

MANUAL DE RIESGO OPERACIONAL

MANUAL DE RIESGO OPERACIONAL

UNIDAD DE RIESGOS

San Salvador, noviembre de 2023

JEN

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

INDICE

1.	OBJETIVO	3
2.	DEFINICIONES	3
3.	ALCANCE	5
4.	RESPONSABILIDADES.....	6
5.	PENSAMIENTO ESTRATÉGICO INSTITUCIONAL.....	6
6.	MARCO NORMATIVO	7
7.	POLÍTICA DE GESTIÓN DE RIESGO OPERACIONAL	8
7.1	Factores de Riesgo	8
7.2	Clasificación de Eventos de Riesgo Operacional	10
7.3	Estructura de gestión de riesgo operacional	11
7.4	Funciones y Responsabilidades para la Gestión de Riesgo Operacional.....	12
7.5	Etapas del Proceso de Gestión de Riesgos.....	14
7.6	Categorías de Eventos de Pérdida	15
8.	METODOLOGÍA PARA LA GESTIÓN DE RIESGO OPERACIONAL	15
8.1	Clasificación de los Eventos de Riesgo.....	15
8.2	Identificación.....	16
8.3	Medición	16
8.4	Control y Mitigación del Riesgo	20
8.5	Monitoreo y comunicación.....	21
9.	PRESTACIÓN DE SERVICIOS POR TERCEROS.....	24
9.1	Riesgo Legal.....	25
10.	PERIODICIDAD DE EVALUACIONES E INFORMES	25
10.1	Informes de seguimiento	25
10.2	Informe Anual	26
11.	SANCIONES.....	26
12.	VIGENCIA	26
13.	ANEXOS.....	27
13.1	Anexo No. 1: Tipos de Eventos por Riesgo Operacional.....	27
13.2	Anexo No. 2: Detalle de Líneas de Negocio	29
13.3	Anexo No. 3: Tabla de contenido de la Base de Datos de Registro de Eventos... ..	30
13.4	Anexo No. 4: Listado de controles tipo para disminuir probabilidad de ocurrencia e impacto.....	31
13.5	Anexo No. 5: Modelo de Plan de Acción y Mitigación.....	32
13.6	Anexo No. 6: Modelo de Matriz de Seguimiento de Riesgos Materializados	33

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

1. OBJETIVO

Fortalecer la gestión de riesgo operacional, estableciendo políticas e implementando metodologías que permitan identificar, medir, controlar y dar seguimiento oportuno a los riesgos a los que está expuesto FONAVIPO, por la naturaleza de sus operaciones.

2. DEFINICIONES

Para efectos del presente Manual de Riesgo Operacional, los términos utilizados se describen a continuación:

- a) **Alta Gerencia:** Dirección Ejecutiva y Jefes de Unidades que reportan a Dirección Ejecutiva y Presidencia.
- b) **Apetito de riesgo:** el nivel y los tipos de riesgos que una entidad está dispuesta a asumir en relación a sus actividades, para alcanzar sus objetivos estratégicos y planes de negocio.
- c) **Director Ejecutivo:** es aquel que ejerce la más alta autoridad administrativa dentro de la entidad, y que además puede formar parte de la Junta Directiva.
- d) **Evento con afectación masiva:** fallas o errores en los procesamientos por lotes que deriva en una afectación a los clientes ya sean propios de la entidad o de otras entidades a las cuales se brinda servicios de procesamiento, tales como: cargos erróneos aplicados en una tarjeta o cuenta durante un procesamiento por lote.
- e) **Evento de riesgo operacional:** es un suceso o serie de sucesos, de origen interno o externo, los cuales incluyen los incidentes ocurridos y eventos potenciales que pudieren generar pérdidas económicas y pueden o no afectar el estado de resultados.
- f) **Factor de riesgo operacional:** es la causa primaria o el origen de un evento operacional, los cuales pueden ser causados por los factores, tales como, procesos, personas, tecnología de información y acontecimientos externos.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

- g) **Junta Directiva:** Órgano colegiado u órgano equivalente encargado de la administración de la entidad, con funciones de supervisión, dirección y control.
- h) **Línea de negocio:** es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios para atender un segmento de mercado objetivo.
- i) **Mapa de riesgos:** es una herramienta que permite presentar una imagen panorámica de los riesgos a los que está expuesta la entidad; independiente de la forma de su presentación, en el que se identifican y se ubican las áreas/actividades/activos (procesos) que podrían verse afectados durante la ocurrencia de un evento adverso. Permite ver las amenazas y medir la magnitud de cada riesgo (probabilidad e impacto económico). Es un instrumento gráfico de gestión de los riesgos que permite comparar los riesgos por su importancia relativa, así como en conjunto, permitiendo a la entidad establecer niveles aceptables de riesgo.
- j) **Perfil de riesgo:** resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.
- k) **Proceso:** Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el usuario, sea interno o externo.
- l) **Procesamiento por lotes:** método de ejecución de tareas de forma repetitiva y en gran volumen en términos de cantidad de operaciones o transacciones.
- m) **Riesgo inherente:** nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- n) **Riesgo operacional:** posibilidad de incurrir en pérdidas debido a fallas en los procesos, en las personas, en los sistemas de información y a causa de acontecimientos externos; incluye el riesgo legal que consiste en la posibilidad de ocurrencia de pérdidas debido a fallas en la ejecución de contratos o acuerdos, al

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

incumplimiento de normas, así como a factores externos tales como cambios regulatorios, procesos judiciales, entre otros.

- o) **Riesgo residual:** nivel resultante del riesgo después de aplicar los controles. Es el riesgo que queda, una vez se han instrumentado los controles pertinentes para su tratamiento. En todo caso exige un permanente monitoreo para observar su evolución.
- p) **Tolerancia al riesgo:** niveles de toma de riesgos aceptables para lograr un objetivo específico o administrar una categoría de riesgo. La tolerancia al riesgo representa la aplicación práctica del apetito por el riesgo y, por lo general, está alineada con categorías de riesgo, como estrategia, finanzas, personas o reputación.
- q) **Riesgo legal:** consiste en la posibilidad de ocurrencia de pérdidas debido a fallas en la ejecución de contratos o acuerdos, al incumplimiento de normas, así como a factores externos tales como cambios regulatorios, procesos judiciales, entre otros.
- r) **Criterio o juicio de experto:** es la opinión referente a la probabilidad de ocurrencia e impacto de un evento de riesgo, que puede brindar el gestor de un proceso y/o profesionales expertos en una disciplina o área de conocimiento.
- s) **Servicios críticos:** son los servicios y actividades definidas por Fonavipo como prioritarios cuya no disponibilidad compromete la existencia de la entidad.
- t) **Ley:** Ley del Fondo Nacional de Vivienda Popular.

3. ALCANCE

El presente Manual de gestión de riesgo es aplicable a todas las operaciones rutinarias y no rutinarias del quehacer de FONAVIPO, las cuales por su naturaleza son susceptibles a diferentes eventos de riesgos.

Dicho Manual contiene las políticas y procedimientos mínimos para gestionar el Riesgo Operacional.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

4. RESPONSABILIDADES

- 4.1 **De la Junta Directiva**, aprobar este Manual.
- 4.2 **De la Unidad de Riesgos**, ejecutar, actualizar, proponer mejoras y modificar este Manual de Riesgo Operacional.
- 4.3 **De los líderes de procesos y gestores de riesgo, jefes**; la ejecución, gestión y cumplimiento de este Manual.

5. PENSAMIENTO ESTRATÉGICO INSTITUCIONAL

5.1 Visión

Ser líderes en facilitar a las familias salvadoreñas de más bajos ingresos el acceso a una solución habitacional integral, por medio de programas que les permitan mejorar su calidad de vida, a través del fortalecimiento financiero institucional.

5.2 Misión

Facilitamos el acceso a soluciones habitacionales integrales a las familias salvadoreñas de más bajos ingresos; mediante programas de subsidios, créditos y desarrollo de proyectos habitacionales que permitan mejorar su calidad de vida.

5.3 Política de Calidad

En FONAVIPO, como una institución financiera autónoma, estamos comprometidos a mejorar continuamente los procesos, para satisfacer a nuestros clientes y partes interesadas, facilitando el acceso a soluciones habitacionales integrales mediante créditos y subsidios.

5.4 Valores Institucionales

Los valores son muy importantes en las bases de la estructura organizacional de una empresa, actúan como principios fundamentales y orientan nuestra forma de ser y actuar en la vida profesional y personal.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

- a) **Solidaridad**, porque apoyamos el esfuerzo de las familias para solucionar su problema habitacional, en apoyo a su inclusión social.
- b) **Transparencia**, porque actuamos de manera accesible para que toda persona natural o jurídica, que tenga interés legítimo, pueda conocer si las actuaciones del servidor público son apegadas a la ley.
- c) **Compromiso**, porque realizamos nuestro trabajo con alto espíritu de servicio hacia la población y con total identificación.
- d) **Integridad**, porque actuamos con honestidad, transparencia y probidad en cumplimiento al marco legal.
- e) **Equidad**, porque promovemos la igualdad de oportunidades, para el acceso a los beneficios que ofrece la Institución a las familias salvadoreñas.
- f) **Excelencia**, porque realizamos nuestro trabajo con calidad para satisfacer las expectativas de nuestros clientes, utilizando nuestras mejores habilidades técnicas y humana.

6. MARCO NORMATIVO

6.1 Ley del Fondo Nacional de Vivienda Popular.

6.2 NRP-42 Normas Técnicas para la Gestión del Riesgo Operacional en las Entidades Financieras.

6.3 NRP-20: Normas Técnicas para la Gestión Integral de Riesgos de las Entidades Financieras.

6.4 NRP-17: Normas Técnicas de Gobierno Corporativo.

6.5 NRP-23: Normas Técnicas para la Gestión de la Seguridad de la Información.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

6.6 NRP-24: Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio.

7. POLÍTICA DE GESTIÓN DE RIESGO OPERACIONAL

La gestión de riesgo operacional es un elemento determinante para FONAVIPO, dada la naturaleza de sus operaciones, para lo cual se definen las presentes políticas encaminadas a identificar, medir, controlar y mitigar oportunamente los eventos que pudieran representar riesgos para la institución:

- a) Se contará con un Comité de Riesgos, para el asesoramiento en materia de prevención de riesgos a la Junta Directiva de FONAVIPO.
- b) Se desarrollará a nivel institucional una cultura de prevención de riesgos que propicie la reducción de los niveles de exposición al riesgo.
- c) Será la Unidad de Riesgos de FONAVIPO la responsable de la implementación y la periódica actualización de las políticas, metodologías y procesos vinculados del presente Manual.
- d) La gestión de riesgo operacional será de tal forma que asegure los cambios de forma oportuna de los perfiles de riesgos a los que está expuesto FONAVIPO, así como del establecimiento de controles adecuados a los mismos que permitan la actualización del nivel de riesgo y al mismo tiempo la prevención y solución de conflictos de interés, en la recolección de la información, los registros de eventos y su posterior seguimiento.
- e) En FONAVIPO estamos comprometidos a identificar, valorar, controlar, y monitorear los riesgos, a los cuales se encuentran expuestas las operaciones bajo la responsabilidad de quien las ejecuta, de tal forma que se garantice el logro de los objetivos institucionales.

7.1 Factores de Riesgo

Los factores generadores de riesgo operacional contemplados en el presente Manual se detallan a continuación:

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

- a) **Procesos:** Este factor corresponde a los riesgos asociados a los procesos definidos, documentados y actualizados permanentemente por la institución pudiendo estos ser agrupados como estratégicos u operativos que pudieran contener fallas o debilidades que representen un riesgo para el desarrollo eficiente de las operaciones; dichos procesos deberán contar con los documentos, definidos y actualizados permanentemente.
- b) **Personas:** Es un factor que permite identificar y gestionar fallas, insuficiencias, negligencia, sabotaje, robo, inadecuada capacitación, apropiación indebida de información, entre otros aspectos, asociados al personal, vinculado directa o indirectamente a la entidad, con el fin de minimizar la posibilidad de que ocurran pérdidas económicas. En dicho factor se involucra el establecimiento adecuado de políticas, procesos y procedimientos que procuren una adecuada planificación y administración del capital humano que incluyan proceso de contratación, permanencia y desvinculación del personal.

Por vinculación directa deberá entenderse aquella que emana de un contrato interno de trabajo, de acuerdo a la legislación laboral respectiva. Por otro lado, deberá entenderse por vinculación indirecta la relación jurídica con la entidad que emana de un contrato para la prestación de determinados servicios, diferente de aquella que se origina de un contrato interno de trabajo.

- c) **Tecnología de información:** Es un factor de riesgo asociado a la tecnología de información, entre otros, los 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, así como en la calidad de la información que estos proporcionan y una adecuada inversión tecnológica.
- d) **Acontecimientos externos:** Es un factor asociado a acontecimientos ajenos al control de la institución, que pudieran alterar el desarrollo normal de las actividades de la institución, relacionadas a fallas en los servicios críticos provistos por terceros, contingencias legales, la ocurrencia de desastres naturales atentados y actos delictivos entre otros factores.

MANUAL DE RIESGO OPERACIONAL

7.2 Clasificación de Eventos de Riesgo Operacional

Los eventos de riesgos son considerados como aquellas situaciones que afectan el normal desarrollo de las operaciones de FONAVIPO, los cuales incluyen los incidentes ocurridos y eventos que pudieran generar pérdidas y afectar económicamente los resultados de institución, los cuales se clasifican como se detallan a continuación:

- 1) **Fraude Interno:** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o eludir regulaciones, leyes o políticas empresariales en las que se encuentra implicado, al menos, un miembro de la entidad;
- 2) **Fraude Externo:** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o eludir la legislación, por parte de un tercero.
- 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 reclamaciones por daños personales, o sobre casos relacionados con la diversidad o discriminación.
- 4) **Clientes, productos y prácticas del negocio:** 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.
- 5) **Daños a Activos Materiales:** Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.
- 6) **Interrupción del negocio y fallos en los sistemas:** Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.
- 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.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

7.3 Estructura de gestión de riesgo operacional

Para la ejecución de las actividades de gestión integral de riesgos, FONAVIPO cuenta con una estructura organizacional integrada por diferentes niveles jerárquicos y la debida segregación de funciones, siendo esta la siguiente:

Estructura de Gestión de Riesgo



Director Ejecutivo



	NORMATIVA	CÓDIGO: DE-N-035 FECHA: NOVIEMBRE 2023 REVISIÓN: 4 PÁGINA: 12
MANUAL DE RIESGO OPERACIONAL		

7.4 Funciones y Responsabilidades para la Gestión de Riesgo Operacional

7.4.1 Junta Directiva

- a) Aprobar las estrategias, políticas, manuales y planes de continuidad del negocio de la entidad para la gestión del riesgo operacional, y asegurarse que la Alta Gerencia los implemente efectivamente;
- b) Asignar y aprobar los recursos necesarios para implementar y mantener en funcionamiento la gestión del riesgo operacional en forma efectiva y eficiente; y
- c) Asegurarse de que Auditoría Interna verifique la existencia y el cumplimiento del esquema de gestión del riesgo operacional.
- d) Designar a la unidad de riesgos de la comunicación de la ocurrencia de eventos de riesgo operacional, para el envío de la Base de Datos a la Superintendencia del Sistema Financiero de forma anual a más tardar el 31 de enero de cada año.

7.4.2 Comité de Riesgos

- a) Evaluar, revisar y proponer para aprobación de la Junta Directiva las estrategias, políticas, manuales y planes de continuidad del negocio de gestión del riesgo operacional;
- b) Supervisar que la gestión del riesgo operacional sea efectiva y que los eventos de riesgos sean consistentemente identificados, evaluados, mitigados y monitoreados;
- c) Proponer los mecanismos para la implementación de las acciones correctivas requeridas en caso de que existan desviaciones con respecto al nivel de tolerancia al riesgo operacional;
- d) Aprobar las metodologías de gestión del riesgo operacional; y

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

- e) Apoyar la labor de la Unidad de Riesgos en la implementación de la gestión de riesgo operacional.

7.4.3 Alta Gerencia

La Alta Gerencia es la responsable de la implementación de la gestión del riesgo operacional, de las estrategias, políticas, manuales y planes de continuidad del negocio, autorizados por la Junta Directiva.

7.4.4 Unidad de Riesgos

- a) Diseñar y someter a la aprobación de la Junta Directiva, a través del Comité de Riesgos, las estrategias, políticas, manuales y planes de continuidad del negocio para la gestión del riesgo operacional;
- b) Diseñar y someter a la aprobación del Comité de Riesgos la metodología para la gestión del riesgo operacional;
- c) Apoyar y asistir a las demás unidades de gestión para la implementación de la metodología del riesgo operacional;
- d) Elaborar una opinión sobre el riesgo de nuevos productos o servicios, previo a su lanzamiento; así como también ante cambios importantes en el ambiente operacional o informático, y
- e) Reportar oportunamente y de forma completa y detallada las fallas en los diferentes factores de riesgo operacional a la Junta Directiva a través del Comité de Riesgos.

7.4.5 Unidad de Auditoría Interna

Evaluar al menos anualmente, el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional y dar seguimiento al cumplimiento del plan de trabajo de la Unidad de Riesgos.

Director Ejecutivo



	NORMATIVA	CÓDIGO: DE-N-035 FECHA: NOVIEMBRE 2023 REVISIÓN: 4 PÁGINA: 14
MANUAL DE RIESGO OPERACIONAL		

7.5 Etapas del Proceso de Gestión de Riesgos

FONAVIPO para la gestión de riesgo operacional realizará el proceso de gestión considerando las siguientes etapas:

Identificación: Para efectos de establecer un mapa de riesgo operacional los eventos de riesgo se identificarán y clasificarán de acuerdo a lo establecido en este Manual en el Anexo No. 1 Tipos de Eventos por Riesgo Operacional.

Medición: Los riesgos se estimarán y cuantificarán considerando la probabilidad de ocurrencia y el impacto económico en los resultados de la institución, esta cuantificación es esencial para el establecimiento de los controles adecuados y estrategias de mitigación de los mismos.

Control y mitigación: Son las acciones o mecanismos de cobertura y controles implementados por FONAVIPO para prevenir o reducir los efectos negativos en caso de materializarse los eventos de riesgo operacional. Debe establecerse un Plan con detalle de acciones a implementar, el plazo estimado de ejecución y los responsables directos de dicha ejecución.

Monitoreo y comunicación: En esta etapa del proceso se dará seguimiento sistemático y oportuno a los eventos de riesgo operacional identificados, así como las acciones o controles adoptados. Además, se informará a Comité de Riesgos y a Junta Directiva mediante informes semestrales para asegurar una revisión periódica y la generación de información suficiente para apoyar los procesos de toma de decisiones.

Los líderes, gestores del riesgo operacional o jefes de unidades organizativas, deben realizar un monitoreo permanente de su mapa de riesgos y exposición a pérdidas por riesgo operacional, debiendo cumplir como mínimo con los siguientes aspectos:

- i. Desarrollar procesos de seguimiento efectivo y permanente que permitan la rápida detección y corrección de las deficiencias;
- ii. Establecer indicadores que evidencien potenciales riesgos operacionales;

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

- iii. Asegurar que los controles internos establecidos se encuentren funcionando en forma efectiva y eficiente; y
- iv. Asegurar que los riesgos residuales se encuentren bajo el nivel de tolerancia establecido por cada entidad.

FONAVIPO debe contar con sistemas de información gerencial y bases de datos estadísticas que posibiliten la generación de información oportuna, confiable, consistente y homogénea para los reportes periódicos a la Junta Directiva, Comité de Riesgos y/o Alta Gerencia, así como a otros interesados responsables de la toma de decisiones en la gestión de riesgo operacional.

7.6 Categorías de Eventos de Pérdida

- 7.6.1 **Eventos de pérdida económica:** Son aquellos eventos de pérdida que ocasionan un impacto negativo en los resultados económicos de la institución.
- 7.6.2 **Eventos de pérdida no económica:** Son aquellos eventos de riesgo que no generan una pérdida económica para la institución.

8. METODOLOGÍA PARA LA GESTIÓN DE RIESGO OPERACIONAL

La metodología para la gestión del riesgo operacional de FONAVIPO se fundamenta en cuatro etapas: Identificación, Medición, Control y Monitoreo, cuyos lineamientos para la ejecución de cada una de éstas se presentan a continuación:

8.1 Clasificación de los Eventos de Riesgo

Previo al desarrollo de las etapas de gestión del riesgo, estos se clasificarán de acuerdo a los siguientes criterios:

Eventos Ex – antes o fallas potenciales

La identificación de las fallas potenciales se realizará conjuntamente con los líderes, gestores del riesgo operacional o jefes de unidades organizativas, mediante equipos de trabajo o comisiones destinadas para su levantamiento, con el objetivo de anticiparse y

	NORMATIVA	CÓDIGO: DE-N-035 FECHA: NOVIEMBRE 2023 REVISIÓN: 4 PÁGINA: 16
MANUAL DE RIESGO OPERACIONAL		

evaluar fallas potenciales priorizando en los procesos de realización, incluyendo el riesgo legal, riesgo de nuevos productos o servicios y otros tipos de amenazas.

Las fallas potenciales podrán comprender eventos de riesgo, provenientes de observación, aplicación del juicio de experto, simulaciones basadas en escenarios, pérdidas o riesgos acontecidos en procesos similares dentro de FONAVIPO o experimentados por otras instituciones de igual naturaleza, comparación con estándares de la misma industria, entre otros.

Eventos Ex-post

Estarán conformados por aquellos eventos, cuya materialización representa un impacto de reducción en los resultados y en consecuencia en el patrimonio de FONAVIPO; siempre y cuando, su causa u origen esté incluida en la definición de riesgo operacional.

8.2 Identificación

En esta etapa del proceso de gestión de riesgos, los eventos de riesgo se clasificarán de acuerdo a los tipos de riesgo ya definidos en el Anexo No.1 "Tipos de Eventos de Riesgo Operacional"

8.3 Medición

En esta etapa, los riesgos se miden considerando los criterios de probabilidad de ocurrencia y el posible impacto en los resultados de la institución:

8.3.1 Criterios para la valoración de los eventos de riesgo:

a) En cuanto a la probabilidad de ocurrencia

Nivel	Tipo de probabilidad	Descriptivo	Rango de probabilidad
5	Casi seguro	Ocurrirá en la mayoría de las circunstancias.	Probabilidad por arriba del 80% que este se presente.
4	Probable	Probablemente ocurrirá en la mayoría de las circunstancias.	Entre el 60% y el 80% de probabilidad que este se presente.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

3	Posible	Es posible que ocurra bajo ciertas circunstancias.	Entre el 40% y el 60% de probabilidad que este se presente.
2	Improbable	Podría ocurrir en algún momento.	Entre el 20% y el 40% de probabilidad que este se presente.
1	Rara	Puede ocurrir en circunstancias excepcionales.	Entre el 1% y el 20% de probabilidad que este se presente.

La valoración cuantitativa de la probabilidad de ocurrencia de los eventos de riesgo, se realizará sobre la base de los rangos de probabilidad anteriormente definidos. Para la valoración cualitativa, se realizará mediante la aplicación del juicio de un grupo de expertos.

b) En cuanto a su impacto:

Nivel	Tipo de impacto	Descriptivo	Rango de impacto
5	Significativo	Pérdidas económicas de alto impacto	≥ 25%
4	Mayor	Pérdidas económicas sustanciales	15% y <25%
3	Moderado	Pérdidas económicas moderadas	5% y <15%
2	Menor	Pérdidas económicas relativamente bajas	1% y < 5%
1	Insignificante	Pérdidas económicas bajas	< 1%

Para la valoración cuantitativa del impacto de los eventos de riesgo se utilizarán los rangos de impacto previamente definidos, preferentemente sobre la base de los resultados anuales proyectados, considerándose dentro de estos, los ajustes que pudiesen haberse realizado durante el período de evaluación.

8.3.2 Mapa de riesgos

El resumen de la valoración combinada entre la probabilidad de ocurrencia y el impacto que provee el perfil de los eventos de riesgo operacional, se muestra en el siguiente esquema:

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

		PERFIL DEL EVENTO DE RIESGO					
		1	2	3	4	5	
PROBABILIDAD	Casi seguro	5	Moderado (5)	Moderado (10)	Alto (15)	Alto (20)	Extremo (25)
	Probable	4	Bajo (4)	Moderado (8)	Alto (12)	Alto (16)	Alto (20)
	Posible	3	Bajo (3)	Moderado (6)	Moderado (9)	Alto (12)	Alto (15)
	Improbable	2	Bajo (2)	Bajo (4)	Moderado (6)	Moderado (8)	Moderado (10)
	Raro	1	Bajo (1)	Bajo (2)	Bajo (3)	Bajo (3)	Moderado (5)
			1	2	3	4	5
			Insignificante	Menor	Moderado	Mayor	Significativo
			IMPACTO				

8.3.3 Perfil de riesgo

De la valoración combinada entre la probabilidad de ocurrencia y el impacto, se establecerá el perfil de riesgo inherente del evento identificado, de conformidad a los rangos definidos en la siguiente tabla:

Perfil	Rangos de Riesgo	Consideración
Extremo	21 → 25	El riesgo es inaceptable
Alto	11 → 20	El riesgo es importante
Moderado	5 → 10	El riesgo es tolerable
Bajo	< 4	El riesgo es aceptable

8.3.4 Efectividad de los controles

Se debe evaluar como el perfil de riesgo inherente del evento de riesgo identificado, es mitigado por la efectividad de los controles asociados a dicho evento.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

a) Identificación de los controles.

Una vez establecido el perfil de riesgo inherente de los eventos de riesgo, los líderes, gestores del riesgo operacional o jefes de unidades organizativas; deberán identificar los controles existentes para mitigar el riesgo en cuestión. Asimismo, éstos podrán determinar el tipo de control, tomando en cuenta el listado de los controles tipo y las tipificaciones de: Preventivo, Detectivo, Protección o Correctivo; plasmadas en el Anexo No.2 Detalle de Líneas de Negocio.

b) Ponderación de la efectividad de los controles.

La ponderación de la efectividad de los controles identificados, se realizará mediante la aplicación de la siguiente tabla:

Ponderación	Efectividad	Descriptivo
0.20	Alta	Los controles existentes proporcionan la seguridad razonable suficiente para mitigar la probabilidad de ocurrencia o el impacto asociado al evento de riesgo identificado.
0.40	Media	Los controles existentes proporcionan la seguridad razonable para mitigar la probabilidad de ocurrencia o el impacto asociado al evento de riesgo identificado; no obstante, éstos presentan oportunidades de mejora.
0.60	Baja	Los controles existentes no son suficientes para mitigar los riesgos asociados al evento de riesgo identificado; implicando su fortalecimiento y/o la creación de nuevos controles.
1.00	Sin Control	No existen controles que mitiguen los riesgos asociados al evento de riesgo identificado.

c) Determinación del perfil de riesgo residual

El perfil de riesgo residual será determinado, multiplicando el nivel del perfil de riesgo inherente por la ponderación de la efectividad de los controles asociados al evento de riesgo.

Para el análisis de resultados, el mapa de riesgo inherente, será comparado con el mapa de riesgo residual.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

8.4 Control y Mitigación del Riesgo

8.4.1 Tipos de control

En esta etapa del proceso deben implementarse controles que se traduzcan en la disminución de la probabilidad de ocurrencia y/o el impacto potencial de los eventos de riesgo identificados, los cuales se clasificaran de la siguiente manera:

a) Controles Preventivos

Actúan sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos.

b) Controles Detectivos

Se diseñan para descubrir un evento, irregularidad o un resultado no previsto; alertan sobre la presencia de los riesgos y permiten tomar medidas inmediatas; pueden ser manuales o computarizados. Generalmente sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos. Ofrecen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear, o alertar a los funcionarios.

c) Controles de Protección

Su objetivo es establecer medidas de control o planes de acción que protejan a la institución contra pérdidas que impacten en los resultados económicos de FONAVIPO.

d) Controles Correctivos

Permiten el restablecimiento de una actividad, después de ser detectado un evento no deseable, posibilitando la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan, y

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

permiten mejorar las deficiencias. Por lo general, actúan con los controles detectivos, implicando reprocesos.

8.4.2 Mitigación

En esta etapa se determinan las acciones a seguir para reducir y/o mantener los riesgos dentro de los niveles de tolerancia aceptables por la institución.

Las estrategias de mitigación para gestionar los riesgos deben ser determinadas por los gestores de riesgo operacional, en tal sentido las estrategias se pueden clasificar según se detalla:

- a) Aceptación:** No se lleva a cabo ninguna acción y se asume la pérdida económica o el riesgo;
- b) Mitigación:** Se toman acciones que permitan la reducción del impacto de la ocurrencia del riesgo;
- c) Transferencia:** Se toman acciones para transferir a un tercero el impacto o pérdida esperada por los riesgos asumidos.

8.5 Monitoreo y comunicación

El objetivo de esta etapa es asegurar continuamente que las acciones establecidas para mitigar los eventos de riesgo, sean eficaces y se cumplan según lo establecido.

En este sentido, el monitoreo estará enfocado al seguimiento de las acciones realizadas, respecto a la condición o evolución de los eventos de riesgo identificados, con el objeto de obtener una seguridad razonable de que éstas han permitido reducir el perfil de los eventos de riesgo; fortaleciendo así, la gestión de riesgo operacional.

Los gestores de riesgo operacional y la Unidad de Riesgos deberán dar seguimiento oportuno a los eventos de riesgo operacional, así como a los resultados de las acciones realizadas.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

8.5.1 Registro de eventos de riesgo

Los eventos de riesgo identificados, deberán ser registrados en la base de datos de eventos de riesgo en el SIN módulo de riesgos, por el líder, gestor de riesgo operacional, jefe o designado en cada unidad organizativa, este registro deberá realizarlo dentro del tiempo vigente en cada trimestre, además contará como máximo de tiempo de 20 días hábiles del siguiente mes al finalizar un trimestre.

De no dar cumplimiento al plazo establecido, el responsable de la unidad organizativa deberá solicitar a la unidad de riesgos la gestión para la habilitación vía sistema y pueda registrar los eventos de riesgos acaecidos en un trimestre.

Los tipos de eventos de riesgo, podrán agruparse de acuerdo a lo establecido en los Anexos No. 1, 2 y 3 de este Manual.

8.5.2 Indicadores de evolución de riesgos

La Unidad de Riesgos en conjunto con los gestores de riesgo operacional, deberán evaluar para dar seguimiento a los riesgos operacionales identificados, así como los que se hayan decidido mitigar en vía de aceptación o transferencia. Estos indicadores podrán proveer información sobre la efectividad de los controles o de las acciones tomadas para la minimización de los riesgos que se están evaluando.

Cuando se hayan evaluado los riesgos por dos o más períodos consecutivos, se podrá comparar el valor del riesgo residual obtenido en un período de tiempo comparándolo con el anterior, utilizando la siguiente escala de disminución, para clasificar el nivel de riesgo del indicador que se está evaluando.

Escala de disminución	Clasificación
De 0% a 25%	Riesgo Extremo
De 25.01% a 50.00%	Riesgo Alto
De 50.01% a 75.00%	Riesgo Moderado
De 75.01% al 100%	Riesgo Bajo

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

Utilización de la escala

- Los riesgos cuya reducción sea entre el 0% al 25% se catalogarán como riesgo extremo.
- Los riesgos que su reducción esté en el rango del 25.01% al 50.00% se clasificarán como de riesgo alto.
- Los riesgos que su reducción esté en el rango del 50.01% al 75.00% se clasificarán como de riesgo moderado.
- Los riesgos que se reduzcan entre una 75.01% al 100% serán clasificados como de riesgo bajo.

La escala de la categorización de los riesgos, será en concordancia con la evaluación y determinación del nivel de riesgo según la disminución que se haga en un periodo específico, con las causas identificadas y mitigadas según el seguimiento respectivo.

En caso que el riesgo no reporte en el seguimiento ningún tipo de reducción, o se mantenga en el mismo nivel o al contrario aumentó al perfil de riesgo residual, el líder, gestor de los procesos o área responsable deberá adoptar la elaboración de Plan de Acción y Mitigación de Riesgos, con el objetivo de implementar nuevas acciones que conlleven a que disminuya el perfil de riesgo. Para esta implementación, se documentará mediante el Anexo No. 5.

Para los eventos de riesgos en seguimiento documentados en matrices de riesgo operacional y que se hayan materializado, los responsables (líderes y gestores de riesgos) deberán de proceder a elaborar Matriz de Seguimiento de Riesgos Materializados de acuerdo al Anexo No. 6 con el objetivo de medir la eficacia de los controles o acciones de mitigación. Para el caso que se materialice algún evento y no esté en matriz de riesgo operacional, se deberá proceder a documentarlo en el seguimiento de la matriz del riesgo operacional y en la matriz de Riesgos Materializados Anexo 6.

Posteriormente de haber documentado el evento de riesgo en ambas matrices, los responsables (líderes y gestores de riesgos), tendrán que volver a evaluar nuevamente con las acciones o controles determinados o implementados para efectos de continuar la gestión de mitigación de riesgos materializados; los

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

controles o acciones que trataban ese evento de riesgo ya no serán considerados en la nueva evaluación que se efectúe.

Para los riesgos que se materialicen por segunda vez por la misma causa, se deberá elevar la probabilidad de riesgo a su máxima clasificación (riesgo extremo).

9. PRESTACIÓN DE SERVICIOS POR TERCEROS

El Fondo ha establecido políticas y procedimientos apropiados para evaluar, administrar y monitorear los servicios críticos brindados por terceros, es decir aquellos servicios y actividades definidas como prioritarios cuya no disponibilidad compromete la existencia de la entidad;

La prestación de servicios debe formalizarse mediante contratos firmados, que incluyan el alcance del servicio y defina claramente las responsabilidades del proveedor y del Fondo. Por otra parte, debe incluir una cláusula que obligue al proveedor a documentar los servicios brindados y le garantice el establecimiento de planes de contingencia y de continuidad del servicio brindado.

Además, deben incluirse cláusulas que faciliten una adecuada revisión de la respectiva prestación de servicios por parte del Fondo, así como entes externos que supervisan dichos servicios por terceros. Independientemente que determinados servicios sean realizados por terceras partes, el Fondo es responsable de asegurar el cumplimiento de las disposiciones que le son aplicables.

Previo a la contratación de servicios críticos tercerizados, las unidades solicitantes deberán cumplir las condiciones de tercerización establecidas en las normas relacionadas a la gestión de los riesgos operacionales, seguridad de la información y continuidad del negocio; mismas que deberán considerarse en las especificaciones técnicas o descripción del servicio a adquirir e informar a la Unidad de Compras Públicas que el servicio solicitado está identificado como servicio crítico.

La Unidad de Compras Públicas, es la unidad responsable de la centralización del control de todos los servicios prestados por terceros que como mínimo debe contener el nombre del proveedor, el tipo de servicio, monto contratado, contraparte dentro de la entidad y

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

su vigencia. Dicho control debe estar a disposición de la Superintendencia del Sistema Financiero.

9.1 Riesgo Legal

El Fondo a través de las unidades Organizativas, ha establecido mediante las políticas, subprocesos y controles específicos de las diferentes áreas según les aplique, que previo a la celebración de contratos, actos jurídicos u operaciones que realizan, se analice la validez jurídica y se procure la adecuada verificación legal.

Asimismo, dichas políticas y procedimientos deben contener aspectos relativos a la conservación ordenada, completa, íntegra y oportuna de la información y documentación que soporta las operaciones del Fondo.

Por otra parte, las unidades organizativas cuentan con una matriz de riesgo legal, como apoyo al cumplimiento y mitigación de riesgos legales, la cual contiene la identificación de los cumplimientos o compromisos obligatorios según las leyes o normas aplicables, a las cuales se deben dar fiel cumplimiento.

10. PERIODICIDAD DE EVALUACIONES E INFORMES

10.1 Informes de seguimiento

La Unidad de Riesgos realizará capacitaciones y talleres sobre la gestión de riesgo operacional y rendirá informes al Comité de Riesgos en los meses de julio y diciembre de cada año. Dicha gestión de riesgos será desarrollada en conjunto con los líderes de procesos del Sistema de Gestión de Calidad y gestores de riesgo operacional designados para cada unidad organizativa. Asimismo, dicha unidad divulgará de forma continua el pensamiento basado en riesgos; y amplía el espectro de capacitaciones enfocadas según tipos de riesgo a diversas unidades de la organización. Dichas actividades, deberán de contemplarse en el Plan Operativo Anual que la unidad formula cada año.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

10.2 Informe Anual

En el mes de abril de cada año, la Unidad de Riesgos presentará al Comité de Riesgos para su aprobación el Informe Anual de Gestión de Riesgo Operacional y posterior remisión a la Superintendencia del Sistema Financiero.

11. SANCIONES

Los líderes, gestores del riesgo operacional o jefes de unidades organizativas deberán participar activamente, apoyar y cumplir con lo establecido en este Manual, en su defecto deberá aplicarse el Reglamento Interno de Trabajo.

12. VIGENCIA

- a) Este Manual sustituye las modificaciones aprobadas por Junta Directiva en fecha 26 de julio de 2023, Acta No. 1304/1329/07/2023 Acuerdo No. 9426/1304.
- b) Este Manual ha sido modificado de conformidad a lo aprobado por Junta Directiva en fecha 29 de noviembre de 2023, Acta No. 1317/1342/11/2023, Acuerdo No. 9520/1317.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

13. ANEXOS

13.1 Anexo No. 1: Tipos de Eventos 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 eludir regulaciones, leyes o políticas empresariales en las que se encuentra implicado, al menos, un miembro de la entidad.	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas económicas), 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 eludir la legislación, por parte de un tercero.	Robo y fraude	Robo, falsificación.
		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 de negocios	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.	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información (conocimiento del cliente, etc.), infringir la privacidad de información sobre clientes minoristas, infringir la privacidad, ventas agresivas, abuso de información confidencial.
		Prácticas empresariales o de mercado impropiedades	Prácticas restrictivas de la competencia, prácticas comerciales / de mercado impropiedades, manipulación del mercado, abuso de información privilegiada (en favor de la entidad), 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

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

			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	Desastres naturales, pérdidas causadas por personas 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	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.
		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.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

13.2 Anexo No. 2: Detalle de Líneas de Negocio

Nivel 1	Nivel 2	Grupos de Actividades
Finanzas corporativas	Finanzas corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, titularización, servicio de estudios, deuda (pública, alto rendimiento), acciones, sindicaciones, ofertas públicas iniciales, colocaciones privadas en mercados secundarios.
	Finanzas de Administraciones locales / públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Renta fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda.
	Creación de Mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Préstamos y depósitos de clientes minorista, servicios bancarios, fideicomisos.
	Banca privada	Préstamos y depósitos de particulares, servicios bancarios, fideicomisos y asesoramiento de inversión.
	Servicios de tarjetas	Tarjetas de empresas / comerciales, de marca privada y minoristas.
Banca comercial	Banca comercial	Financiación de proyectos, bienes raíces, financiación de exportaciones, financiación comercial, factoraje, arrendamiento financiero, préstamos, garantías, letras de cambio.
Pago y liquidación	Clientes externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación.
Servicios de agencia	Custodia	Certificados de depósitos, operaciones para préstamo de títulos valores.
	Agencia para empresas	Agentes de emisiones de deudas y pagos.
	Fideicomisos de empresas	Comisiones de confianza y otros servicios
Administración de activos	Administración discrecional de fondos	Minoristas, institucionales, cerrados, abiertos, participaciones accionariales.
	Administración no discrecional de fondos	Minoristas, institucionales, de capital fijo, de capital variable.
Intermediación minorista	Intermediación minorista	Ejecución y servicio completo.

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

13.3 Anexo No. 3: Tabla de contenido de la Base de Datos de Registro de Eventos.

1	Referencia	Código interno que identifique el evento en forma secuencial.
2	Factor de riesgo operacional	De acuerdo a la clasificación establecida en Capítulo II de estas Normas.
3	Tipo de evento de pérdida	Identifica el tipo de pérdida, de acuerdo con la clasificación del Anexo No. 1.
4	Líneas de negocio	Identificación de la línea de negocio que origino el evento, siendo las principales para el caso de bancos, bancos cooperativos y sociedades de ahorro y crédito las detalladas en Anexo No.2. Para las Sociedades de Seguro, las principales líneas de negocios, se detallan en Anexo No.3.
5	Descripción del evento	Descripción detallada del evento. Canal de servicio o atención al cliente (cuando aplica) Zona geográfica.
6	Fecha de inicio del evento	Fecha en que se inicia el evento. Día, mes, año.
7	Fecha de finalización del evento	Fecha en que finaliza el evento. Día, mes, año.
8	Fecha del descubrimiento	Fecha en que se descubre el evento. Día, mes, año.
9	Fecha de contabilización	Fecha en que se registra contablemente la pérdida económica por el evento. Día, mes, año, hora.
10	Monto	El monto a que asciende la pérdida, cuantificación económica de la ocurrencia del evento de riesgo operacional y los gastos derivados de su atención.
11	Divisa	Moneda extranjera en la que se materializa el evento.
12	Cuentas contables afectadas	Identifica las cuentas del Catálogo de Cuentas afectadas.
13	Proceso	Identifica el proceso afectado.
14	Valor total recuperado	El valor total recuperado por la acción directa de la entidad. Incluye los montos recuperados por seguros.
15	Valor recuperado por seguros	Corresponde al valor recuperado por la cobertura a través de un seguro.
16	Producto o servicio afectado	Identifica el producto o servicio afectado por el evento de riesgo operacional.
17	Cuantificación de la severidad del daño	Monto a que asciende la pérdida (neta de cualquier mitigante o recuperación)



Director Ejecutivo

MANUAL DE RIESGO OPERACIONAL

13.4 Anexo No. 4: Listado de controles de tipo para disminuir probabilidad de ocurrencia e impacto.

No	Controles	Tipo			
		Preventivo	Detectivo	Protección	Correctivo
1	Acceso restringido	X			
2	Actualización periódica de procedimientos				X
3	Alarmas contra robo		X		
4	Auditoria Internas		X		
5	Capacitación y entrenamiento	X			
6	Claves de acceso	X			
7	Código de conducta y /o ética	X			
8	Control de calidad		X		
9	Evaluaciones separadas externas		X		
10	Copias de seguridad			X	
11	Diseño de documentos preimpresos	X			
12	Establecimiento de límites para efectuar pagos y / o desembolsos			X	
13	Estandarización	X			
14	Evaluación de desempeño		X		
15	Evaluación grado de satisfacción del cliente		X		
16	Firmas autorizadas	X			
17	Inspecciones no programadas		X		
18	Mantenimiento preventivo	X			
19	Manuales actualizados	X			
20	Medición de eficiencia en el uso de equipos		X		
21	Planes de contingencia			X	
22	Planes de continuidad del negocio			X	
23	Planes de emergencia			X	
24	Políticas de seguridad de la información y los sistemas	X			
25	Procedimientos para la corrección de errores				X
26	Procedimientos para recuperación de desastres				X
27	Programa de selección de personal	X			
28	Reportes de quejas y reclamos		X		X
29	Respaldos para interrupción de energía			X	
30	Revisar antecedentes de personal en el proceso de selección	X			
31	Rotación de funciones	X			
32	Segregación de funciones	X			
33	Tercerización o subcontratación	X			
34	Uso de medios de comunicación para aclarar eventos negativos para la entidad.			X	
35	Vigilancia	X			
36	Validación de cumplimiento de normas			X	
	Total	16	9	8	4

Director Ejecutivo



MANUAL DE RIESGO OPERACIONAL

13.5 Anexo No. 5: Modelo de Plan de Acción y Mitigación

PLAN DE ACCIÓN Y MITIGACIÓN DE RIESGOS

PROCESO:

REF. UNIDAD	DESCRIPCIÓN DEL EVENTO	SUBPROCESO VINCULADO	PERFIL DE RIESGO INHERENTE	CONTROLES O ACCIONES (SEGUN MATRIZ DE RIESGO OPERACIONAL)	PERFIL DE RIESGO RESIDUAL	ANÁLISIS DE LAS CAUSAS PARA DETERMINAR QUE OTRAS ACCIONES SE FORTALECERÁN Y PASARÁN AL PLAN DE ACCIÓN O MITIGACIÓN	PLAN DE ACCIÓN O MITIGACIÓN	AREA RESPONSABLE (LIDER Y/O GESTOR)	TIEMPOS ESTIMADOS PARA REALIZAR LAS GESTIONES (DESDE HASTA)
A	B	C	D	E	F	G	H	I	J

Nota. En columna

- A Tomar referencia de la identificación de la unidad y el número correlativo del evento de riesgo según matriz de riesgo operacional según proceso.
- B Copiar el evento de riesgo según matriz de riesgo operacional del proceso correspondiente
- C Detallar el subproceso respectivo según la descripción del evento según matriz de riesgo operacional del proceso
- D Copiar el perfil del riesgo inherente de la matriz de riesgo operacional del proceso respectivo.
- E Copiar las acciones o controles de acuerdo a la matriz de riesgo operacional
- F Copiar perfil del riesgo residual de acuerdo a la matriz de riesgo operacional
- G Revisar y analizar los controles de la columna E de este Plan, y describir las causas por las cuales no fueron efectivos los controles. Ejemplo: No fueron efectivos porque no se dio seguimiento, porque no se actualizaron, porque no estaban enfocados al evento de riesgo, y otros
- H Después de haber diagnosticado las causas según columna G, determine cuales nuevas acciones se implementarán para mitigar el nivel de riesgo en nivel moderado y alto.
- I Enunciar los responsables del proceso o subproceso respectivo
- J Establecer el inicio y finalización para el plan de mitigación.



[Handwritten signature]

Director Ejecutivo



CÓDIGO: DE-N-035
FECHA: NOVIEMBRE DE 2023
REVISIÓN: 4
PÁGINA: 33

NORMATIVA

MANUAL DE RIESGO OPERACIONAL

13.6 Anexo No. 6: Modelo de Matriz de Seguimiento de Riesgos Materializados

MATRIZ DE SEGUIMIENTO DE RIESGOS MATERIALIZADOS

PROCESO: _____ SUB-PROCESO: _____ LIDER DEL PROCESO: _____ FECHA: _____

Perfil de Riesgo

- 1. Riesgo Extremo
- 2. Riesgo Alto
- 3. Riesgo Moderado
- 4. Riesgo Bajo

No. Ref. del riesgo	DESCRIPCIÓN DEL RIESGO	NIVEL DEL RIESGO (PERFIL)	ACCIONES	RESPONSABLE	FECHA PROGRAMADA		EFICACIA DE LAS ACCIONES PARA ABORDAR RIESGOS
					DESDE	HASTA	
1	2	3	4	5	6	7	

Indicaciones para el llenado:

1. Extraer de matriz de riesgo operacional, la referencia del riesgo
 2. Extraer de matriz de riesgo operacional, el nombre del evento de riesgo
 3. Extraer de matriz de riesgo operacional, el nivel de riesgo
 4. Estas acciones copielas de la matriz de riesgo o del archivo de controles
 5. Responsables líderes y gestores de riesgo del proceso respectivo
 6. Revise y determine el periodo de inicio y finalización como vigilancia que ejecutará esas acciones o controles
 7. Con base al análisis efectuado de las acciones que implementó según Plan de Mitigación Anexo 3 del Manual ROPE, describa del porqué fueron o no efectivas las nuevas acciones que implementó después que se materializo el riesgo.
- Después:
 Ir a la matriz de riesgo operacional a revisar nuevamente y actualizar con las acciones implementadas según columna D, deberá revisar y actualizar archivo de controles y matriz de riesgo operacional, para determinar nuevamente los niveles de controles y perfil de riesgo.



Director Ejecutivo

