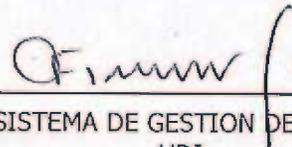
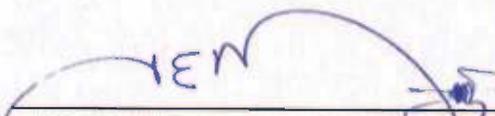


Solicitud de cambio.

Solicitante: Unidad de Riesgos	Fecha: 28 de Noviembre de 2019
Nombre del documento: MANUAL DE RIESGO OPERACIONAL Código: DE-N-035	
Revisión: 1	
Motivo del cambio: Mejorar el Manual de Riesgo Operacional incorporando el apartado de Responsabilidades, además se actualiza el plazo estipulado para el registro de eventos de riesgo y el periodo o fecha del año en el que se rendirá Informe al Comité de Riesgo sobre la gestión de riesgo operacional, de conformidad a la aprobado por Junta Directiva de fecha 30 de octubre de 2019, según Acta No. 1123/1148/10/2019, Acuerdo No. 8287/1123.	
Descripción del cambio: <ol style="list-style-type: none">1. Se adiciona al Manual de Riesgo Operacional el apartado "4. Responsabilidades".2. En el apartado "7.5.1 Registro de eventos de riesgo", se modifica el plazo del registro de eventos de riesgo, ampliándolo de 15 a 20 días hábiles.3. En el apartado "8.1 Informes de seguimiento" se modifica la periodicidad en que se rinde informe al comité de riesgo sobre seguimiento de riesgo operacional.	
Temporal <input type="checkbox"/>	Permanente <input checked="" type="checkbox"/>
Válido hasta:	
Vo.Bo.:  GESTOR DEL SUB-PROCESO* 	Revisado por:  SISTEMA DE GESTION DE LA CALIDAD UDI 
*Normativa firma de acuerdo al proceso o área relacionada.	
Aprobado por:  DIRECTOR EJECUTIVO O LIDER DEL PROCESO** ** Normativa y Lineamientos firma el director ejecutivo 	

UDI-F-02

COPIA NO CONTROLADA



NORMATIVA

CÓDIGO: DE-N-035
FECHA: OCTUBRE DE 2019
REVISIÓN: 1
PÁGINA: 1

TÍTULO: **MANUAL DE RIESGO OPERACIONAL**

MANUAL DE RIESGO OPERACIONAL

UNIDAD DE RIESGOS

San Salvador, octubre de 2019


Director Ejecutivo



COPIA NO CONTROLADA



NORMATIVA

CÓDIGO: DE-N-035
FECHA: OCTUBRE DE 2019
REVISIÓN: 1
PÁGINA: 2

TÍTULO: **MANUAL DE RIESGO OPERACIONAL**

1.	OBJETIVO	3
2.	DEFINICIONES	3
3.	ALCANCE	4
4.	RESPONSABILIDADES	4
5.	MARCO NORMATIVO:	4
6.	POLÍTICA DE GESTIÓN DE RIESGO OPERACIONAL	4
6.1	Factores de Riesgo	5
6.2	Clasificación de Eventos de Riesgo Operacional	6
6.3	Estructura de gestión de riesgo operacional	7
6.4	Funciones y Responsabilidades para la Gestión de Riesgo Operacional	8
6.4.1	Junta Directiva	8
6.4.2	Comité de Riesgos	8
6.4.3	Alta Gerencia	8
6.4.4	Unidad de Riesgos	9
6.4.5	Unidad de Auditoría Interna	9
6.5	Etapas del Proceso de Gestión de Riesgos	9
6.6	Categorías de Eventos de Pérdida	10
7.	METODOLOGÍA PARA LA GESTIÓN DE RIESGO OPERACIONAL	10
7.1	Clasificación de los Eventos de Riesgo	10
7.2	Identificación	11
7.3	Medición	11
7.3.1	Criterios para la valoración de los eventos de riesgo:	11
7.3.2	Mapa de riesgos	12
7.3.3	Perfil de riesgo	13
7.3.4	Efectividad de los controles	13
7.4	Control y Mitigación del Riesgo	14
7.4.1	Tipos de control	14
7.4.2	Mitigación	15
7.5	Monitoreo y comunicación	16
7.5.1	Registro de eventos de riesgo	16
7.5.2	Indicadores de evolución de riesgos	16
8.	PERIODICIDAD DE EVALUACIONES E INFORMES.	17
8.1	Informes de seguimiento	17
8.2	Informe Anual	18
9.	VIGENCIA	18
10.	ANEXOS	19
10.1	Anexo No. 1: Tipos de Eventos por Riesgo Operacional	19
10.2	Anexo No. 2: Listado de controles tipo para disminuir probabilidad de ocurrencia e impacto	21

Director Ejecutivo



COPIA NO CONTROLADA

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) **Riesgo Operacional:** Es la posibilidad de incurrir en pérdidas, debido a las fallas en los procesos, personal, sistemas de información y a causa de acontecimientos externos incluyendo el riesgo legal.
- c) **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.
- d) **Factores de Riesgo:** Son los factores generadores de un evento de riesgo operacional.
- e) **Junta Directiva:** Órgano colegiado encargado de la administración de la entidad, con funciones de supervisión y control.
- f) **Ley:** Ley del Fondo Nacional de Vivienda Popular.
- g) **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.
- h) **Mapa de Riesgo:** Es el instrumento que muestra de forma esquemática y resumida la valoración de los eventos de riesgo operacionales de la institución.
- i) **Riesgo Inherente:** Es aquél al que se enfrenta una entidad en ausencia de acciones para modificar su probabilidad de ocurrencia o impacto.

Director Ejecutivo



COPIA NO CONTROLADA

TÍTULO: **MANUAL DE RIESGO OPERACIONAL**

- j) **Riesgo Residual:** Es aquél al que se enfrenta una entidad después de la evaluación de los controles y/ o la aplicación de acciones encaminadas al tratamiento de los eventos de riesgos.
- k) **Perfil de Riesgo:** Es el nivel de riesgo asignado a un evento de riesgo, en función de su probabilidad de ocurrencia e impacto.

3. ALCANCE

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

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. MARCO NORMATIVO:

- 5.1 Ley del Fondo Nacional de Vivienda Popular.
- 5.2 NPB4-50: Normas para la gestión del riesgo operacional de las entidades financieras, dictada por la Superintendencia del Sistema Financiero.
- 5.3 NPB4-47: Normas para la Gestión Integral de Riesgos de las entidades financieras.

6. 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:

Director Ejecutivo



COPIA NO CONTROLADA

TÍTULO: **MANUAL DE RIESGO OPERACIONAL**

- a) Se contará con un Comité de Riesgo, 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.

6.1 Factores de Riesgo

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

- a) **Procesos:** este factor corresponde a los riesgos asociados a los procesos definidos por la institución que pudieran contener fallas o debilidades que representen un riesgo para el desarrollo eficiente de las operaciones.
- b) **Personas:** es un factor que se deriva de las fallas en 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.
- c) **Tecnología de la Información:** es un factor de riesgo asociado a las fallas en el desarrollo e implementación de los sistemas de seguridad y continuidad operativa de los sistemas informáticos, así como en la calidad de la información que estos proporcionan.

Director Ejecutivo



COPIA NO CONTROLADA



NORMATIVA

CÓDIGO: DE-N-035
FECHA: OCTUBRE DE 2019
REVISIÓN: 1
PÁGINA: 6

TÍTULO: **MANUAL DE RIESGO OPERACIONAL**

- d) **Acontecimientos externos:** es un factor asociado a acontecimientos externos, ajenos al control de la institución, que pudieran alterar el desarrollo normal de las actividades de la institución.

6.2 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 en Activos Materiales:** Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.
- 6) **Interrupción del negocio y fallas en los sistemas:** Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

Director Ejecutivo



COPIA NO CONTROLADA

- g) **Ejecución y 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.

6.3 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



COPIA NO CONTROLADA

6.4 Funciones y Responsabilidades para la Gestión de Riesgo Operacional

6.4.1 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.
- c) Asegurarse de que Auditoría Interna verifique la existencia y el cumplimiento del esquema de gestión del riesgo operacional.

6.4.2 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
- e) Apoyar la labor de la Unidad de Gestión de Riesgos en la implementación de la gestión de riesgo operacional.

6.4.3 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.

Director Ejecutivo



COPIA CONTROLADA

6.4.4 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.

6.4.5 Unidad de Auditoría Interna

Evaluar 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.

6.5 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 esta política en el apartado 5.2 Clasificación de Eventos de Riesgo Operacional.


Director Ejecutivo



COPIA NO CONTROLADA



NORMATIVA

CÓDIGO: DE-N-035
FECHA: OCTUBRE DE 2019
REVISIÓN: 1
PÁGINA: 10

TÍTULO: **MANUAL DE RIESGO OPERACIONAL**

Medición: los riesgos se estimarán y cuantificarán considerando la probabilidad de ocurrencia 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: 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.

Monitoreo: 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.

6.6 Categorías de Eventos de Pérdida

6.6.1 Eventos de pérdida económica: son aquellos eventos de pérdida que ocasionan un impacto negativo en los resultados económicos de la institución.

6.6.2 Eventos de pérdida no económica: son aquellos eventos de riesgo que no generan una pérdida económica para la institución.

7. 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:

7.1 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 gestores, gerentes y jefes, mediante equipos de trabajo o comisiones destinadas para su levantamiento, con el objetivo de anticiparse y evaluar fallas potenciales priorizando en

Director Ejecutivo



COPIA NO CONTROLADA

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 este incluida en la definición de riesgo operacional.

7.2 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"

7.3 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:

7.3.1 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% de 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.
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.

Director Ejecutivo



COPIA CONTROLADA

TÍTULO: MANUAL DE RIESGO OPERACIONAL

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 periodo de evaluación.

7.3.2 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



COPIA NO CONTROLADA

		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							

7.3.3 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

7.3.4 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.

a) Identificación de los controles

Una vez establecido el perfil de riesgo inherente de los eventos de riesgo, los gestores, gerentes o jefes; deberán identificar los controles existentes para mitigar el riesgo en cuestión. Así mismo, éstos podrán determinar el tipo de control, tomando en cuenta el

Director Ejecutivo



COMPLETAMENTE CONTROLADA

listado de los controles tipo y las tipificaciones de: Preventivo, Detectivo, Protección o Correctivo; plasmadas en el Anexo No.2.

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.

7.4 Control y Mitigación del Riesgo

7.4.1 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 clasificarán de la siguiente manera:

Director Ejecutivo



COPIA NO CONTROLADA

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

7.4.2 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 del riesgo.

Director Ejecutivo



COPIA NO CONTROLADA



NORMATIVA

CÓDIGO: DE-N-035
FECHA: OCTUBRE DE 2019
REVISIÓN: 1
PÁGINA: 16

TÍTULO: **MANUAL DE RIESGO OPERACIONAL**

- 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.

7.5 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.

7.5.1 Registro de eventos de riesgo

Los eventos de riesgo identificados, serán registrados en la base de datos de eventos de riesgo en el SIN módulo de riesgos, por el gestor de riesgo operacional designado en cada unidad organizativa, al finalizar cada mes o trimestre, contando como máximo de tiempo de 20 días hábiles del siguiente mes al finalizar cada trimestre. Los tipos de eventos de riesgo, podrán agruparse de acuerdo a lo establecido en el Anexo No. 1.

7.5.2 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 periodos consecutivos, se podrá comparar el valor del riesgo residual obtenido en un periodo de tiempo comparándolo con

Director Ejecutivo



COPIA NO CONTROLADA

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 Alto
De 25.01% a 75.00%	Riesgo Medio
De 75.01% al 100%	Riesgo Bajo

Utilización de la escala

- Los riesgos cuya reducción sea entre el 0% al 25% se catalogarán como riesgo alto.
- Los riesgos que su reducción este en el rango del 25.01% al 75.00% se clasificaran como de riesgo medio.
- Los riesgos que se reduzcan entre una 75.01% al 100% serán clasificados como de riesgo bajo.

En caso que el riesgo no reporte en el seguimiento ningún tipo de reducción, sino al contrario aumento al perfil de riesgo residual, el área responsable deberá adoptar un plan de acción que disminuya el perfil de riesgo.

8. PERIODICIDAD DE EVALUACIONES E INFORMES.

8.1 Informes de seguimiento

La Unidad de Riesgos realizará capacitaciones y talleres sobre la gestión de riesgo operacional y rendirá informes al Comité de Riesgo 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



COPIA NO CONTROLADA



NORMATIVA

CÓDIGO: DE-N-035
FECHA: OCTUBRE DE 2019
REVISIÓN: 1
PÁGINA: 18

TÍTULO: **MANUAL DE RIESGO OPERACIONAL**

8.2 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.

9. VIGENCIA

- a) Este Manual deroga el aprobado por Junta Directiva, Acuerdo No. 8038/1067, Acta No. 1067/1092/07/2018, de fecha 27 de julio de 2018.
- b) Este Manual ha sido modificado según Acuerdo de Junta Directiva No. 8287/1123, Acta No. 1123/1148/10/2019, de fecha 30 de octubre de 2019 y entrará en vigencia a partir de la fecha de su aprobación.

Director Ejecutivo



COPIA NO CONTROLADA

10. ANEXOS

10.1 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 de los límites de riesgo

Director Ejecutivo



CONTROLADA

TÍTULO: MANUAL DE RIESGO OPERACIONAL

			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



COPIA NO CONTROLADA



NORMATIVA

CÓDIGO: DE-N-035
FECHA: OCTUBRE DE 2019
REVISIÓN: 1
PÁGINA: 21

TÍTULO: MANUAL DE RIESGO OPERACIONAL

10.2 Anexo No. 2: Listado de controles 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		
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	X	3

Director Ejecutivo



COPIA NO CONTROLADA