático de la organización. El gestor de riesgo operacional debe completar el Anexo 1 y remitirlo al Departamento de Riesgos Operacionales, a fin de determinar si es un cambio importante o no.

**6.4.2.** De tratarse de un cambio importante, la Gerencia de Riesgos y Desarrollo presenta al Comité de Riesgos un informe de riesgos por nuevos productos o cambios importantes en el ambiente de negocios, operativo o informático para su posterior envío a la SBS.

## 7. SERVICIO SIGNIFICATIVO Y SUBCONTRATACIÓN SIGNIFICATIVA

### 7.1. Etapas del proceso de evaluación de proveedores

**7.1.1.** Las unidades orgánicas, a través de sus gestores de riesgos, informan al Departamento de Riesgos Operacionales, las propuestas que tienen respecto a la contratación de un servicio de tercero al contratar un servicio de tercero.

**7.1.2.** El Departamento de Riesgos Operacionales hace un cruce de información mensual de las propuestas de contratación de servicio remitidas por los gestores de riesgos con la base de datos del Departamento de Contrataciones (pedidos de servicio).

**7.1.3.** Para identificar si un pedido de servicio corresponde a un servicio significativo, se debe completar un cuestionario que agrupa cuatro (4) criterios para calificar el servicio. De acuerdo a la calificación obtenida, es catalogado como servicio significativo, servicio importante o servicio no significativo:

**Cuadro: Cuestionario para la identificación de servicios significativos**

| Identificación de Servicios Significativos | | | | |
|---|---|---|---|---|
| Gerencia o unidad solicitante: | | | | |
| Proveedor: | | | | |
| Descripción del servicio: | | | | |
| **Criterios** | | | | **Marque con X** |
| **1. INGRESOS** | Nivel de ingresos que la empresa dejaría de generar en caso de interrupción o suspensión del servicio. | a. | Menor igual a S/ 14000 | |
| | | b. | Mayor a S/ 14000 hasta S/ 49000 | |
| | | c. | Mayor a S/ 49000 hasta S/ 97000 | |
| | | d. | Mayor a S/ 97000 | |
| **2. CONTINUIDAD OPERATIVA** | Impacto en la continuidad de los procesos críticos en caso de interrupción o suspensión del servicio | a. | No interrumpe ningún macroproceso critico | |
| | | b. | Interrumpe a uno o más macroprocesos criticos | |
| **3. REPUTACIÓN** | Impacto en la reputación de la entidad en caso de interrupción o suspension del servicio | a. | No impacta en la reputación de la entidad | |
| | | b. | Impacta parcialmente en la reputación de la entidad (genera incomodidad, reclamos o | |
| | | c. | Impacta seriamente en la reputación de la entidad (difusión en redes sociales u otros medios informativos) | |
| **4. SEGURIDAD DE LA INFORMACIÓN** | Impacto en la Seguridad de la Información de la entidad, considerando la información a la que se tiene acceso a partir del servicio | a. | No afecta a la confidencialidad, integridad o disponibilidad de información confidencial | |
| | | b. | Afecta a la confidencialidad, integridad o disponibilidad de información confidencial | |

| Calificación | Criterio de evaluación |
|---|---|
| > 2 | Servicio significativo |
| < 1.5, 2 ] | Servicio importante |
| < 0, 1.5 ] | Servicio no significativo |

**7.1.4.** Si el servicio a contratar corresponde a un servicio significativo, se deben incluir en el contrato las cláusulas que figuran en los anexos 5, 6 y se debe realizar una autoevaluación de riesgos y controles, en coordinación con los gestores de riesgo operacional, según lo desarrollado en el numeral 3 del capítulo III, cuyos resultados deben ser presentados en el Comité de Riesgos.

**7.1.5.** En caso de que el servicio significativo sea provisto por un tercero bajo la modalidad de subcontratación, esta se considera significativa y como tal, se debe remitir una copia de los informes de resultados a la SBS, dentro de los diez (10) días hábiles de presentados al Comité de Riesgos.

**7.1.6.** Los gestores de riesgos son responsables de verificar que se incluyan en los contratos las cláusulas de riesgo operacional necesarias.

# 8. SISTEMA DE INCENTIVOS

## 8.1 Lineamientos

**8.1.1** La evaluación para la aplicación de incentivos es realizada por la Gerencia de Riesgos y Desarrollo en forma anual con la finalidad de premiar al mejor gestor de riesgo operacional.

**8.1.2** La CPMP otorga incentivos no monetarios de reconocimiento a los gestores que hayan destacado en la gestión de riesgo operacional.

**8.1.3** Los gestores de riesgo operacional deben obtener como mínimo una calificación de 13, en caso sea inferior se comunicará al gerente de la unidad orgánica a fin de coordinar planes de acción para mejorar su desempeño.

## 8.2 Criterios de evaluación

Para la evaluación de desempeño de los gestores de riesgo operacional se considera una calificación máxima de veinte (20) puntos, los cuales se distribuyen entre los criterios que se presentan en la siguiente tabla. Asimismo, se muestra el puntaje por cada criterio y gestión (Gestión de Riesgo Operacional, Gestión de Continuidad del Negocio y Gestión de Seguridad de la Información y Ciberseguridad).

| Nº | Criterios | Peso | Calificación | Descripción | Puntaje | Gestiones | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | RO | SI | CN |
| 1 | Autoevaluación de riesgos | 15% | Cumplió | El gestor atiende el requerimiento de información en el plazo establecido y participa en las actividades de acuerdo lo planificado. | 3 | 1 | 1 | 1 |
| | | | Cumplió parcialmente | El gestor atiende el requerimiento de información en el plazo establecido o participa en las actividades de acuerdo lo planificado. | 1.5 | 0.5 | 0.5 | 0.5 |
| | | | No cumplió | - | 0 | 0 | 0 | 0 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **2** | Reporte de eventos de pérdida / incidentes | **15%** | Cumplió | El gestor reporta el evento de pérdida en el plazo establecido. | 3 | 1 | 1 | 1 |
| | | | No cumplió | El gestor reporta el evento de pérdida fuera del plazo establecido. | 0 | 0 | 0 | 0 |
| **3** | Cumplimiento de planes de acción | **15%** | Implementado | El gestor implementa los planes de acción en la fecha programada | 3 | 1 | 1 | 1 |
| | | | No implementado | - | 0 | 0 | 0 | 0 |
| **4** | Participación en las capacitaciones | **15%** | Participó | El gestor participa en las capacitaciones programadas. | 3 | 1 | 1 | 1 |
| | | | No participó | - | 0 | 0 | 0 | 0 |
| **5** | Reporte de indicadores claves de riesgo | **10%** | Reportó | El gestor atiende el requerimiento de información en el plazo establecido. | 2 | 2 | - | - |
| | | | No reportó | - | 0 | 0 | 0 | 0 |
| **6** | Participación en las pruebas de continuidad del negocio | **15%** | Participó | El gestor participa en las pruebas programadas. | 3 | - | - | 3 |
| | | | No participó | - | 0 | 0 | 0 | 0 |
| **7** | Cumplimiento del inventario de activos de información | **15%** | Cumplió | El gestor brinda conformidad el inventario de activos en el plazo establecido | 3 | - | 3 | - |
| | | | No cumplió | - | 0 | 0 | 0 | 0 |

De no aplicar un criterio en un periodo determinado, el puntaje de dicho criterio es distribuido entre los demás criterios. Asimismo, de no aplicar un criterio para una gestión, los puntos de dicho criterio son distribuidos entre las demás gestiones.

### 8.3 Penalidades

En caso de presentarse las siguientes situaciones, se penaliza con un (1) punto menos a la calificación total del gestor de riesgo operacional en el periodo evaluado.

**8.3.1** Indicadores claves de riesgos: El mantener indicadores fuera del umbral esperado por más de dos (2) periodos consecutivos.

**8.3.2** Eventos de pérdida por riesgo operacional: El presentarse un evento de perdida, a pesar de haber implementado un plan de acción para evitar recurrencia.

**8.3.3** Pruebas de continuidad: La reprogramación injustificada de las pruebas de continuidad del negocio.

**8.3.4** Planes de acción: La reprogramación injustificada de los planes de acción o mantener planes en estado vencido.

# CAPÍTULO III: ANEXOS

## 1. ANEXOS

- Anexo 1: Tipos de eventos de pérdida por riesgo operacional
- Anexo 2: Árbol de decisiones para determinar el tipo de evento de pérdida por riesgo operacional.
- Anexo 3: Lista no limitativa de recuperaciones relacionadas a los eventos de pérdida de riesgo operacional.
- Anexo 4: Lista no limitativa de eventos con pérdidas múltiples.
- Anexo 5: Cláusula de riesgo de operación.
- Anexo 6: Cláusula de seguridad de información.

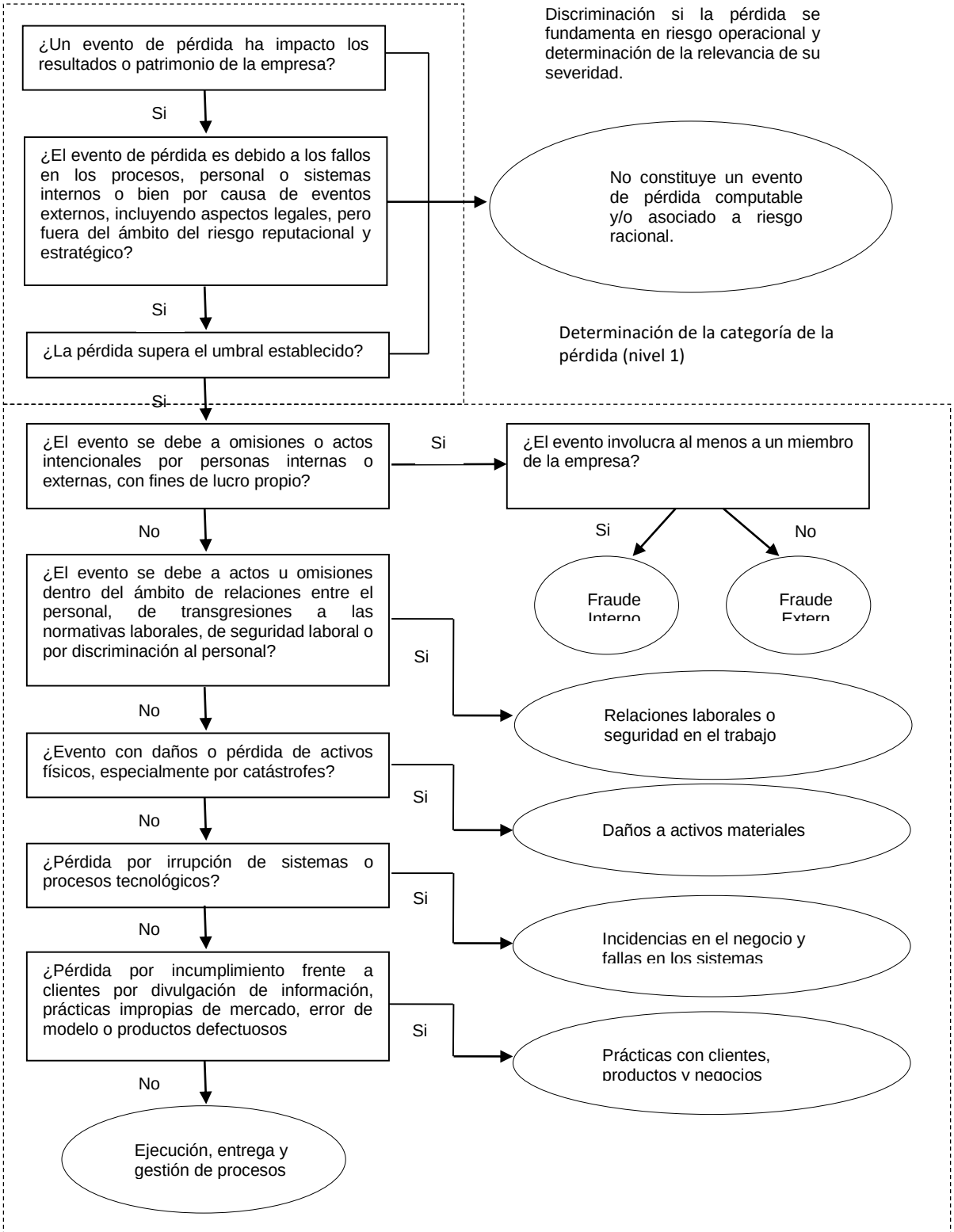
# TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

| Tipo de evento (nivel 1) | Definición | Tipo de evento (nivel 2) | Ejemplos |
|---|---|---|---|
| Fraude Interno | Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicado, al menos, un miembro de la empresa. | Actividades no autorizadas | Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones (intencional). |
| | | Robo y fraude | Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional). |
| 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. | Robo y fraude | Robo, falsificaciones |
| | | Seguridad de los Sistemas | Daños por ataques informáticos, robo de información |
| 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. | Relaciones laborales | Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos. |
| | | Higiene y seguridad en el trabajo | Casos relacionados con las normas de higiene y seguridad en el trabajo, indemnización a los trabajadores. |
| | | Diversidad y discriminación | Todo tipo de discriminación. |
| Clientes, productos y prácticas empresariales | Pérdidas derivadas del incumplimiento involuntario o negligente de una | Adecuación, divulgación de información y confianza | Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación |

| | | | |
|---|---|---|---|
| | obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto. | | de información (conocimiento del cliente, etc.), quebrantamiento de la privacidad de información sobre clientes minoristas, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial. |
| | | Prácticas empresariales o de mercado improcedentes | Prácticas restrictivas de la competencia, prácticas comerciales / de mercado improcedentes, manipulación del mercado, abuso de información privilegiada (en favor de la empresa), lavado de dinero. |
| | | Productos defectuosos | Defectos del producto (no autorizado, etc.), error de los modelos. |
| | | Selección, patrocinio y riesgos | Ausencia de investigación a clientes conforme a las directrices, exceso de los límites de riesgo frente a clientes. |
| | | Actividades de asesoramiento | Litigios sobre resultados de las actividades de asesoramiento. |
| Daños a activos materiales | Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos | Desastres y otros acontecimientos | Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo). |
| Interrupción del negocio y fallos en los sistemas | Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas. | Sistemas | Pérdidas por fallas en equipos de hardware, software o telecomunicaciones, falla en energía eléctrica. |

| | | | |
|---|---|---|---|
| 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 | Recepción, ejecución y mantenimiento de operaciones | Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo (p.ej. en la Entrega contra pago). |
| | | Seguimiento y presentación de informes | Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas). |
| | | Aceptación de clientes y documentación | Inexistencia de autorizaciones / rechazos de clientes, documentos jurídicos inexistentes / incompletos. |
| | | Gestión de cuentas de clientes | Acceso no autorizado a cuentas, registros incorrectos de clientes (con generación de pérdidas), pérdida o daño de activos de clientes por negligencia. |
| | | Contrapartes comerciales | Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes. |
| | | Distribuidores y proveedores | Subcontratación, litigios con proveedores. |

# ÁRBOL DE DECISIONES PARA DETERMINAR EL TIPO DE EVENTO DE PÉRDIDA POR RIESGO OPERACIONAL



| **LISTA NO LIMITATIVA DE RECUPERACIONES RELACIONADAS A LOS EVENTOS DE PÉRDIDA DE RIESGO OPERACIONAL** |
| --- |
| ▪ Pagos recibidos de una compañía de seguros luego de la ejecución de pólizas contratadas.<br>▪ Pagos recibidos como resultado favorable de un proceso judicial o arbitral.<br>▪ Pagos entregados por un tercero que preste servicios a la empresa, con el objetivo de mitigar el impacto negativo de la ocurrencia de un evento de pérdida de su responsabilidad que afectó a ambas partes.<br>▪ Pagos recibidos de afiliados o trabajadores como resultado del proceso de recuperación. |

| LISTA NO LIMITATIVA DE EVENTOS CON PÉRDIDAS MÚLTIPLES |
| --- |
| ▪ Errores repetidos originados por una falla en un proceso o producto.<br>▪ Reembolsos a varios afiliados provenientes de unos reclamos comunes u originados por un solo evento (por ejemplo, la pérdida de documentos durante una mudanza o por un incendio).<br>▪ Pérdidas por fraude realizadas a través de una misma acción y por la misma persona o grupo criminal.<br>▪ Una interrupción de los servicios de tecnología que afecte a múltiples líneas de negocio.<br>▪ Un individuo o grupo de trabajadores que recibe instrucciones erradas que genera pérdidas múltiples. |

# CLÁUSULA DE RIESGO DE OPERACIÓN

LA EMPRESA y LA CPMP declaran tener conocimiento de lo dispuesto por la Resolución SBS 272 – 2017 "Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos" y sus modificatorias, cuyo objeto es que las empresas supervisadas cuenten con un sistema de control de riesgos que les permitan identificar, medir, controlar y reportar los riesgos que enfrentan, a fin de minimizar la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de procesos considerados como indispensables para la continuidad de sus operaciones y servicios, y cuya falta o ejecución deficiente puede tener un impacto financiero significativo.

En mérito de lo antes señalado y cumpliendo lo dispuesto por la norma acotada, LA EMPRESA se obliga a mantener a disposición de la CPMP, su Órgano de Control Institucional y su Sociedad de Auditora Externa, así como por las personas que la Superintendencia de Banca, Seguros y AFP designe para tal fin, y en el momento que así lo consideren conveniente, lo siguiente:

- Todas las facilidades que sean necesarias para realizar y obtener las pruebas que permitan realizar una adecuada revisión del servicio prestado.

- Proporcionar toda la información y/o documentación que sea requerida y únicamente en relación al servicio contratado, en salvaguarda de la protección de datos de los clientes de LA EMPRESA.

Para tal fin, bastará que LA CPMP envíe una comunicación a LA EMPRESA, con tres (3) días calendarios de anticipación.

# CLÁUSULA DE SEGURIDAD DE INFORMACIÓN

LA EMPRESA declara conocer, y se compromete a cumplir con todas las normas vigentes en Perú relacionada con las condiciones mínimas de seguridad que deben tenerse en cuenta respecto de la información proporcionada por la CPMP y a su procesamiento.

LA EMPRESA asume responsabilidad de tomar todas las medidas necesarias para garantizar que la información materia del presente contrato y su procesamiento sea manejada de forma aislada en todo momento y bajo cualquier circunstancia.

LA EMPRESA proveerá a solo requerimiento de la CPMP, su Órgano de Control Institucional y su Sociedad de Auditora Externa, así como por las personas que la Superintendencia de Banca, Seguros y AFP designe para tal fin, el acceso suficiente y oportuno a la información materia de este contrato, el mismo que deberá ser otorgado en tiempos razonables.

Las partes acuerdan que toda la información y/o documentación suministrada directa o indirectamente por la CPMP a LA EMPRESA en virtud de este contrato deberá ser considerada como información confidencial la misma que es de exclusiva propiedad de la CPMP, LA EMPRESA no podrá usar la información provista para propósito distinto al permitido o requerido en el presente contrato.

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| 1.OBJETIVO | Establecer ~~las políticas y~~ procedimientos~~, así como las funciones y responsabilidades~~ para identificar, medir, controlar y reportar el riesgo operacional al que está expuesta la Caja de Pensiones Militar Policial (CPMP), dentro del marco del Sistema de Gestión Integral de Riesgos. | Establecer **los** procedimientos para identificar, medir, controlar y reportar el riesgo operacional al que está expuesta la Caja de Pensiones Militar Policial (CPMP), dentro del marco del Sistema de Gestión Integral de Riesgos. | Se retiró la menciona a políticas y funciones y responsabilidades para que formen parte de la directiva "Política de Gestión de Riesgo Operacional". |
| 2. REFERENCIA LEGAL Y NORMATIVA | (…)<br>▪ Manual de Descripción de Cargos de la Caja de Pensiones Militar Policial<br>(…)<br>▪ Resolución SBS Nº 877-2020 – Reglamento para la Gestión de la Continuidad del Negocio **y sus modificatorias**<br>▪ 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**<br>(…)<br>~~▪ Manual de Descripción de Cargos de la Caja de Pensiones Militar Policial~~<br>▪ Directiva de Consejo Directivo Nº ~~12-2018~~ – Reglamento de Comité de Riesgos<br>(…) | (…)<br>▪ **Decreto Legislativo Nº 1133 – Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial, y sus modificatorias**<br>▪ **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**<br>(…)<br>▪ Resolución SBS Nº 877-2020 – Reglamento para la Gestión de la Continuidad del Negocio **y sus modificatorias**<br>▪ 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**<br>(…)<br>▪ Directiva de Consejo Directivo Nº **14-2024** – Reglamento de Comité de Riesgos<br>**Directiva de Consejo Directivo Nº 01-2025 – Política de Gestión de Riesgo Operacional** | Se actualizó la referencia legal y normativa. |
| 4. GLOSARIO | (…) | (…)<br>**4.20. Servicios significativos: Los servicios significativos provistos por terceros son aquellos que, en caso de falla o suspensión, pueden poner en riesgo importante a la empresa al afectar sus ingresos, solvencia, continuidad operativa o reputación. En caso de que algún bien y/o servicio significativo sea provisto por un tercero bajo la modalidad de subcontratación, la subcontratación se considera significativa.**<br>(…) | Se actualizó el glosario y se agregó la terminología correspondiente a servicios significativos. |
| | ~~5.1. Del Consejo Directivo~~<br>~~a) Aprobar la política general que guíe las actividades de la CPMP en la gestión de sus riesgos operacionales.~~<br>~~b) Asignar los recursos necesarios para la gestión de riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiado.~~<br>~~c) Establecer un sistema de incentivos que fomente la gestión de riesgo operacional y que favorezca la toma apropiada de riesgos y que a su vez contribuya a ampliar el compromiso del personal de la CPMP en la aplicación de la metodología para la administración del riesgo operacional.~~<br>~~d) Aprobar el apetito de riesgo operacional de la CPMP.~~<br>~~e) Aprobar el Manual de Gestión de riesgo operacional; así como sus modificaciones.~~<br>~~f) Conocer los principales riesgos operacionales afrontados por la CPMP.~~ | | Se retiró la sección "Responsabilidades " para que forme parte de la directiva "Política de Gestión de Riesgo Operacional". |

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | ~~g) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.~~<br>~~h) Tener una seguridad razonable de que la CPMP cuenta con una gestión de riesgo operacional, y que los principales riesgos identificados se encuentran bajo control, dentro de los límites establecidos.~~<br>~~5.2. Del Comité de Riesgos~~<br>~~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.~~<br>~~b) Proponer al Consejo Directivo la capacidad, el apetito y los límites de riesgo operacional que la CPMP está dispuesta a asumir en el desarrollo del negocio.~~<br>~~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.~~<br>~~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.~~<br>~~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.~~<br>~~f) Proponer mejoras en la gestión de riesgo operacional.~~<br>~~5.3. De la Gerencia General~~<br>~~a) Asegurar que las actividades de la entidad sean consistentes con la estrategia del negocio, el apetito de riesgo operacional, la cultura y valores corporativos, una adecuada conducta de mercado, y las políticas aprobadas por el Consejo Directivo; así como de informar al Consejo Directivo de manera periódica los resultados de dicho aseguramiento.~~<br>~~b) Implementar la gestión de riesgo operacional conforme a las disposiciones del Consejo Directivo.~~<br>~~c) Informar al Consejo Directivo respecto a nuevos productos y, en general, sobre iniciativas gerenciales relevantes (cambios de sistemas, procesos, modelos de negocios, inversiones sustanciales, etc.), que puedan tener un impacto material en el perfil de riesgo operacional de la entidad.~~<br>~~d) Impulsar la comunicación sobre la gestión de riesgos operacionales en toda la CPMP.~~<br>~~e) Recibir y revisar informes periódicos de las diversas unidades involucradas en la administración del riesgo operacional.~~<br>~~f) Delegar funciones al personal de la entidad y velar por su cumplimiento.~~<br>~~g) Es responsable de la veracidad de la información que proporcione al Consejo Directivo.~~<br>~~5.4. De las unidades orgánicas:~~<br>~~a) Gestionar y administrar el riesgo operacional relacionado al logro de los objetivos de sus respectivas unidades.~~<br>~~b) Asegurar la consistencia entre las operaciones y apetito por riesgo operacional definido por la entidad.~~ | | |

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | ~~c) Asegurar que los roles y responsabilidades que estén relacionados a la gestión de riesgo operacional sean definidos y difundidos claramente en la gerencia.~~<br>~~d) Trasmitir y dirigir las políticas y procedimientos desarrollados para la administración del riesgo operacional.~~<br>~~e) Nombrar a los gestores de riesgo operacional de las unidades a su cargo.~~<br>~~f) Definir planes de acción para tratar el riesgo operacional en caso se considere necesario.~~<br>~~g) Las subgerencias, gerencias y departamentos son responsables de la subcontratación significativa de servicios externos, deberán mantener una comunicación efectiva con el Departamento de Riesgos Operacionales en forma previa y durante los procesos de contratación, para gestionar los riesgos operacionales de dichas subcontrataciones.~~<br>~~h) Asumir, ante el Gerente General, los resultados de la gestión de riesgo operacional correspondiente a su unidad.~~<br>~~5.5. De la Gerencia de Riesgos y Desarrollo~~<br>~~a) Velar por una adecuada gestión de riesgo operacional, promoviendo el alineamiento de la toma de decisiones de la entidad con el apetito de riesgo operacional.~~<br>~~b) Establecer un lenguaje común de gestión de riesgos basado en las definiciones de esta norma y de los demás reglamentos aplicables.~~<br>~~c) 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.~~<br>~~d) Informar trimestralmente al Comité de Riesgos, según sea el caso, los aspectos relevantes de la gestión de riesgos para una oportuna toma de decisiones.~~<br>~~e) Informar trimestralmente 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.~~<br>~~5.6. Del Departamento de Riesgos Operacionales~~<br>~~a) Proponer y elaborar las políticas, procedimientos y metodologías apropiadas para la gestión de riesgo operacional.~~<br>~~b) Participar en el diseño y permanente actualización del Manual de Gestión de Riesgo Operacional.~~<br>~~c) Desarrollar la metodología para la gestión de riesgo operacional.~~<br>~~d) Apoyar y asistir a las demás unidades orgánicas para la aplicación de la metodología de gestión de riesgo operacional, promoviendo el alineamiento de las medidas de tratamiento de los riesgos operacionales con los niveles de apetito y tolerancia aprobadas por el Consejo Directivo.~~<br>~~e) Velar por el cumplimiento de las funciones y responsabilidades asignadas a los gestores de riesgo operacional, gerentes y personal de la~~ | | |

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | ~~CPMP, en relación a la gestión de riesgo operacional.~~<br>~~f) Identificar las necesidades de capacitación y difusión para una adecuada gestión de riesgo operacional por parte de los gestores de riesgo operacional.~~<br>~~g) Administrar la cartera de riesgos operacionales y la base de datos de eventos de pérdida por riesgo operacional.~~<br>~~h) Informar a la Gerencia de Riesgos y Desarrollo, los aspectos relevantes de la gestión de riesgos operacionales, para una oportuna toma de decisiones.~~<br>~~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.~~<br>~~j) Evaluar los riesgos operacionales asociados a cambios importantes en el ambiente de negocio, operativo o informático, y asociados al lanzamiento de nuevos productos, cubriendo 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.~~<br>~~5.7. De los gestores de riesgo operacional~~<br>~~a) Aspectos generales Gestionar los riesgos operacionales que se identifiquen en los procesos que lidera, utilizando la metodología de gestión de riesgo operacional.~~<br>~~b) Aspectos específicos~~<br>~~✓ Desarrollar los reportes e informes sobre la gestión de riesgo operacional en la CPMP.~~<br>~~✓ Mantener una permanente comunicación y coordinación con todo el personal de su unidad orgánica respectiva.~~<br>~~✓ Participar en los programas de capacitación desarrollados por la Gerencia de Riesgos y Desarrollo.~~<br>~~✓ Cumplir con lo siguiente:~~<br>~~▪ Autoevaluación de riesgos y controles~~<br>~~- Ejecutar en la periodicidad establecida las actividades de autoevaluación de los procesos bajo su supervisión.~~<br>~~- Participar en el análisis y evaluación del nivel de exposición de los riesgos operacionales identificados.~~<br>~~- Definir planes de acción para el control de los riesgos operacionales identificados.~~<br>~~- Realizar el seguimiento mensual del avance de los planes de acción y reportarlos al Departamento de Riesgos Operacionales.~~<br>~~▪ Indicador clave de riesgo~~<br>~~- Definir el indicador clave de riesgo.~~<br>~~- Ejecutar en la periodicidad establecida las actividades relacionadas al indicador clave de riesgo, manteniendo la documentación de soporte necesaria que permita a auditoría interna o externa la validación del cálculo y el registro del indicador clave de riesgo.~~<br>~~- Realizar el seguimiento periódico del indicador clave de riesgo y reportarlo al Departamento de Riesgos Operacionales.~~<br>~~▪ Base de datos de eventos de pérdida~~<br>~~Reportar al Departamento de Riesgos Operacionales, los eventos de pérdida~~ | | |

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | ~~presentados en los departamentos bajo su supervisión, enviando la información necesaria para la cuantificación de las pérdidas económicas que se hubieran presentado. Asimismo, el personal informará a través del gestor de riesgo operacional de las unidades orgánicas al Dpto. de Contabilidad y Presupuesto los eventos de pérdida a fin de ser registrados en las cuentas contables, para lo cual deberán remitir y comunicar todos los sustentos.~~<br>~~- Coordinar con los involucrados el establecimiento de los planes de acción para la atenuación de las causas que originan las principales pérdidas.~~<br>~~- Realizar el seguimiento periódico del avance de los planes de acción y reportarlo al Departamento de Riesgos Operacionales.~~<br>~~▪ Nuevos productos y cambios importantes en el ambiente operativo y/o informático~~<br>~~- Enviar la información de nuevos productos, nuevos servicios o cambios importantes en el ambiente operativo e informático, que desarrollen los departamentos bajo su supervisión.~~<br>~~- Participar en la evaluación de riesgos del nuevo producto o cambio significativo.~~<br>~~- Coordinar la definición y ejecución de planes de acción para los riesgos operacionales identificados.~~<br>~~- Realizar el seguimiento y reportar el avance de los planes de acción de Riesgo Operacional.~~<br>~~5.8. De todo el personal:~~<br>~~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.~~<br>~~b) Informar a los gestores de riesgo operacional, la existencia de cualquier evento que signifique un riesgo operacional, a través de los mecanismos~~<br>~~establecidos y de cumplir con las políticas y procedimientos que se establecen en el presente manual.~~ | | |
| | **~~CAPÍTULO II: POLÍTICAS DE RIESGO OPERACIONAL~~** | | |
| 1. DISPOSICIONES GENERALES | ~~1.1. 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 que la gestión de riesgo operacional se realice con líneas muy definidas de responsabilidad, evaluación y reporte.~~<br><br>~~1.2. Establecer una cultura organizacional que promueva prácticas adecuadas de gestión de riesgos, las cuales para ser efectivas deberán formar parte integral de las actividades regulares de la CPMP.~~<br><br>~~1.3. El Comité de Riesgos y todas las instancias involucradas, deberán revisar anualmente el esquema de administración del riesgo operacional.~~<br><br>~~1.4. Ejecutar programas de capacitación sobre mecanismos de administración del riesgo operacional, con el objetivo de asegurar que el personal cuente con las habilidades y~~ | | Se retiró la sección para que forme parte de la directiva "Política de Gestión de Riesgo Operacional". |

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | ~~experiencia apropiadas y optimizar las actividades de gestión de riesgo operacional de la organización.~~<br><br>~~1.5. Las políticas, procesos, procedimientos y controles establecidos en el presente manual deberán ser cumplidos por todas las unidades orgánicas involucradas de la organización y cada nivel de administración es responsable por la idoneidad y efectividad de los mismos dentro de su competencia.~~<br><br>~~1.6. La Gerencia de Riesgos y Desarrollo propone al Comité de Riesgos el apetito de riesgo operacional de acuerdo al perfil de riesgo establecido por la CPMP.~~<br><br>~~1.7. La Gerencia de Riesgos y Desarrollo identifica y evalúa el riesgo operacional de todos los productos, actividades, procesos y sistemas relevantes; debiendo también asegurarse que antes del lanzamiento de nuevas productos y cambios significativos se evalúe los riesgos operacionales si fuera el caso.~~<br><br>~~1.8. Realizar reportes trimestrales al Comité de Riesgos sobre la gestión de riesgo operacional.~~ | | |
| 2. DISPOSICIONES ESPECÍFICAS | ~~2.1. Proveedores críticos y subcontratación significativa~~<br><br>~~2.1.1. Se debe gestionar los riesgos asociados a los proveedores críticos y a la subcontratación significativa, considerando normas y procedimientos relacionados a la evaluación de proveedores, mecanismos de subcontratación y procedimientos del nivel de prestación de servicio.~~<br><br>~~2.1.2. 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 que garanticen una clara asignación de responsabilidades, debiendo establecer cláusulas de riesgo operacional en dichos contratos y en los casos que corresponda.~~<br><br>~~2.2. Base de datos y eventos de pérdida~~<br><br>~~2.2.1. 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.~~<br><br>~~2.2.2. Los eventos de pérdida mayores a mil soles (S/ 1,000.00) deberán ser registrados en la base de datos de eventos de pérdida y deberán contar con documentos de sustento. Asimismo, deberán contar con un plan de acción, en caso el nivel del riesgo operacional asociado lo requiera.~~<br><br>~~2.2.3. Todos los eventos de riesgo operacional, deben ser reportados y registrados de acuerdo a los procedimientos establecidos en el presente manual.~~ | | Se retiró la sección para que forme parte de la directiva "Política de Gestión de Riesgo Operacional". |

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | ~~2.3. Sistema de incentivos~~<br><br>~~2.3.1. La CPMP debe contar con un sistema de incentivos para fortalecer la gestión de riesgo operacional.~~<br><br>~~2.3.2. La evaluación del desempeño de los gestores de riesgo operacional se realizará una (1) vez al año en coordinación con la Gerencia de Riesgos y Desarrollo; los resultados serán comunicados al Departamento de Recursos Humanos.~~<br><br>~~2.3.3. Los incentivos serán no monetarios: Entrega de reconocimientos o premios, por haber realizado una gestión destacada durante el periodo de evaluación, lo cual estará a cargo del Departamento de Recursos Humanos.~~<br><br>~~2.4. Autoevaluación de riesgos y controles~~<br><br>~~2.4.1. La CPMP debe contar con una base de riesgos, en función a la identificación de los riesgos operacionales de cada proceso.~~<br><br>~~2.4.2. El Departamento de Riesgos Operacionales en coordinación con los gestores de riesgo operacional, debe desarrollar los talleres de auto evaluación para cada uno de los procesos de la CPMP. La revisión de cada proceso se deberá realizarse con una periodicidad anual.~~<br><br>~~2.4.3. Todo producto o servicio que requiera ser implementado o modificado sustancialmente, debe ser evaluado utilizando la metodología establecida para las autoevaluaciones de riesgos.~~<br><br>~~2.5. Indicador clave de riesgo~~<br><br>~~2.5.1. Cuando se identifique un riesgo residual con nivel de exposición alto, dentro del proceso de autoevaluación de riesgos y controles, se deberá definir, e implementar un indicador clave de riesgo, que deberá ser monitoreado por un periodo de seis (6) meses, periodo que puede ser extendido en caso sea necesario.~~<br><br>~~2.5.2. Todos los indicadores clave de riesgos, deben ser definidos, implementados, registrados, reportados y monitoreados de acuerdo a los procedimientos establecidos en el presente manual.~~<br>~~2.6. Requerimiento de información~~<br><br>~~2.6.1. La CPMP debe presentar a la Superintendencia de Banca, Seguros y AFP, 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 Superintendencia de Banca, Seguros y AFP.~~ | | |

<table>
<tr><th colspan="4">MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 “MANUAL DE GESTIÓN DE RIESGO OPERACIONAL”</th></tr>
<tr><th>SECCIÓN</th><th>DCD Nº 13-2023</th><th>MODIFICACIÓN</th><th>COMENTARIOS</th></tr>
<tr><td></td><td>~~2.6.2. La CPMP debe presentar a la Superintendencia de Banca, Seguros y AFP, copia de los informes de riesgos por nuevos productos o cambios importantes en el ambiente de negocios, operativo o informático, dentro de los diez (10) días hábiles de presentados al Comité de Riesgos que haya evaluado dicho informe.~~<br><br>~~2.6.3. La CPMP debe designar un funcionario responsable por la información a ser reportada a través del IG-ROp, del portal supervisado por la Superintendencia de Banca, Seguros y AFP. El funcionario responsable deberá corresponder al Gerente de Riesgos y Desarrollo o funcionario principal, según las disposiciones de la Circular G-213-2021.~~<br><br>~~2.6.4. La CPMP debe tener a disposición de la Superintendencia de Banca, Seguros y AFP, toda la información de sustento de la gestión de riesgo operacional.~~<br><br>~~2.6.5. El Comité de Riesgos informa al Consejo Directivo sobre la exposición al riesgo operacional de la CPMP, en los informes periódicos que presentará a esa instancia.~~</td><td></td><td></td></tr>
<tr><th colspan="4">CAPÍTULO II: METODOLOGÍA</th></tr>
<tr><td>3. AUTOEVALUACIÓN DE RIESGOS Y CONTROLES</td><td>(…)<br>3.3. Identificación de riesgos<br>(…)<br><br>3.4.2. Evaluación de controles<br>(…)<br>Tabla N° 1: Calificación del diseño de control<br><table><tr><th>Condiciones</th><th>Alternativas (*)</th><th>Peso ponderado</th></tr><tr><td rowspan="3">Funcionalidad</td><td>Manual</td><td>6 %</td></tr><tr><td>Semiautomático</td><td>10 %</td></tr><tr><td>Automático</td><td>30 %</td></tr><tr><td rowspan="3">Persona que realiza el control</td><td>La misma persona encargada de la operación o proceso.</td><td>0 %</td></tr><tr><td>Es una persona diferente, pero de la misma unidad orgánica</td><td>4 %</td></tr><tr><td>Es una persona de un unidad orgánica distinta</td><td>8 %</td></tr><tr><td rowspan="2">Alcance del control</td><td>Se revisa una muestra</td><td>4 %</td></tr><tr><td>Se revisa todas las operaciones /transacciones / documentos</td><td>8 %</td></tr><tr><td rowspan="3">Documentación del control (procedimientos)</td><td>No Documentado</td><td>0 %</td></tr><tr><td>Documento interno de la unidad orgánica (no oficial)</td><td>4 %</td></tr><tr><td>Documento formal</td><td>6 %</td></tr><tr><td rowspan="2">Tipo</td><td>Detectivo</td><td>4 %</td></tr><tr><td>Preventivo</td><td>30 %</td></tr><tr><td rowspan="2">Evidencia</td><td>No deja evidencia</td><td>0 %</td></tr><tr><td>Deja evidencia</td><td>8 %</td></tr><tr><td>Total (**)</td><td></td><td></td></tr></table></td><td>(…)<br>3.3. Identificación de riesgos<br>(…)<br>3.3.2.4. Análisis de directivas internas.<br>(…)<br>3.3.3. En caso se identifique que los procesos y/o directivas no recogen las actividades que se realizan en la actualidad, según lo relevado por el gestor, se recomienda la actualización de dichos documentos.<br>3.4.2. Evaluación de controles<br>(…)<br>Tabla Nº 1: Calificación del diseño de control<br><table><tr><th colspan="4">Calificación del diseño de control</th></tr><tr><th rowspan="2">Atributo</th><th rowspan="2">Opciones</th><th colspan="2">¿El control puede ser automatizado?</th></tr><tr><th>Sí</th><th>No</th></tr><tr><td rowspan="3">Funcionalidad</td><td>Manual</td><td>6 %</td><td>30 %</td></tr><tr><td>Semiautomático</td><td>15 %</td><td>-</td></tr><tr><td>Automático</td><td>30 %</td><td>-</td></tr><tr><td rowspan="3">Persona que realiza el control</td><td>La misma persona encargada de la operación o proceso.</td><td>0 %</td><td>0 %</td></tr><tr><td>Es una persona diferente, pero de la misma unidad orgánica</td><td>2 %</td><td>2 %</td></tr><tr><td>Es una persona de una unidad orgánica distinta</td><td>8 %</td><td>8 %</td></tr><tr><td rowspan="2">Alcance del control</td><td>Se revisa una muestra</td><td>2 %</td><td>2 %</td></tr><tr><td>Se revisa todas las operaciones /transacciones / documentos</td><td>6 %</td><td>6 %</td></tr><tr><td rowspan="3">Documentación del control (directivas)</td><td>No documentado</td><td>0 %</td><td>0 %</td></tr><tr><td>Documento interno del área (no oficial)</td><td>2 %</td><td>2 %</td></tr><tr><td>Documento formal</td><td>6 %</td><td>6 %</td></tr><tr><td rowspan="2">Tipo</td><td>Detectivo</td><td>4 %</td><td>4 %</td></tr><tr><td>Preventivo</td><td>10 %</td><td>10 %</td></tr><tr><td rowspan="2">Evidencia</td><td>No deja evidencia</td><td>0 %</td><td>0 %</td></tr><tr><td>Deja evidencia</td><td>18 %</td><td>18 %</td></tr><tr><td rowspan="2">Frecuencia</td><td>El control no se ejecuta cada vez que se realiza la actividad de riesgo</td><td>1 %</td><td>1 %</td></tr><tr><td>El control se ejecuta cada vez que se realiza la actividad de riesgo</td><td>4 %</td><td>4 %</td></tr><tr><td rowspan="2">Idoneidad técnica</td><td>Persona que realiza el control no es idónea</td><td>0 %</td><td>0 %</td></tr><tr><td>Persona que realiza el control es idónea</td><td>4 %</td><td>4 %</td></tr><tr><td rowspan="3">Rotación de personal</td><td>Cantidad de veces que ha sido cubierta la posición en el año con personal nuevo: Más de una (1) vez</td><td>0 %</td><td>0 %</td></tr><tr><td>Cantidad de veces que ha sido cubierta la posición en el año con personal nuevo: una (1) vez</td><td>1 %</td><td>1 %</td></tr><tr><td>Cantidad de veces que ha sido cubierta la posición en el año con personal nuevo: cero (0) veces</td><td>4 %</td><td>4 %</td></tr><tr><td>Total</td><td>90%</td><td></td><td></td></tr></table><br>Los resultados correspondientes al análisis, clasificación y tratamiento de los riesgos se registran en la matriz de riesgos operacionales.</td><td>Se actualizó la sección “Autoevaluación de riesgos y controles”.<br><br>Se precisó que la metodología actualizada utiliza como referencia los principios de la ISO 31000.</td></tr>
</table>

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | 3.6. Tratamiento de riesgos<br>(…) | 3.6. Tratamiento de riesgos<br>(…)<br>**Los resultados correspondientes al análisis, clasificación y tratamiento de los riesgos se registran en la matriz de riesgos operacionales.**<br>**Los procesos o sus modificaciones en el ambiente operativo y tecnológico, deben ser evaluados utilizando la metodología establecida para las autoevaluaciones de riesgos y los resultados deben ser presentados al Comité de Riesgos.**<br>(…) | |
| 4. INDICADOR CLAVE DE RIESGO | 4.1. Definición del indicador clave de riesgo<br>~~a) Cuando se identifique un riesgo residual con nivel de exposición alto, dentro del proceso de Autoevaluación de Riesgos y Controles, se deberá definir e implementar un indicador clave de riesgo.~~<br>(…) | 4.1. Definición del indicador clave de riesgo<br>**4.1.1. Un indicador clave de riesgos se debe definir e implementar cuando se presente alguna de las siguientes situaciones:**<br>**4.1.1.1. Riesgos con nivel inherente alto y extremo.**<br>**4.1.1.2. Riesgos que mantienen un nivel residual moderado posterior a la implementación de planes de acción.**<br>**4.1.1.3. Riesgos con nivel residual moderado con una frecuencia igual o mayor a seis (6) veces al año.**<br>**El indicador clave de riesgo debe ser monitoreado por un periodo de seis (6) meses, periodo que puede ser extendido en caso sea necesario.**<br>(…) | Se actualizó la sección "Indicador clave de riesgo". |
| 5. BASE DE DATOS DE EVENTOS DE PÉRDIDA (BDEP) | (…)<br>5.1. Recolección de datos internos de eventos de pérdida<br>~~a)~~ Criterios generales<br>(…) | (…)<br>**5.1. Recolección de datos internos de eventos de pérdida**<br>**5.1.1. Criterios generales**<br>(…)<br>**5.1.1.6. El registro en la base de datos de eventos de pérdida solo se lleva a cabo cuando la pérdida se refleje en las cuentas contables.**<br>**5.1.1.7. Para los eventos de pérdida que superen el umbral definido de acuerdo al apetito de riesgos, se debe elaborar un informe, el cual debe contener como mínimo la causa del evento, una descripción del modo en que se produjo el evento, la unidad orgánica que originó la pérdida, el riesgo asociado y las acciones adoptadas para mitigar la ocurrencia de eventos similares a futuro.** | Se actualizó la sección "Base de datos de eventos de pérdida (BDEP)". |
| 7. SERVICIO SIGNIFICATIVO Y SUBCONTRATACIÓN SIGNIFICATIVA | 7.1. Etapas del proceso de evaluación de ~~proveedores~~<br>~~a)~~ (…)<br>~~b)~~ El Departamento de Riesgos Operacionales hace un cruce de información mensual de las propuestas de contratación de servicio remitidas por los gestores de riesgos con la base de datos del Departamento de ~~Logística~~ (pedidos de servicio).<br>~~c) El Departamento de Riesgos Operacionales apoya a los gestores de riesgos en la evaluación de riesgos.~~<br>~~d) Los gestores de riesgos son responsables de verificar que se incluyan en los contratos, las cláusulas de riesgo operacional necesarias.~~<br>~~e) Para identificar si un pedido de servicio corresponde a una subcontratación significativa, primero se analiza si el servicio a contratar es una subcontratación, de acuerdo a su definición. De ser afirmativo, corresponde~~ | **7.1. Etapas del proceso de evaluación**<br>**7.1.1.** (…)<br>**7.1.2.** El Departamento de Riesgos Operacionales hace un cruce de información mensual de las propuestas de contratación de servicio remitidas por los gestores de riesgos con la base de datos del Departamento de **Contrataciones** (pedidos de servicio).<br>**7.1.3.** Para identificar si un pedido de servicio corresponde a un **servicio significativo, se debe completar un cuestionario, que agrupa 4 criterios, para calificar el servicio. De acuerdo a la calificación obtenida, será catalogado como servicio significativo, servicio importante o servicio no significativo:** | Se actualizó la sección "Servicio significativo y subcontratación significativa", y se agregaron precisiones respecto al servicio significativo. |

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | ~~realizar una evaluación con los siguientes criterios mencionados por la SBS en la Circular SBS Nº G-165-2012:~~<br><br>~~Ítem Criterio de evaluación~~<br>~~C1 Afecta Ingresos~~<br>~~C2 Afecta Solvencia~~<br>~~C3 Afecta Continuidad Operativa~~<br><br>~~De confirmarse que se trata de una subcontratación significativa, deberá realizarse una autoevaluación de riesgos y controles según lo desarrollado en el numeral 3 del capítulo III. Asimismo, se deben incluir en el contrato las cláusulas que figuran en los anexos 5, 6.~~ | **Cuadro: Cuestionario para la identificación de servicios significativos**<br>**Identificación de Servicios Significativos**<br>Gerencia o unidad solicitante:<br>Proveedor:<br>Descripción del servicio:<br>Criterios / Marque con X<br>1. INGRESOS — Nivel de ingresos que la empresa dejaría de generar en caso de interrupción o suspensión del servicio: a. Menor igual a S/ 14000; b. Mayor a S/ 14000 hasta S/ 49000; c. Mayor a S/ 49000 hasta S/ 97000; d. Mayor a S/ 97000<br>2. CONTINUIDAD OPERATIVA — Impacto en la continuidad de los procesos críticos en caso de interrupción o suspensión del servicio: a. No interrumpe ningún macroproceso crítico; b. Interrumpe a uno o más macroprocesos críticos<br>3. REPUTACIÓN — Impacto en la reputación de la entidad en caso de interrupción o suspensión del servicio: a. No impacta en la reputación de la entidad; b. Impacta parcialmente en la reputación de la entidad (genera incomodidad, reclamos o …; c. Impacta seriamente en la reputación de la entidad (difusión en redes sociales u otros medios informativos)<br>4. SEGURIDAD DE LA INFORMACIÓN — Impacto en la Seguridad de la Información de la entidad, considerando la información a la que se tiene acceso a partir del servicio: a. No afecta a la confidencialidad, integridad o disponibilidad de información confidencial; b. Afecta a la confidencialidad, integridad o disponibilidad de información confidencial<br>Calificación / Criterio de evaluación: > 2 Servicio significativo; < 1.5, 2 ] Servicio importante; < 0, 1.5 ] Servicio no significativo<br>**7.1.4. Si el servicio a contratar corresponde a un servicio significativo, se deben incluir en el contrato las cláusulas que figuran en los anexos 5, 6 y se debe realizar una autoevaluación de riesgos y controles, en coordinación con los Gestores de Riesgo Operacional, según lo desarrollado en el numeral 3 del capítulo III, cuyos resultados deben ser presentados en Comité de Riesgos.**<br>**7.1.5. En caso de que el servicio significativo sea provisto por un tercero bajo la modalidad de subcontratación, la subcontratación se considera significativa y como tal, se debe remitir una copia de los informes de resultados a la SBS, dentro de los 10 días hábiles de presentados al Comité de Riesgos.**<br>**7.1.6. Los gestores de riesgos son responsables de verificar que se incluyan en los contratos, las cláusulas de riesgo operacional necesarias.** | |
| 8. SISTEMA DE INCENTIVOS | (…)<br>~~8.1. Evaluación~~<br>~~a) Las calificaciones se obtienen evaluando la aplicación de las metodologías y buenas prácticas en la gestión de riesgo operacional:~~<br>~~▪ Autoevaluación y Control de Riesgos – RCSA~~<br>~~▪ Evaluación en Eventos de Pérdida~~<br>~~▪ Iniciativas de mejora en la Gestión de Riesgo Operacional~~<br>~~b) Cada una de las metodologías tiene tres (3) criterios de calificación, estas son:~~<br>~~▪ Autoevaluación y Control de Riesgos – RCSA~~<br>~~- Oportunidad en la entrega de la información:~~<br>~~Descripción Valor~~<br>~~Dentro del plazo según cronograma de actividades 3~~<br>~~Fuera del plazo según cronograma de actividades 2~~<br>~~No presenta información 1~~<br>~~- Consistencia o calidad de la información:~~<br>~~Descripción Valor~~<br>~~Información suficiente y consistente como evidencia de desarrollo de actividad o control 3~~<br>~~Información insuficiente como evidencia de desarrollo de actividad o control 2~~<br>~~No muestra información como evidencia de actividad o control 1~~<br>~~Grado de implementación de los planes de acción de riesgo identificado:~~<br>~~Descripción Valor~~<br>~~Implementado dentro del plazo original 3~~<br>~~Implementado dentro del plazo reprogramado 2~~<br>~~No implementado y vencido 1~~ | **8.1. Lineamientos**<br>**8.1.1.** La evaluación para la aplicación de incentivos es realizada por la Gerencia de Riesgos y Desarrollo en forma anual con la finalidad de premiar al mejor gestor de riesgo operacional.<br>(…)<br>**8.2. Criterios de evaluación**<br>**Para la evaluación de desempeño de los gestores de riesgo operacional se considerará una calificación máxima de 20 puntos, los cuales se distribuirán entre los criterios que se presentan en la siguiente tabla. Asimismo, se muestra el puntaje por cada criterio y gestión (Gestión de Riesgo Operacional, Gestión de Continuidad del Negocio y Gestión de Seguridad de la Información y Ciberseguridad).**<br><br>Nº / Criterios / Peso / Calificación / Descripción / Puntaje / Gestiones (RO, SI, CN)<br>1 Autoevaluación de Riesgos 15%: Cumplió — El Gestor atiende el requerimiento de información en el plazo establecido y participa en las actividades de acuerdo lo planificado. — 3 — 1 1 1; Cumplió Parcialmente — El Gestor atiende el requerimiento de información en el plazo establecido o participa en las actividades de acuerdo lo planificado. — 1.5 — 0.5 0.5 0.5; No cumplió — 0 — 0 0 0<br>2 Reporte de eventos de pérdida / incidentes 15%: Cumplió — El Gestor reporta el evento de pérdida en el plazo establecido. — 3 — 1 1 1; No cumplió — El Gestor reporta el evento de pérdida fuera del plazo establecido. — 0 — 0 0 0<br>3 Cumplimiento de Planes de acción 15%: Implementado — El Gestor implementa los planes de acción en la fecha programada — 3 — 1 1 1; No implementado — - — 0 0 0 0<br>4 Participación en las capacitaciones 15%: Participó — El Gestor participa en las capacitaciones programadas. — 3 — 1 1 1; No participó — 0 — 0 0 0<br>5 Reporte de indicadores claves de riesgo 10%: Reportó — El Gestor atiende el requerimiento de información en el plazo establecido. — 2 — 2 - -; No reportó — 0 — 0 0 0<br>6 Participación en las pruebas de Continuidad del Negocio 15%: Participó — El Gestor participa en las pruebas programadas. — 3 — - - 3; No participó — 0 — 0 0 0<br>7 Cumplimiento del Inventario de Activos de Información 15%: Cumplió — El Gestor brinda conformidad el inventario de activos en el plazo establecido — 3 — - 3 -; No cumplió — 0 — 0 0 0<br>**De no aplicar un criterio en un periodo** | Se actualizó la sección "Sistema de incentivos". |

| MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD Nº 13-2023 "MANUAL DE GESTIÓN DE RIESGO OPERACIONAL" | | | |
|---|---|---|---|
| **SECCIÓN** | **DCD Nº 13-2023** | **MODIFICACIÓN** | **COMENTARIOS** |
| | ~~Evaluación en Eventos de Pérdida~~<br>~~- Oportunidad en la entrega de la información:~~<br>~~Descripción Valor~~<br>~~Hasta el 5to día hábil del cierre de mes 3~~<br>~~Hasta el 10mo día hábil del cierre del mes 2~~<br>~~No entrega 1~~<br>~~Consistencia o calidad de la información:~~<br>~~Descripción Valor~~<br>~~Información suficiente y consistente como evidencia de identificación de pérdida 3~~<br>~~Información insuficiente como evidencia de identificación de pérdida 2~~<br>~~No muestra información como evidencia de identificación de pérdida 1~~<br>~~Grado de implementación de los planes de acción a evento de pérdida identificado:~~<br>~~Descripción Valor~~<br>~~Implementado dentro del plazo original 3~~<br>~~Implementado dentro del plazo reprogramado 2~~<br>~~No implementado y vencido 1~~<br>~~Iniciativas de mejora en la Gestión de Riesgo Operacional~~<br>~~Las iniciativas de mejora en la gestión de riesgo operacional no tienen carácter obligatorio, pero si estas fueran presentadas por los gestores de riesgos, son evaluadas y calificadas por el Departamento de Riesgos Operacionales, en función al valor agregado a la gestión de riesgo operacional, en una escala ordinal de 1 a 3.~~<br>~~8.2. El Departamento de Riesgos Operacionales realiza la evaluación a los gestores de riesgo operacional.~~<br>~~8.3. El Departamento de Riesgos Operacionales realiza capacitaciones en forma anual dirigida a todo el personal de la CPMP y a los gestores de riesgo operacional.~~<br>~~8.4. La CPMP otorga incentivos no monetarios de reconocimiento o premios a los gestores de riesgo operacional de las unidades orgánicas que hayan destacado en la gestión de riesgo operacional.~~<br>~~8.5. Los gestores de riesgo operacional deben obtener como mínimo una calificación de 1.5, en caso sea inferior se comunicará al gerente de la unidad orgánica a fin de coordinar planes de acción para mejorar su desempeño.~~ | **determinado el puntaje de dicho criterio es distribuido entre los demás criterios. Asimismo, de no aplicar un criterio para una gestión los puntos de dicho criterio serán distribuidos entre las demás gestiones.**<br>**8.3. Penalidades**<br>**En caso de presentarse las siguientes situaciones se penalizará con un (1) punto menos a la calificación total del Gestor de Riesgo Operacional en el periodo evaluado.**<br>**8.3.1. Indicadores claves de riesgos: El mantener indicadores fuera del umbral esperado por más de dos periodos consecutivos.**<br>**8.3.2. Eventos de pérdida por riesgo operacional: El presentarse un evento de perdida, a pesar de haber implementado un plan de acción para evitar recurrencia.**<br>**8.3.3. Pruebas de Continuidad: La reprogramación injustificada de las pruebas de continuidad del negocio.**<br>**Planes de acción: La reprogramación injustificada de los planes de acción o mantener planes en estado vencido.** | |
| **CAPÍTULO III: ANEXOS** | | | |
| **ANEXOS** | | • **Anexo 1: Tipos de eventos de pérdida por riesgo operacional**<br>• **Anexo 2: Árbol de decisiones para determinar el tipo de evento de pérdida por riesgo operacional.**<br>• **Anexo 3: Lista no limitativa de recuperaciones relacionadas a los eventos de pérdida de riesgo operacional.**<br>• **Anexo 4: Lista no limitativa de eventos con pérdidas múltiples.**<br>• **Anexo 5: Cláusula de riesgo de operación.**<br>**Anexo 6: Cláusula de seguridad de información.** | Se agregó la sección "Anexos". |

Nota: Para la elaboración del cuadro comparativo, se ha considerado lo siguiente:

- El orden de la comparación es en base a la nueva propuesta.
- Negrita: Lo que se ha agregado en la nueva propuesta.
- Tachado: Lo que se ha eliminado en la nueva propuesta.
- Subrayado: Cambios en signos de puntuación.