



MANUAL DE GESTION DE RIESGOS OPERACIONALES

LIMA, MARZO DEL 2022

1. INTRODUCCION

El presente manual describe un conjunto de políticas, metodologías y procedimientos que permiten una adecuada gestión de los riesgos operacionales a los cuales se encuentra expuesta SERVIPERU con el objetivo de identificarlos, evaluarlos y mitigarlos.

2. OBJETIVO

Establecer las políticas, metodologías y procedimientos para realizar una adecuada gestión del Riesgo Operacional que enfrenta SERVIPERU.

3. BASE LEGAL

Acuerdo de Consejo de Administración de fecha 31 de marzo de 2017.

4. ALCANCE

El presente Manual es de aplicación para todas las Gerencias y/o Jefaturas de SERVIPERU así como la Dirección de la clínica.

5. RESPONSABILIDADES

La Unidad de Riesgos es la responsable de gestionar, vigilar, verificar y/o evaluar el Riesgo Operacional siguiendo los lineamientos, metodología y procedimientos definidos en el presente manual. Asimismo, es la responsable de aplicar y vigilar su cumplimiento.

Es responsabilidad de los miembros del Consejo de Administración, Gerente General, Gerentes y Jefes de área, hacer cumplir el presente manual.

6. VIGENCIA

El presente manual entrará en vigencia a partir de la publicación y difusión interna dentro de SERVIPERU, una vez aprobado por el Consejo de Administración.

7. DEROGATORIAS Y/O MODIFICACIONES.-

El presente manual podrá ser actualizado las veces que sea necesario por acuerdo del Consejo de Administración.

8. TERMINOS Y DEFINICIONES.-

Para una mejor comprensión y aplicación del presente manual, es pertinente tener en cuenta la definición y alcance de los términos utilizados en el ámbito de la administración de riesgos.

8.1. 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.

A continuación detallamos algunas definiciones relacionadas al riesgo operacional:

8.1.1. Indicadores de riesgo;

Alarmas tempranas en los sistemas, procesos, productos, gente y el ambiente externo.

8.1.2. Pérdidas

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

8.1.3. Perfil de Riesgo

Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.

8.1.4. Plan de continuidad del negocio

Tiene como objetivo dotar a la empresa de la capacidad de mantener, o de ser el caso recuperar, los principales procesos de negocio dentro de los parámetros previamente establecidos.

8.1.5. Riesgo

Es la posibilidad de que un evento ocurra y afecte en forma adversa el cumplimiento de unos objetivos

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

8.1.7. Riesgo residual

Nivel resultante del riesgo después de aplicar los controles.

8.1.8. Apetito por el riesgo y/o Grado de Exposición al Riesgo

Nivel de riesgo que la empresa está dispuesta a asumir en su búsqueda de rentabilidad y valor.

8.1.9. Tolerancia al riesgo

El nivel de variación que la empresa está dispuesta a asumir en caso de desviación de los objetivos empresariales trazados.

8.1.10. Evento

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.

8.1.11. Evento por riesgo operacional

El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional. Se distingue dos tipos de evento, evento por pérdida financiera y evento por lucro cesante.

8.1.12. Eventos por pérdida financiera

Cualquier impacto negativo registrado en cuentas de resultados o en la situación patrimonial de la Entidad, y que haya sido provocado a consecuencia de cualquier evento de riesgo operacional. La pérdida está constituida por un registro contable contabilizado en cuentas de resultados, en rúbricas de gastos generales y/o cuentas patrimoniales.

8.1.13. Eventos por lucro cesante

Impacto negativo que no trasciende en cuentas de resultados o en la situación patrimonial de la Entidad.

8.1.14. Información

Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

8.1.15. Proceso

Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.

8.1.16. Proceso Crítico

Conjunto de actividades indispensables para la continuidad de las operaciones y servicios que brinda SERVIPERU, cuya falta o ejecución deficiente puede producir no cumplir con los objetivos del proceso, ni con los objetivos estratégicos de SERVIPERU y/o generar pérdidas financieras.

8.1.17. Riesgo legal

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

8.1.18. Nuevo Producto

Producto lanzado por primera vez por la empresa, se considera también un “nuevo producto” cuando se realiza un cambio en un producto existente que modifica su perfil de riesgo

8.1.19. Producto

Bienes y/o servicios brindados por las empresas a sus clientes y usuarios.

8.1.20. Subcontratación

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

8.1.22. Servicios

La actividad o labor que realiza una persona natural o jurídica para atender una necesidad de la entidad, pudiendo estar sujeta a resultados para considerar terminadas sus prestaciones.

8.1.23. Servicios Importantes

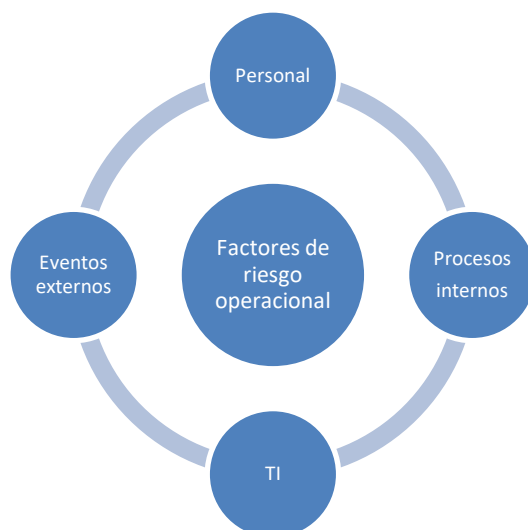
Son aquellos servicios que, en caso de falla o suspensión del mismo, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia o continuidad operativa, este servicio no puede ser desarrollado por la empresa contratante.

8.1.24. Principales Proveedores de Servicios

Son aquellos proveedores cuyos servicios brindados son considerados como subcontrataciones significativas o servicios importantes cuya suspensión o falla puede poner en riesgo las actividades de SERVIPERU.

8.2. FACTORES QUE ORIGINAN EL RIESGO OPERACIONAL

Los factores de riesgo, son aquellas fuentes generadoras de eventos, internas o externas, que pueden originar pérdidas en las operaciones o afectar el cumplimiento de los objetivos estratégicos y/o operativos de SERVIPERU.



8.2.1. Personal

Las empresas deben gestionar apropiadamente los 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.

8.2.2. Procesos internos

Las empresas deben gestionar apropiadamente los 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 los mismos.

8.2.3. Tecnología de información (TI)

Las empresas deben gestionar los 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 los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

8.2.4. Eventos externos

Las empresas deberán gestionar los 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.

8.3. CLASIFICACIÓN DE LOS RIESGOS OPERATIVOS

Un evento es un incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado, ocasionado por diferentes causas y que puede conllevar consecuencias positivas o negativas.

Los eventos por riesgo operacional pueden ser agrupados de la manera descrita a continuación:

8.3.1. Fraude interno

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.

8.3.2. Fraude externo

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.

8.3.3. 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 reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

8.3.4. Clientes, productos y prácticas empresariales

Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos, o de la naturaleza o diseño de un producto.

8.3.5. Daños a activos materiales

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

8.3.6. Interrupción del negocio y fallos en los sistemas

Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

8.3.7. 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.

9. DISPOSICIONES GENERALES

9.1. GENERALIDADES

El Sistema de Gestión del Riesgo Operacional, es un conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional y responsabilidades, registro de eventos por riesgo operativo, órganos de control, plataforma tecnológica, divulgación de la información y capacitación, mediante los cuales la entidad identifica, mide, controla y monitorea el Riesgo Operacional.

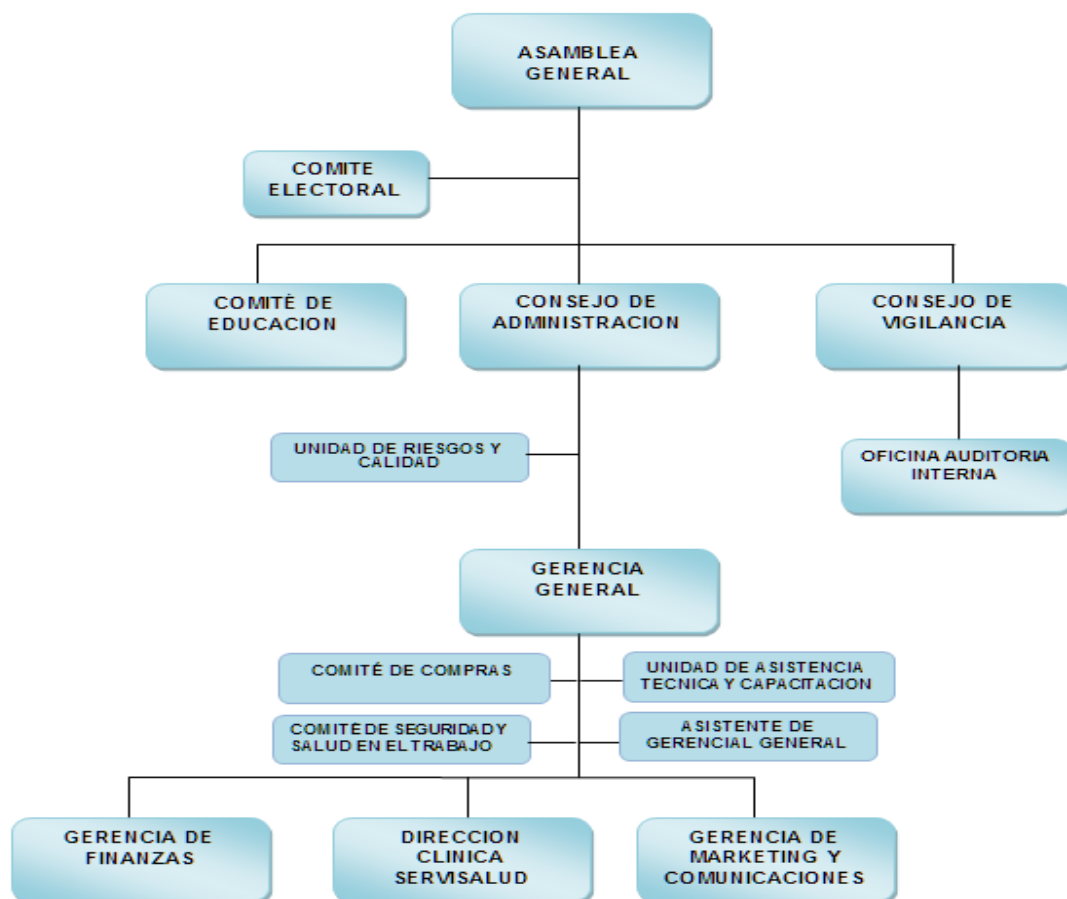
9.2. ESTRUCTURA ORGANIZACIONAL Y RESPONSABILIDADES

9.2.1. Estructura Organizacional

La administración de Riesgo Operacional involucra a todas las unidades de SERVIPERU, cada una de ellas con diversas funciones y responsabilidades que permiten una adecuada gestión de los riesgos operacionales.

SERVIPERU ha definido la siguiente estructura organizacional (ver Cuadro N° 1), para la gestión de riesgos operacionales, así como las funciones y responsabilidades de cada una de las unidades involucradas.

Cuadro N° 1
Estructura Organizacional para la Administración
Del Riesgo Operacional en SERVIPERU



9.2.2. Roles y Responsabilidades

CONSEJO DE ADMINISTRACION

- a. Definir la política general para la gestión del riesgo operacional.
- b. Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiados.
- c. Establecer un sistema de incentivos que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.
- d. Aprobar el manual de gestión del riesgo operacional, el cual incluye las políticas y la organización para la Gestión del Riesgo Operacional, así como las modificaciones que se realicen a los mismos.
- e. Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia y por el riesgo.

- f. Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.
- g. Asegurar que la empresa cuenta con una efectiva gestión del riesgo operacional.

GERENCIA GENERAL

- a. La Gerencia General tiene la responsabilidad de implementar la gestión del riesgo operacional conforme a las disposiciones del Consejo de Administración asignando los recursos necesarios para una adecuada gestión.
- c. Decidir las acciones necesarias para la implementación de las acciones correctivas requeridas, en caso existan desviaciones con respecto a los niveles de tolerancia al riesgo y a los grados de exposición asumidos.
- d. Proponer mejoras en la Gestión del Riesgo Operacional.

GERENCIAS Y DIRECCIÓN DE LA CLÍNICA

- a. Los gerentes y/o jefes de las unidades organizativas y el Director de la clínica tienen la responsabilidad de gestionar el riesgo operacional en su ámbito de acción, dentro de las políticas, límites y procedimientos establecidos, así como fomentar la cultura de la administración del riesgo operacional dentro de su ámbito de acción.

UNIDAD DE RIESGOS Y CALIDAD

La unidad de Riesgos y Calidad deberá cumplir con las siguientes funciones:

- a. Proponer políticas para la gestión del riesgo operacional.
- b. Participar en el diseño y permanente actualización del Manual de Gestión del Riesgo Operacional.
- c. Desarrollar la metodología para la gestión del riesgo operacional.
- d. Coordinar con las demás unidades organizativas de la empresa para la aplicación de la metodología de gestión del riesgo operacional.
- e. Informar a la Gerencia General sobre los riesgos asociados a nuevos productos y a 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.
- f. Consolidación y desarrollo de reportes e informes sobre la gestión del riesgo operacional por proceso, o unidades de negocio y apoyo.
- g. Identificación de las necesidades de capacitación y difusión para una adecuada gestión del riesgo operacional.
- h. Administrar el registro de eventos de riesgo operacional.

9.3. POLITICAS

Con el fin de asegurar el adecuado funcionamiento del Sistema de Gestión del Riesgo Operacional, se han definido las siguientes políticas:

9.3.1. Del ambiente adecuado de la Gestión de Riesgos

- a. Establecer y fortalecer la estructura organizacional para llevar a cabo la Gestión del Riesgo Operacional teniendo en cuenta los roles y responsabilidades claramente establecidos, que permitan mantener una adecuada gestión de dicho riesgo en SERVIPERU, así como la independencia entre las áreas de negocio y la Unidad de Riesgos para evitar conflictos de intereses.
- b. La responsabilidad inicial de la gestión del riesgo operacional recae en las diferentes Gerencias de la organización, como parte integral del desarrollo de sus actividades de negocio, bajo un criterio de autocontrol, dado que no es responsabilidad únicamente de la Unidad de Riesgos.
- c. Las políticas y procedimientos establecidos en el presente manual deberán ser cumplidos por todas las unidades involucradas de la organización y cada Gerencia es responsable de su cumplimiento dentro de su área de competencia.
- d. Todo el personal de SERVIPERU tiene la responsabilidad y obligación de informar a la Unidad de Riesgos, sobre los riesgos operacionales o los probables eventos de pérdida que podrían generarse.
- e. La Unidad de Riesgos deberá definir la forma y periodicidad con la que se deberá informar al Consejo de Administración, a la Gerencia General y demás Gerencias y/o Jefaturas sobre la exposición del Riesgo Operacional de SERVIPERU y de cada una de las Gerencias y/u Oficinas involucradas en los procesos críticos.
- f. SERVIPERU deberá contar con una base de datos de los eventos por riesgo operacional.
- g. La Unidad de Riesgos debe asegurarse que los riesgos operacionales se traten como información confidencial de SERVIPERU. Cualquier solicitud o entrega de información a terceros debe ser aprobada por la Gerencia General.
- h. El proceso de gestión del riesgo operacional, es un elemento del Control Interno de SERVIPERU.

9.3.2. Gestión del Riesgo Operacional:

- a. Se deberá establecer un plan de trabajo que permita gestionar los riesgos operacionales de SERVIPERU, dicho plan deberá ser actualizado cada año.
- b. Se deberán establecer los criterios necesarios para la administración del riesgo operacional de SERVIPERU.
- c. Para la identificación y evaluación de los riesgos operacionales, se aplicará la metodología descrita en el presente manual.

d. Se deberán desarrollar políticas, procesos y procedimientos para controlar y mitigar el riesgo operacional identificado, debiendo evaluar la viabilidad de estrategias alternativas de control y limitación de los riesgos.

9.3.3. Registro y Control de los Eventos por Riesgo Operacional:

a. Todo el personal de SERVIPERU es responsable de detectar, registrar e informar, mediante **la Data de eventos de pérdida (Anexo N°3) los eventos de pérdida por Riesgo Operacional hasta la suma equivalente a 2UIT dentro de cualquier proceso.**

La pérdida está constituida por un registro contable contabilizado en cuentas de resultados, en rúbricas de gastos generales y/o cuentas patrimoniales. Así mismo, debe de informar al Responsable de Riesgo Operacional.

b. La Unidad de Riesgos es responsable de realizar la evaluación de riesgos operacionales, de acuerdo a la metodología establecida.

c. La Unidad de Riesgos debe de clasificar los eventos por riesgo operacional en base al aspecto que lo origina y el tipo de evento.

d. **Para las pérdidas mayores a 2 UIT**, se deberá abrir un expediente físico o electrónico que contenga información adicional que permita conocer el modo en que se produjo el evento, características especiales y otra información relevante, así como las acciones que hubiera tomado SERVIPERU, incluyendo entre otras, las mejoras o cambios requeridos en sus políticas o procedimientos.

9.3.4. Aprobación de Nuevos Productos o cambios importantes en el ambiente de negocios, operativo e informático.

a. Todo nuevo producto que requiera ser aprobado o todo cambio importante en el ambiente de negocios, operativo o informático, deberá pasar necesariamente por un proceso de Evaluación de Riesgos.

9.3.5. Cumplimiento:

El no cumplimiento de las políticas establecidas en el presente manual, así como la omisión del reporte de incidencias de pérdida por Riesgo Operacional, son consideradas como **falta y serán sancionadas de acuerdo al Reglamento Interno de Trabajo (RIT).**

9.4. METODOLOGIA

9.4.1. Gestión del Riesgo Operacional:

La Gestión de Riesgo Operacional de SERVIPERU consta de las siguientes etapas:

A. Identificación de los Riesgos Operacionales.

B. Análisis y evaluación de los Riesgos Operacionales.

C. Tratamiento/Mitigación de los Riesgos Operacionales.

D. Monitoreo

DI-GG-016

Rev. 1

26/03/2022

Estas etapas son de vital importancia para desarrollar con éxito la gestión del riesgo operacional. Se cuenta con la participación de las personas que ejecutan los procesos, para lograr que las acciones de control alcancen los niveles esperados.

A. Identificación de los Riesgos Operacionales:

En esta etapa se identifican los eventos por riesgo operacional en cada uno de los procesos y procedimientos.

Esta etapa involucra los siguientes aspectos:

1)- Lograr un conocimiento del proceso a evaluar, documentando su perfil de riesgo, de acuerdo al modelo mostrado en el **Anexo N°1**.

En caso el proceso no esté documentado se procederá a realizarlo siendo de responsabilidad del Gerente y/o Jefe del Area.

2) Desarrollar sesiones de trabajo con personal vinculado a los diferentes procesos involucrados aplicando la técnica de lluvia de ideas considerando las siguientes preguntas:

-Qué puede ocurrir que nos haga perder dinero?

-A qué estamos expuestos?

-Qué puede fallar?

-Qué puede ocurrir para no llegar al objetivo?

3)- Identificar los problemas (eventos/riesgos) que pueden afectar el cumplimiento del objetivo del proceso y clasificarlos de acuerdo con las categorías referenciales establecidas en el **Cuadro N°2 y de acuerdo al ítem 8.3 del presente manual**.

**CUADRO N°2
CATEGORIAS REFERENCIALES DE RIESGO OPERACIONAL**

ASPECTO	CODIGO	CATEGORIA DE RIESGO OPERACIONAL
PERSONAS	R001	Actividades no autorizadas
	R002	Robo
	R003	Fraude
	R004	Delito informático
	R005	Relaciones laborales y seguridad en el puesto de trabajo
	R006	Ocultamiento y mal uso de información importante
	R007	Malas prácticas y actos ilegales
	R021	Prácticas inadecuadas de negocio
PROCESOS	R008	Ineficiencia en el diseño de procesos
	R009	Litigios con clientes y/o proveedores
SISTEMAS	R010	Interrupción del negocio
	R011	Fallas en el hardware
	R012	Fallas en el software

EXTERNOS	R013	Daños a activos físicos
	R014	Fraude
	R015	Delitos informáticos
	R016	Competencia
	R017	Mercado
	R018	Legal
	R019	Innovación tecnológica
	R020	Sector

4)- Documentar la información obtenida en una matriz de riesgos de acuerdo al modelo **sugerido en el anexo N°2-A**

B. Análisis y evaluación de los Riesgos Operacionales:

Se realiza de la siguiente manera:

1.-Bajo el supuesto de la no existencia de controles, se determina el **nivel de riesgo absoluto o inherente**:

$$\text{RIESGO ABSOLUTO} = \text{Impacto(I)} \times \text{Probabilidad(P)}$$

Donde:

Probabilidad (P): Es una estimación de la frecuencia con que ocurre un evento (riesgo).

Impacto (I): Es una estimación de la magnitud del daño actual o potencial asociado a un aspecto e impacto ambiental, físico y humano y que puede medirse mediante criterios cualitativos o cuantitativos-

Con esto se pretende conocer el **nivel de daño potencial que tiene el riesgo**.

Para tal efecto SERVIPERU ha desarrollado los siguientes criterios cuantitativos y cualitativos de impacto y probabilidad lo que se detallan en los cuadros N° 3 y 4

CUADRO N°3

IMPACTO: CRITERIOS CUANTITATIVOS/CUALITATIVOS

NIVEL CUANTITATIVO	DESCRIPCION CUALITATIVA	IMPACTO
1	Insignificante	Pérdida menor; -No hay daño a la reputación -,No aumentan las quejas de los clientes, - No hay exposición mediática.
2	Menor	Pérdida moderada, -Daño mínimo a la reputación; -Aumento pequeño en los reclamos de los clientes ;

		- No hay impacto negativo en la situación financiera de la unidad de negocio o de la organización. -Exposición mediática moderada
3	Moderado	Pérdida o daño importante ; -Daño moderado a la reputación -Reclamos de clientes a gran escala; pérdida de algunos clientes -Efecto negativo potencial en la situación financiera de la unidad de negocio o de la organización. -Exposición mediática de mediana dimensión -Posible involucramiento de la Alta Gerencia
4	Mayor	Pérdida o daño mayor, -Daño importante a la reputación - Pérdida importante de clientes - Pérdida en la situación financiera; -Investigación formal del regulador; -Exposición mediática mayor -Involucramiento de la alta Dirección.
5	Catastrófico	Pérdida o daño catastrófico; -Daño mayor a la reputación - Pérdida de clientes a gran escala -Pérdida importante en la situación financiera; -Intervención formal del regulador; -Exposición mediática de grandes dimensiones -Involucramiento directo de la alta Gerencia y Alta Dirección. -Entregas de productos o servicios no conformes,

CUADRO N°4

PROBABILIDAD: CRITERIOS CUANTITATIVOS /CUALITATIVOS

NIVEL CUANTITATIVO	DESCRIPCION CUALITATIVA	IMPACTO
5	Casi seguro	Ocurrirá en la mayoría de las circunstancias
4	Probable	Probablemente ocurrirá en la mayoría de las circunstancias
3	Posible	Puede ocurrir en algún momento
2	Improbable	Podría ocurrir en algún momento
1	Raro	Puede ocurrir en circunstancias excepcionales

Lo que ha permitido diseñar una matriz de evaluación de riesgos (mapa de riesgos) de la organización. (Ver cuadro N°5).

**CUADRO N°5
MATRIZ DE EVALUACION DE RIESGOS**

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi Seguro (5)	A(Alto)	A	E(Extremo)	E	E
Probable (4)	M	A	A	E	E
Posible (3)	B(Bajo)	M(Medio)	A	E	E
Improbable (2)	B	B	M	A	E
Raro (1)	B	B	M	A	A

Los Niveles de riesgo identificados se pueden ver en el cuadro N°6 y son los siguientes:

**CUADRO N°6
NIVELES DE RIESGOS**

SERVIPERU NIVELES DE RIESGO		
NOMENCLATURA	DESCRIPCION	ACCION DE RESPUESTA
E	Extremo	Requieren acción inmediata de la alta dirección
A	Alto	Se necesita atención de la alta dirección
M	Medio	Definir responsabilidades gerenciales
B	Bajo	Aplicar procedimientos rutinarios

ServiPerú ha establecido como política tratar debidamente los riesgos que estén al menos en el nivel medio para arriba.

2. Luego, se identifican **las actividades de control o controles actuales** que se realizan para mitigar el riesgo. Para esto, se consideró lo siguiente:

- Quién hace la actividad y,
- Quién es el responsable de ejecutarla.

Además, para cada control se debe indicar lo siguiente:

- Nombre del manual o texto normativo interno donde se encuentra el control o se hace referencia al mismo.
- La situación de la implementación del control, determinando los siguientes estados:

ESTADO DE SITUACION DE IMPLEMENTACION DEL CONTROL	DETALLE	SEMAFORIZACION
IMP	Implementado. El control se realiza y además está documentado	
IPP	Implementado parcialmente. -El control se encuentra documentado pero no se realiza, o - -Se realiza pero no está documentado	
NINGUNO	No hay control	

La efectividad del diseño de control de acuerdo a los siguientes lineamientos:

EFFECTIVIDAD DE DISEÑO DEL CONTROL	DETALLE	SEMAFORIZACION
DEF	Diseño efectivo que mitiga el riesgo	
DPE	Diseño parcialmente efectivo	
DNE	Diseño no efectivo	

El tipo de control se aborda de acuerdo a las siguientes categorías:

CATEGORIA	TIPO DE CONTROL	DETALLE
1	PREVENTIVO(P)	Ayuda a prevenir el riesgo , generalmente dentro de procedimientos.
	DETECTIVO(R)	Se realiza posterior a la actividad donde puede ocurrir el riesgo
2	MANUAL(M)	Se realiza por personas
	AUTOMATIZADO(A)	Está incorporado dentro de un sistema, el cual lo realiza

3. **Se determina el nivel de riesgo residual o “controlado”**, para lo cual, se realiza la evaluación del riesgo **considerando los controles actuales**, lo que permite analizar qué tan buenos o adecuados son para mitigar el riesgo. Se utilizó los mismos criterios de impacto y probabilidad.

RIESGO RESIDUAL = Impacto x Probabilidad

C. TRATAMIENTO Y MITIGACIÓN DE LOS RIESGOS OPERACIONALES (RESPUESTA AL RIESGO)

Esta etapa implica lo siguiente:

1. Seleccionar los riesgos residuales que están en los niveles, **medio, extremo o alto**, para decidir la respuesta al riesgo:

- Reducir impacto, o nivel de daño
- Reducir probabilidad, o nivel de ocurrencia
- Compartir o transferir, a un tercero
- Aceptar
- Evitar

2. Formular un Plan de Acción para mitigar el riesgo en los casos en que se decidió por reducir o compartir, que incluye el tratamiento elegido, las acciones a realizar, responsables y fechas en que deben ser culminadas. El cumplimiento de estas acciones debe ser monitoreado por la unidad de Riesgos, el mismo que se muestra en el **Anexo N° 2-B**.

3.-Verificación de las acciones tomadas para su revisión, dentro de sus actividades de control anual especificando el nivel de efectividad. Estará a cargo de la unidad de riesgos. Ver **Anexo N° 2-B**.

Al finalizar el proceso tendremos la **MATRIZ DE IDENTIFICACION, EVALUACION DE RIESGOS, PLANES DE ACCION Y VERIFICACION** la misma que se muestra en el **Anexo N°2-A y Anexo 2-B**.

D. MONITOREO DE LA GESTIÓN DE RIESGO OPERACIONAL

El monitoreo es fundamental para vigilar los avances en la gestión del riesgo operacional y lograr una toma de decisiones oportuna sobre los niveles de riesgo, para cada uno de los componentes descritos y en su conjunto.

Existe un monitoreo que se da en el día a día dentro del curso normal de las actividades del negocio, y otro que se da mediante evaluaciones separadas o específicas, para obtener un entendimiento más preciso sobre las deficiencias o puntos de mejora, que una vez superados implementados, permiten el logro de los objetivos de la organización.

Para tener una gestión efectiva y oportuna, es imprescindible contar con un sistema de información, que permita manejar las bases de datos de las evaluaciones realizadas así como de las pérdidas ocurridas.

Los datos que debe contener una base de datos de pérdidas están especificados en el **Anexo N° 3.Data de nuevos eventos de riesgo operacional**.

Las acciones de monitoreo a implementarse serán las siguientes:

PASO	NIVEL JERARQUICO	ACCIONES CLAVES
1	Cada Jefatura/Gerencia	Supervisa las actividades realizadas por el personal operativo de acuerdo al cumplimiento de los procedimientos enfocados en la mitigación de riesgos. Identifica y reporta a la unidad de riesgos las situaciones que incrementan la exposición a riesgos
2	Unidad de riesgo	Analiza y prepara reportes ejecutivos de monitoreo para la Gerencia General y el Consejo de Administración
3	AUDITORIA INTERNA	Prepara informes sobre la gestión de las áreas enfocadas en riesgos.
4	AUDITORIA EXTERNA	Prepara informe sobre el cumplimiento de las normas de gestión de riesgo operacional

ANEXOS

ANEXO N°1 PROCEDIMIENTO

1. OBJETIVO
2. RESPONSABILIDAD
Implementación:

Supervisión:

Ejecución:

3. ALCANCE
4. REFERENCIAS
5. DEFINICIONES
6. DESCRIPCIÓN DEL PROCEDIMIENTO

PASO	RESPONSABLE	DESCRIPCION (ACTIVIDAD)	DOCUMENTO /HERRAMIENTA CLAVE	RIESGO IDENTIFICADO

7. IDENTIFICACIÓN DE RIESGOS Y PELIGROS ASOCIADOS A LA SALUD Y SEGURIDAD EN EL TRABAJO Y RIESGOS Y OPORTUNIDADES ASOCIADAS A LA GESTIÓN DEL PROCESO Y AL PRODUCTO

- 7.1 PELIGROS Y RIESGOS ASOCIADOS A LA SEGURIDAD Y SALUD OCUPACIONAL EN LA IMPLEMENTACION DEL PRESENTE PROCEDIMIENTO

7.1.1. Peligros

7.1.2. Riesgos

7.2 A LA GESTIÓN DEL PROCESO Y AL PRODUCTO

7.2.1 RIESGOS ASOCIADOS AL PROCESO

7.2.2

RIESGO				CONTROLES				
Evento	I	P	Riesgo absoluto	A.control	Propietario	Resp. control	Ref.docu mental	Implementación de planes de acción

7.2.3 OPORTUNIDADES ASOCIADAS AL PROCESO

7.2.4 RIESGOS ASOCIADOS AL PRODUCTO O ELEMENTO DE SALIDA

RIESGO				CONTROLES				
Evento	I	P	Riesgo absoluto	A.control	Propietario	Resp. control	Ref.docu mental	Impleme ntación

7.2.5 OPORTUNIDADES ASOCIADAS AL PRODUCTO O ELEMENTO DE SALIDA(Trasladar a una SAP)

8. MECANISMOS DE CONTROL ESTABLECIDOS A LOS RIESGOS Y PELIGROS ASOCIADOS A LA SALUD Y SEGURIDAD EN EL TRABAJO Y RIESGOS Y OPORTUNIDADES ASOCIADAS A LA GESTIÓN DEL PROCESO Y AL PRODUCTO

8.1. MECANISMOS DE CONTROL ASOCIADOS A LA SEGURIDAD Y SALUD OCUPACIONAL EN LA IMPLEMENTACION DEL PRESENTE PROCEDIMIENTO

8.2. ACCIONES PREVENTIVAS PARA MITIGAR LOS RIESGOS Y APROVECHAR LAS OPORTUNIDADES ASOCIADOS A LA GESTIÓN DEL PROCESO Y AL PRODUCTO

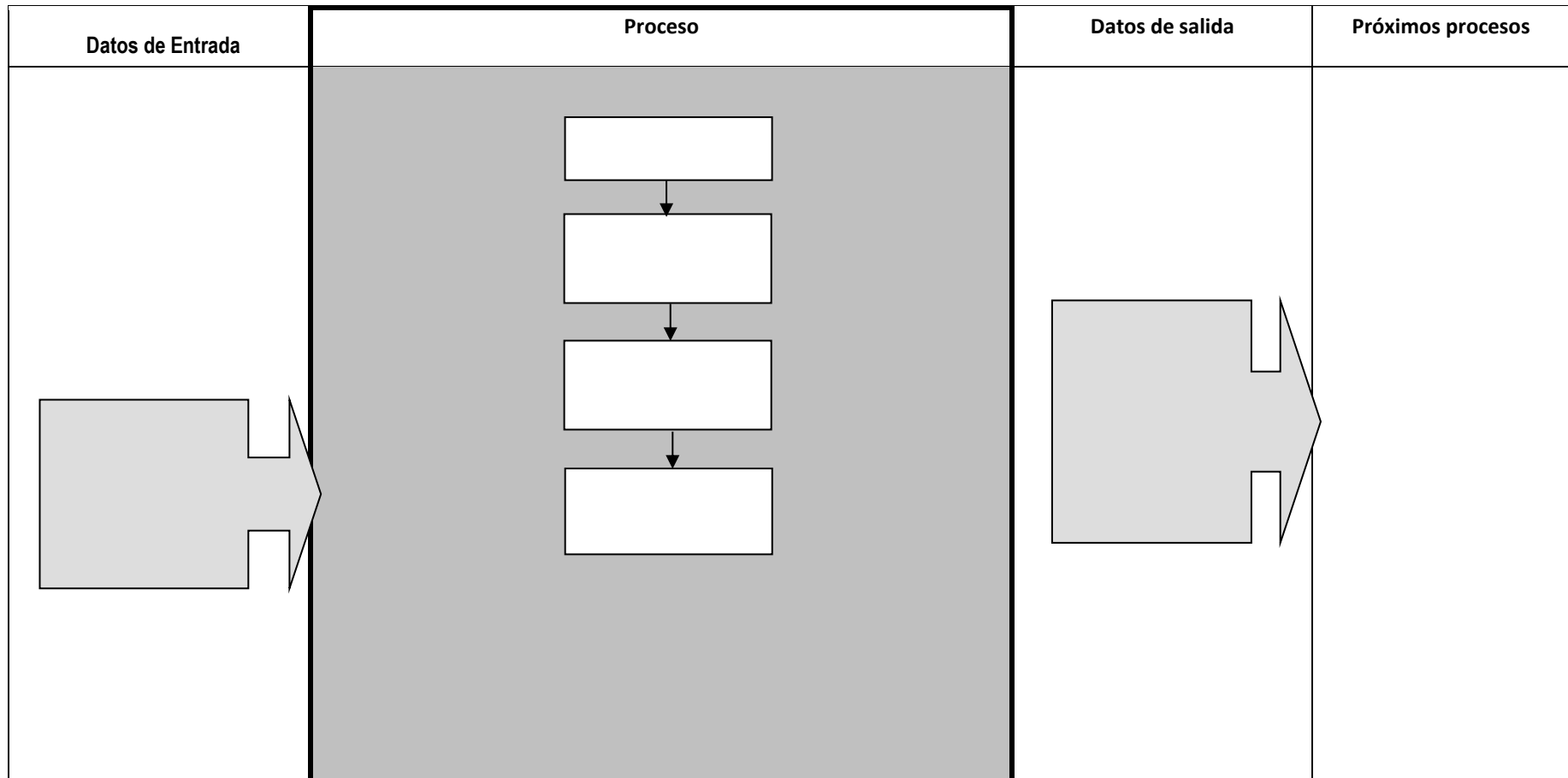
9. MONITOREO Y MEDICION DEL DESEMPEÑO

INDICADOR	META

10. REGISTROS

11. ANEXOS

11.1 Caracterización del proceso



ANEXO N°2-A

MATRIZ DE IDENTIFICACION, EVALUACION DE RIESGOS, PLANES DE ACCION Y VERIFICACION

PROCESO:						DUEÑO DEL PROCESO										
SUB PROCESO/PROCEDIMIENTO:						FECHA DE EVALUACION:										
OBJETIVO:																
I.-RIESGO						II.-CONTROLES										
GRUPO DE ANALISIS DE RIESGOS: Identificación del riesgo						GRUPO DE ANALISIS DE RIESGOS/USUARIO: Mitigación del riesgo										
DESCRIPCION			EVALUACION RIESGO ABSOLUTO			CARACTERISTICAS				SITUACION DE IMPLEMENTACION DEL CONTROL		TIPO DE CONTROL		EVALUACION RIESGO RESIDUAL		
Evento(Peligro)	Categoría de riesgos	Relación con otros riesgos: M,R, E,L	Impacto(I)	Probabilidad(P)	Nivel de Riesgo	A. control/Controles actuales que mitigan el riesgo	Propietario de la actividad	Resp. control	Ref. Documental de soporte a la actividad de control	Estado de Implementación	Efectividad de diseño de control	Preventivo(P) / Detectivo(D)	Manual(M)/Automatizado(A)	Impacto(I)	Probabilidad(P)	Nivel de Riesgo

III.PLAN DE ACCION(Respuesta al riesgo residual)							IV.VERIFICACION DE LAS ACCIONES TOMADAS		
GRUPO DE ANALISIS DE RIESGOS/U.RIESGOS: Tratamiento y gestión del riesgo							U.DE RIESGOS/USUARIO: Resultado alcanzado		
DESCRIPCION				RIESGO ESPERADO			RESULTADO DE LA MITIGACION DEL RIESGO	EVIDENCIAS	
Tratamiento	Acciones de mejora a realizar	Responsable	Fecha de Implementación	Impacto (I)	Probabilidad (P)	Nivel de Riesgo	Se mitigó el riesgo? Si/No	Efectividad de diseño	Documento de soporte

ANEXO N°2-B
PLAN DE RESPUESTA A LA GESTION DE RIESGOS RESIDUALES

MATRIZ DE SEGUIMIENTO

PROCESO:		DUEÑO DEL PROCESO	
PROCEDIMIENTOS		FECHA DE EVALUACION:	

PROCEDIM IENTO	EVENTO DE RIESGO IDENTIFICADO	NIVEL DE RIESGO RELATIVO	ACCIONES DE MEJORA PROPUESTA	HERRAMIENTA/ MEDIO DE VERIFICACIÓN	RESPONSABLE	MONITOREO DE CUMPLIMIENTO 2017-18				
						C: Cumple		P=En proceso		
						NC:No cumple				
MES F.Monit eo:	MES F.Monit oreo:	MES F.Monit oreo:	MES F.Monit oreo:	MES F.Monit oreo:						

ANEXO N°3

DATA DE NUEVOS EVENTOS DE RIESGOS OPERACIONALES

PROCESO:

RESPONSABLE:.....

1.N° DE EVENTO	2.DESCRIPCIÓN DEL EVENTO DE RIESGOS	3 .FECHA DE OCURRENCIA	4.PROCEDIMIENTO INVOLUCRADO	6.PROPIETARIO DE LA ACTIVIDAD (QUIÉN LO EJECUTA?)	6.CAUSA DE OCURRENCIA DEL EVENTO DE RIESGO	7. MONTO ESTIMADO/REAL DE PÉRDIDA	8 . EL MONTO DE PÉRDIDA ESTÁ ASEGURADA?	9 .PÉRDIDA REAL NETA (8-9)	10 .ACCION REALIZADA POR EL RESPONSABLE	11. EL EVENTO ESTÁ INCLUIDO EN LA MATRIZ DE RIESGOS?