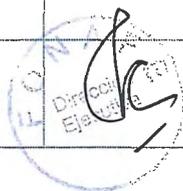


Manual Corporativo: “Guía para la Gestión Integral de Riesgos”

Fecha	Responsable	Visto y Sello
23 ABR. 2018	Elaborado por: Jefe de Órgano de Buen Gobierno Corporativo y Gestión de Riesgos Operacionales	
23 ABR. 2018	Revisado por: Jefe de Órgano de Buen Gobierno Corporativo y Gestión de Riesgos Operacionales	
23 ABR. 2018	Homologado por: Ejecutivo Corporativo de Excelencia Operacional	
23 ABR. 2018	Aprobado por: Director Ejecutivo	

Control de Cambios

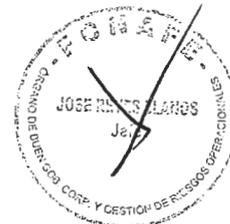
Versión	Sección / Ítem	Descripción del cambio:
00	-----	Nuevo el 23 de Abril del 2018

Fecha	Nº Resolución Dirección Ejecutiva
23/04/18	Nº 030-2018/DE-FONAFE



ÍNDICE

1. INTRODUCCIÓN	4
2. OBJETIVO	4
3. ALCANCE	4
4. POLÍTICAS Y/O NORMAS	4
5. TÉRMINOS Y/O DEFINICIONES	5
6. DESCRIPCIÓN / DESARROLLO	7
6.1 Definición de objetivos a nivel entidad	7
6.2 Mapeo de Procesos	7
6.3 Definición de objetivos a nivel de procesos	8
6.4 Determinación del Apetito, tolerancia y capacidad de riesgo	8
6.5 Selección de procesos críticos	14
6.6 Elaboración del Plan de Gestión Integral de Riesgos	14
6.7 Definición de presupuesto	15
6.8 Identificación de eventos	15
6.9 Identificación de riesgos	15
6.10 Criterios para la documentación de riesgos	16
6.11 Tipos de riesgo	16
6.12 Técnicas para la identificación de riesgos	17
6.13 Riesgos múltiples	19
6.14 Actividades de Control	19
6.15 Matriz de riesgos y controles	20
6.16 Evaluación de riesgos	20
6.16.1 Método para la definición de la probabilidad e impacto	21
6.16.2 Niveles y criterios de probabilidad e impacto	21
6.16.3 Tipos de riesgo de acuerdo a su criticidad	23
6.16.4 Método para determinar el nivel de riesgo o severidad	24
6.16.5 Mapa de riesgos	24
6.17 Definición del plan de tratamiento al riesgo	25
6.17.1 Estrategias de respuesta al riesgo	26
6.17.2 Razones para la selección de la estrategia de tratamiento al riesgo	27
6.17.3 Razones para la selección de la estrategia de tratamiento al riesgo	28
6.17.4 Planes de acción de tratamiento al riesgo	29
6.17.5 Indicadores de desempeño de la Gestión Integral de Riesgos (KRI's)	30
6.18 Seguimiento y monitoreo continuo	32
6.18.1 Cronograma de seguimiento a los planes de acción	32
6.18.2 Evaluación de riesgo residual	33
6.18.3 Criterios para la evaluación de controles	33
6.19 Actividades de reporte	34



1. INTRODUCCIÓN

FONAFE, a través de la presente "Guía para la Gestión Integral de Riesgos", busca documentar criterios y lineamientos contemplados en el desarrollo de la metodología de riesgos, con la finalidad de identificar, medir, controlar, monitorear y reportar los riesgos operacionales que enfrentan las empresas bajo el ámbito de FONAFE.

2. OBJETIVO

Establecer una guía de respuesta para el desarrollo de la Gestión Integral de Riesgos (en adelante, "GIR") en la Corporación. De este modo, a la Empresa le permitirá identificar, analizar y dar respuesta a los riesgos que enfrenta bajo un enfoque que reúna las prácticas líderes de control interno y de GIR, contribuyendo con el fortalecimiento del Gobierno Corporativo de la Empresa.

Por otro lado, con la implementación de la presente guía, se busca:

- Contribuir al establecimiento y fortalecimiento de políticas y procedimientos de la GIR que conducen al logro de los objetivos estratégicos.
- Establecer la metodología para la identificación, evaluación, tratamiento, monitoreo y reporte de riesgos, que permitan determinar el nivel de exposiciones del riesgo.
- Mejorar la cultura de la GIR, a través de un adecuado programa de capacitaciones dirigido a todo el personal.
- Establecer las actividades de control necesarias para asegurar que los planes de acción, se llevan a cabo adecuada y oportunamente.
- Desarrollar actividades de monitoreo permanente para asegurar la implementación de la GIR en la compañía.

3. ALCANCE

Lo establecido en el presente manual es de cumplimiento obligatorio para todos los colaboradores de las empresas bajo el ámbito de FONAFE (trabajadores con contrato a plazo indeterminado, fijo y practicantes) que ejecutan actividades de los procesos y procedimientos; así como de las áreas involucradas en su ejecución.

4. POLÍTICAS Y/O NORMAS

Normas de Control Interno, aprobado por Resolución de Contraloría General N° 320-2006-CG.

- Decreto Legislativo N° 1031, Decreto Legislativo que Promueve la Eficiencia de la Actividad Empresarial del Estado y su reglamento Decreto Supremo N° 176-2010-EF y sus normas modificatorias.
- Código de Buen Gobierno Corporativo para las Empresas bajo el ámbito de FONAFE, aprobado por Acuerdo de Directorio N° 002-2013/003-FONAFE.
- Lineamiento Corporativo del Sistema de Control Interno para las Empresas bajo el ámbito de FONAFE, aprobado por Acuerdo de Directorio N° 015-2015/016-FONAFE.
- Lineamientos para la Gestión de la Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno, aprobado por Resolución Ministerial N° 028-2015-PCM.
- Uso de la NTP ISO/IEC 27001:2014 en las Entidades Integrantes del Sistema Nacional de Informática, aprobado por Resolución Ministerial N° 004-2016-PCM.
- Directiva N° 013-2016-CG/GPROD, Implementación del Sistema de Control Interno en las Entidades del Estado, aprobado por Resolución de Contraloría N° 149-2016-CG.
- Decreto Legislativo N° 1352, Decreto Legislativo que amplía la responsabilidad administrativa de las personas jurídicas.
- Guía para la implementación y fortalecimiento del Sistema de Control Interno en las Entidades del Estado, aprobado por Resolución de Contraloría N° 004-2017-CG.

5. TÉRMINOS Y/O DEFINICIONES

- **Alta Dirección:** La alta dirección está compuesta por el Director Ejecutivo y los Gerentes del Centro Corporativo.
- **Apetito por el riesgo:** El nivel de riesgo que la Empresa decide asumir durante el proceso de consecución de sus objetivos. La determinación de este punto permite controlar y mantener los riesgos en los niveles deseados.
- **Control:** Actividad que tiene como finalidad reducir la criticidad de un riesgo. Debe contar con un responsable designado para su ejecución, seguir una frecuencia determinada y dejar una evidencia de que se realizó la actividad de control.
- **La capacidad al riesgo:** Es el nivel máximo de riesgo que una Empresa puede soportar en la persecución de sus objetivos.
- **Directorio:** Órgano que supervisa a la gerencia.
- **Empresas de la Corporación:** Empresas de la Corporación bajo el ámbito de FONAFE.
- **Estrategia de riesgo:** el tratamiento que se le brinda a un riesgo tiene como propósito mantener el nivel de criticidad dentro de niveles aceptados por empresa.

Las estrategias posibles son:

- Reducir: Establecer controles, o fortalecer los existentes, para disminuir probabilidad de ocurrencia del riesgo.
- Evitar: Dejar de realizar la actividad que genera el riesgo.



- Transferir: Transferir a un tercero la administración del riesgo o enfrentar las pérdidas originadas.
 - Explotar: Aceptar niveles de riesgo altos para aprovechar oportunidades.
 - Retener: Conservar el riesgo sin tomar ninguna acción adicional más que su adecuado monitoreo.
 - Eliminar: Eliminar la causa raíz que ocasiona el riesgo.
 - **Evaluación del riesgo:** Proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgo objetivo u otro criterio.
 - **Exposición al riesgo:** Medida que representa el grado de posibilidad de ocurrencia de un evento negativo o adverso, así como el impacto del mismo en la empresa al momento de materializarse.
 - **Evento:** Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por una misma causa, que ocurren durante el mismo periodo de tiempo.
 - **Gestión Integral de riesgos (GIR):** Proceso de identificación, medición, control, monitoreo, evaluación, retroalimentación y optimización de todas las situaciones que representan riesgos para la organización.
 - **Gobierno Corporativo de la Empresa:** Es el conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la Empresa, como son los tres poderes dentro de una sociedad: los Accionistas, Directorio y Alta Administración.
 - **Identificación de Riesgos:** Proceso de determinar qué ¿puede suceder?, ¿Por qué? y ¿cómo?
 - **Impacto:** Se define como el nivel o grado de exposición ante la posibilidad de materialización de un riesgo.
 - **Indicadores claves de Riesgo - KRI:** Métricas usadas para obtener señales tempranas sobre la exposición creciente de los riesgos a las que estén expuestas las diversas áreas del negocio.
 - **Mapa de Riesgos:** Gráfico que ilustra el impacto y probabilidad de ocurrencia de los riesgos.
 - **Plan de acción:** Conjunto de acciones enfocadas a reducir el nivel de riesgo.
 - **Probabilidad:** es el nivel de posibilidad de que ocurra el evento de riesgo en un periodo determinado (por lo general un año)
 - **Responsable de proceso:** Responsable de la correcta ejecución de los procesos a su cargo y de administrar el mejoramiento continuo, para lo cual cuentan con el apoyo de todos los participantes de su proceso.
- Riesgo:** Incertidumbre o condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.



- **Riesgo Inherente:** Es aquel riesgo en su forma natural sin el efecto mitigante de los controles.
- **Riesgo Residual:** Nivel resultante del riesgo después de aplicar los controles.
- **Tolerancia al riesgo:** Es la desviación del nivel de riesgo que la Empresa quiere aceptar

6. DESCRIPCIÓN / DESARROLLO

Para que exista un buen desarrollo de la GIR, el planteamiento es la fase inicial y fundamental para que las actividades sean implementadas eficiente, oportuna y alineadas a las necesidades de la Empresa.

6.1 Definición de objetivos a nivel entidad

El primer paso del planeamiento de la GIR es la definición de objetivos a nivel entidad. Ello sirve para orientar la GIR en función a los objetivos que la Empresa ha establecido.

Los objetivos corporativos son objetivos de alto nivel, alineados con la misión y visión de la entidad. Estos reflejan la decisión de la Dirección en cuanto a cómo la entidad tratará de crear valor para sus accionistas.

Es importante que las Empresas comuniquen constantemente los objetivos corporativos al personal, con la finalidad de que éste se encuentre alineado con el enfoque de la entidad y, de este modo, hacer más eficiente el proceso de identificación y evaluación de riesgos.

Los objetivos deben estar categorizados en función a su naturaleza para poder orientar de una manera más eficiente las estrategias que la Empresa pretende desarrollar. Se recomienda que los objetivos se categoricen de la siguiente manera o siguiendo una clasificación similar:

- Estratégicos
- Operacionales
- Reporte o presentación de resultados
- Cumplimiento

6.2 Mapeo de Procesos

Es importante que las Empresas cuenten con un adecuado mapeo de sus procesos existentes, debido a que éste permite tener un mayor entendimiento de las operaciones y así poder identificar los riesgos asociados a cada proceso. Asimismo,



el mapeo de procesos permite implementar, y monitorear los controles de una manera más eficiente.

El mapeo de procesos no es responsabilidad directa de los responsables de la GIR en la Empresa, sino que su desarrollo deberá ser liderado por un puesto a nivel gerencial que cuente con conocimiento del flujo de los procesos de la Empresa, al cual se le deberá brindar el apoyo del resto de áreas. Sin embargo, el responsable de la implementación de la GIR deberá involucrarse directamente en el avance y obtención de resultados de esta actividad.

A fin de conocer la metodología corporativa de la gestión de procesos, FONAFE aprobará las disposiciones que sean necesarias.

6.3 Definición de objetivos a nivel de procesos

El objetivo de un proceso es la finalidad por la cual el proceso es desarrollado dentro de la cadena de valor de la Empresa. Es decir, la razón por la cual es importante para la Empresa. Los objetivos de los procesos deben ser definidos durante el mapeo de procesos (Ver punto 6.2). Estos objetivos deben tomar en cuenta la contribución del proceso para el cumplimiento de la misión y visión de la Empresa. En este sentido, los procesos deben encontrarse alineados al Plan Estratégico.

Los objetivos de los procesos deben ser definidos por las Gerencias de línea en coordinación con los dueños de procesos, ello deberá ser supervisado por el responsable a cargo de la implementación de riesgos. Una vez definidos, estos objetivos deben ser aprobados por la dirección de la Empresa.

6.4 Determinación del Apetito, tolerancia y capacidad de riesgo

El apetito, tolerancia y capacidad al riesgo se deberán definir con la Alta Dirección en función a los objetivos estratégicos del plan estratégico de la Empresa, lo cual servirá como marco para la GIR. A continuación las definiciones:

- **Apetito al riesgo**

El apetito de riesgo es el nivel de riesgo que la Empresa decide asumir durante el proceso de consecución de sus objetivos y figura como la zona baja en el mapa de riesgos (verde).

Es decir, el apetito de riesgo es determinado por la dirección de la Empresa con el apoyo durante el proceso del responsable de la implementación de riesgos y debe estar alineado a los objetivos corporativos. Tras ello, debe ser validado por los principales stakeholders y finalmente comunicado a toda la Empresa. La GIR debe estar alineada al apetito de riesgo definido.

El proceso de la fijación del apetito de riesgo debe ser específico para cada una de las Empresas de la Corporación, debido a que la aplicabilidad del apetito de riesgo no es generalizable.

Para la definición del apetito de riesgo se analizará en qué medida los siguientes aspectos impactan en el cumplimiento de los objetivos de la Empresa:

- Negocio de la Empresa
- Aspectos jurídicos y normativos
- Operación de la empresa
- Tecnologías
- Tecnologías de la información
- Aspectos financieros
- Factores sociales y humanitarios
- Fraude

Para ello, el nivel directivo de la Empresa deberá considerar cómo espera que los aspectos señalados se comporten en el tiempo para contribuir con el cumplimiento de los objetivos de la Empresa. Así, el apetito de riesgo se fijará tomando en cuenta el nivel de riesgo tope que se aceptará para no afectar este comportamiento esperado.

Una vez definido el apetito de riesgo, se llevará a cabo la identificación de los riesgos a nivel entidad y por procesos y en función a ello se procederá a definir la tolerancia al riesgo y capacidad de riesgo de Empresa.

- **La tolerancia al riesgo**

Es la desviación con respecto al apetito de riesgo; es decir, la variación del nivel de riesgo que para la Empresa es posible gestionar y figura como la zona moderada en el mapa de riesgos (amarillo).

- **La capacidad de riesgo**

Es el nivel máximo de riesgo que la Empresa puede soportar sin que interfiera en su continuidad. Ésta, es representada por la zona alta y extrema en el mapa de riesgos (anaranjado y rojo).

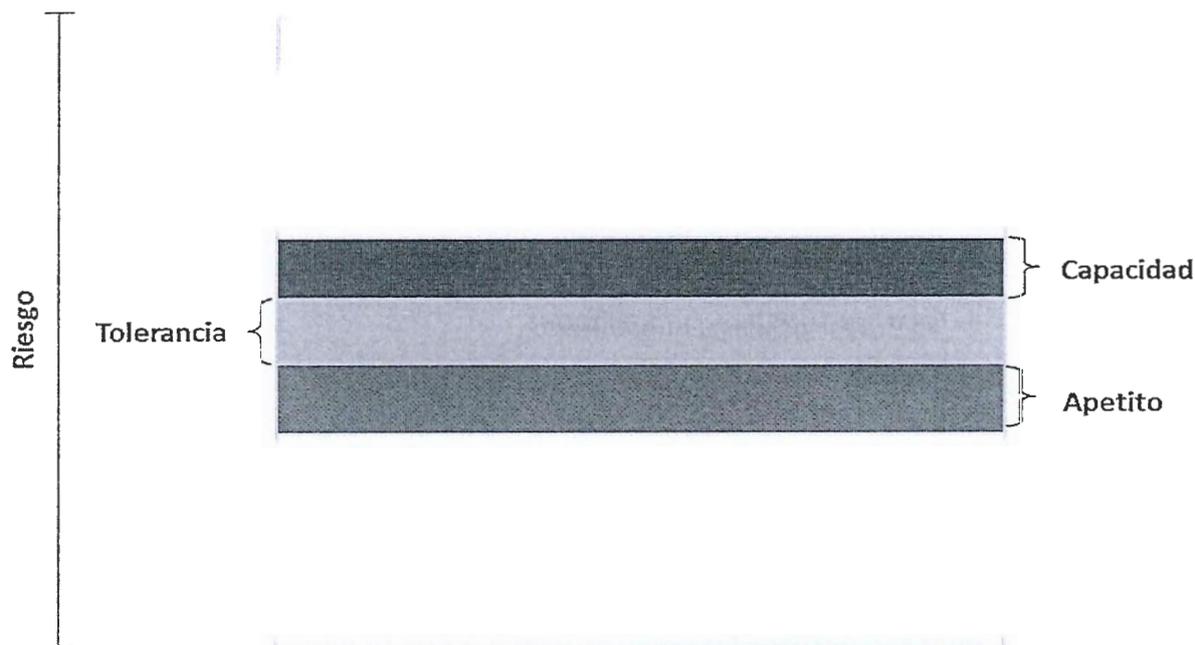
Al igual que el apetito de riesgo, tanto la tolerancia como la capacidad de riesgo deben ser definidas por Alta dirección de la Empresa validadas por los principales stakeholders y luego comunicadas a toda la Empresa. Asimismo, para la definición



Manual Corporativo: "Guía para la Gestión Integral de Riesgos"	
Código: MC-E2-ECI-01-001	Versión: 00

de estos tres conceptos, es fundamental realizar un análisis de los indicadores y metas considerado en el Plan Estratégico de la Empresa, de modo que estén alineados a estos últimos y contribuyan con su cumplimiento.

En el siguiente gráfico se evidencia la relación de los conceptos de apetito, tolerancia y capacidad de riesgo.



A continuación, se presenta un ejemplo del proceso de definición de apetito, tolerancia y capacidad del riesgo, considerando la identificación de riesgos.

a. **Apetito de riesgo:**

"La reputación de la Empresa, la de sus servicios y nuestro personal conforman nuestros principales activos, razón por la cual no toleramos riesgos que puedan impactar negativamente la imagen de la organización y a las personas que la representan. Nuestro propósito es generar valor a todos nuestros grupos de interés e innovar constantemente para que nuestros servicios cuenten con los más altos estándares de calidad y generen bienestar a nuestros clientes".

b. **Riesgo:**

"Que se registren pérdidas en la Empresa por accidentes ocupacionales".

Con el objetivo de cumplir con lo establecido en la declaración de apetito de riesgo no se permitirá que las pérdidas por accidentes ocupacionales sean



mayores a S/. 20 000 nuevos soles o que se presenten más de 5 accidentes ocupacionales por mes.

c. Tolerancia al riesgo:

En este ejemplo, para cumplir con el apetito de riesgo, la tolerancia al riesgo se encuentra en el umbral de pérdidas que va de S/. 20 001 a S/.25 000 ó 5 a 6 accidentes ocupacionales por mes.

d. Capacidad de riesgo:

La capacidad de riesgo se encuentra en el umbral de pérdidas entre S/. 25 001 a S/. 30 000 ó 7 a 8 accidentes ocupacionales por mes.

Una vez realizado este ejercicio, es importante realizar la evaluación de los riesgos identificados ya que será necesaria para la determinación del nivel de tolerancia en función a los parámetros establecidos en el ejemplo anterior.

Los siguientes criterios deben ser considerados para la definición de la tolerancia y capacidad de riesgo, los cuales se presentan acompañados de ejemplos sobre cómo podrían ser plasmados por las Empresas.

a. Negocio de la empresa

Criterio	Tipo de compañía	Ejemplo
Negocio de la empresa	Todas las empresas	Que el incremento de la venta de energía a clientes se encuentre entre # y #.
	Todas las empresas	Que el índice de satisfacción de los usuarios con el servicio se encuentre entre # y #.

b. Aspectos jurídicos y normativos

Criterio	Tipo de compañía	Ejemplo
Aspectos jurídicos y normativos	Todas las empresas	Que no se presenten incumplimientos respecto a las directivas de la Corporación FONAFE.
	Todas las empresas	Que el total de multas al año por incumplimientos legales se encuentre entre # y #.
	Todas las empresas	Que el grado de cumplimiento con la normativa de transparencia se encuentre entre # y #.

Criterio	Tipo de compañía	Ejemplo
	Todas las empresas	Que el nivel de madurez de la gestión integral de riesgos se encuentre en #.
	Todas las empresas	Que el índice de implementación del código de buen gobierno corporativo se encuentre entre # y #.
	Todas las empresas	Que se renueven todas las certificaciones planificadas.
	Todas las empresas	Que el índice de clima laboral se encuentre entre # y #.
	Todas las empresas	Que el nivel de autoevaluación de control interno se encuentre en #.

c. Operación de la empresa

Criterio	Tipo de compañía	Ejemplo
Las operaciones de la empresa	Todas las empresas	Que el número de accidentes laborales se encuentre entre # y #.
	Todas las empresas	Que el índice de rotación de personal se encuentre entre # y #.
	Distribuidoras	Que la pérdida de energía total se encuentre entre # y #.
	Distribuidoras	Que la duración promedio de interrupciones del sistema (SAIDI) se encuentre entre # y #.
	Distribuidoras	Que la frecuencia promedio de interrupciones del sistema (SAIFI) se encuentre entre # y #.
	Generadoras	Que la disponibilidad de líneas de transmisión se encuentre en #.
	Generadoras	Que la eficiencia en la producción de energía se encuentre entre # y #.
	Generadoras	Que la disponibilidad de unidades de generación se encuentre en #.

d. Tecnologías

Criterio	Tipo de compañía	Ejemplo
Tecnologías	Todas las empresas	Que el índice de cumplimiento de implementación de proyectos de tecnológica en las operaciones se encuentre entre # y #.

e. Tecnologías de la información

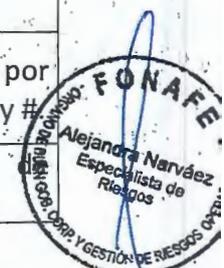
Criterio	Tipo de compañía	Ejemplo
Tecnologías de la información	Todas las empresas	Que el número de ataques cibernéticos se encuentre entre # y #.
	Todas las empresas	Que la disponibilidad de los sistemas de la información se encuentre entre # y #.
	Todas las empresas	Que el número de inconvenientes reportados a mesa de ayuda se encuentre entre # y #.
	Todas las empresas	Que el número de reclamos por pérdidas de información en las bases de datos por fallas en la operatividad de las tecnologías de la información se encuentre entre # y #.

f. Aspectos financieros

Criterio	Tipo de compañía	Ejemplo
Aspectos financieros	Todas las empresas	Que la rentabilidad patrimonial (ROE) se encuentre entre # y #.
	Todas las empresas	Que la rentabilidad operativa (ROA) se encuentre entre # y #.
	Todas las empresas	Que el margen de las ventas se encuentre entre # y #.
	Todas las empresas	Que el índice de solvencia se encuentre entre # y #.
	Todas las empresas	Que el índice de liquidez se encuentre entre # y #.
	Todas las empresas	Que el índice de rotación de activos se encuentre entre # y #.

g. Factores sociales y humanitarios

Criterio	Tipo de compañía	Ejemplo
Factores sociales y humanitarios	Todas las empresas	Que el número de reclamos sociales se encuentre entre # y #.
	Todas las empresas	Que se implementen más del #% de los programas anuales de responsabilidad social empresarial
	Distribuidoras	Que el número de usuarios incorporados por electrificación rural se encuentre entre # y #.
	Generadoras	Que no se identifique la presencia Binofilos Policlorados.



h. Fraude

Critério	Tipo de compañía	Ejemplo
Fraude	Todas las empresas	Que el número de reportes de incumplimientos al Código de Ética se encuentre entre # y #.
	Todas las empresas	Que el número de procesos judiciales por fraude se encuentre entre # y #.
	Todas las empresas	Que el número de despidos causados por fraude se encuentre entre # y #.
	Todas las empresas	Que el gasto ocasionado de manera indirecta por fraude se encuentre entre # y #.

6.5 Selección de procesos críticos

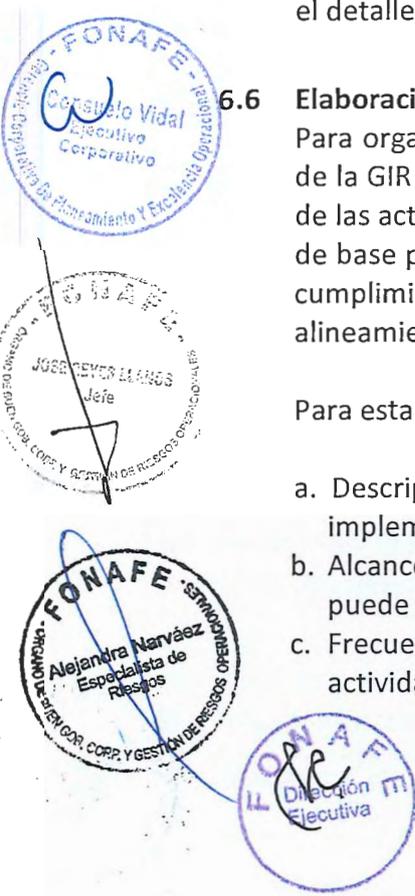
Posteriormente al mapeo de procesos y revisión de los objetivos de la organización, se identificarán los procesos críticos, considerando diversos criterios de calificación. Revisar Manual Corporativo: "Manual para la documentación de procesos y procedimientos para las empresas de la Corporación", donde muestra el detalle del desarrollo de la metodología de priorización de procesos.

6.6 Elaboración del Plan de Gestión Integral de Riesgos

Para organizar el desarrollo de las actividades y asignación de responsabilidades de la GIR en las Empresas de la Corporación, y teniendo en cuenta los resultados de las actividades ya mencionadas, se deberá elaborar una estructura que servirá de base para la elaboración del Plan para la GIR, con la finalidad de promover el cumplimiento de los objetivos de la GIR en las Empresas y procurar su alineamiento con el plan estratégico y plan operativo.

Para esta propuesta, se sugiere desarrollar los siguientes temas:

- Descripción de actividades: Detalle de las actividades que deben ser implementadas de acuerdo a lo establecido en el Plan.
- Alcance de la implementación: Precisa el alcance que deberá tener la actividad, puede ser a nivel entidad/Empresa o a nivel de procesos.
- Frecuencia: Indica la periodicidad de acuerdo a la cual deberá realizarse la actividad relacionada.



6.7 Definición de presupuesto

Con el objetivo de procurar el éxito de la GIR, resulta importante contar con los recursos necesarios para su desarrollo, dimensionando las actividades a ser realizadas y el personal requerido para ejecutarlas.

Para definir el presupuesto necesario para la implementación de la GIR, la Empresa deberá evaluar si las actividades serán realizadas por personal propio o si sería conveniente contar con apoyo externo. De escoger la primera opción, es importante verificar si el personal seleccionado cuenta con el conocimiento necesario para llevar a cabo estas actividades o si se requerirán capacitaciones.

La definición del presupuesto debe ser propuesta por el responsable de la implementación de riesgos y aprobada por la dirección y/o gerente de la Empresa.

6.8 Identificación de eventos

Un evento es una situación o elemento potencial de origen externo o interno que puede afectar a la entidad, los cuales pueden tener consecuencias positivas (oportunidades) o negativas (riesgos).

El proceso de identificación de eventos debe realizarse mediante la formulación de una matriz FODA y es de gran importancia debido a que será el punto de partida para que la Empresa pueda definir sus objetivos y estrategias durante el planeamiento estratégico.

A partir de los eventos negativos, se identificarán los riesgos a los que se enfrenta la Empresa. Por otro lado, los eventos positivos son relevantes para tener conocimiento de aquellas oportunidades que deben ser aprovechadas por la Empresa pues contribuyen al cumplimiento de objetivos. En este sentido, será importante tenerlos en cuenta al momento de definir como estrategia de tratamiento al riesgo.

Las Empresas de la Corporación deben definir una periodicidad para actualizar el inventario de eventos, la cual debería estar alineada al proceso de revisión de los objetivos corporativos.

6.9 Identificación de riesgos

Posteriormente a la planificación de la GIR, se identificarán los riesgos que afectan a los procesos y a la entidad (Riesgos Estratégicos). Este proceso es llevado a cabo empleando técnicas para identificación de riesgos que se detallarán más adelante.

Un riesgo es la amenaza que enfrenta una Empresa cuando un evento o acción puede afectar adversamente su habilidad de alcanzar los objetivos corporativos.

maximizar valor. Al momento de identificar un riesgo, es importante que no se le confunda con el evento o acción que es causa de su existencia.

La identificación de riesgos se realiza a través del desarrollo de talleres, en los que participe el personal clave relacionado y que sean liderados por el responsable de la implementación de la GIR.

En estos talleres se deberá aplicarse las técnicas para la identificación de riesgos detalladas a continuación:

- a. Identificación de riesgos a nivel entidad: se debe llevar a cabo un taller en el que participen las Gerencias, los Directivos, y el personal clave que cuente con conocimiento de la naturaleza del negocio. La dinámica del taller consiste en revisar aquellos eventos que podrían impactar negativamente a la entidad e identificar los riesgos relacionados.
- b. Identificación de riesgos a nivel de procesos: se deben llevar a cabo talleres en los que participen los dueños de los procesos, o aquellas personas que conozcan de cerca el funcionamiento de los mismos. El taller consiste en evaluar aquellos eventos que podrían tener un impacto negativo en el proceso e identificar los riesgos que esto conlleva.

6.10 Criterios para la documentación de riesgos

Para documentar adecuadamente un riesgo, se debe tener en cuenta su composición, que es la siguiente:

1. Consecuencia: Es el impacto que tendrá un riesgo al momento de materializarse.
2. Causa: Es el motivo por el cual se presenta el riesgo.

Ejemplo de Riesgo:

"Consecuencia: Que se produzcan errores en la liquidación o dobles procesamientos debido a Causa: la recepción de información duplicada".

6.11 Tipos de riesgo

Para poder identificar de una manera más efectiva los riesgos y, posteriormente, definir las estrategias de respuesta, es necesario tener en cuenta los tipos de riesgo que existen. Considerando lo propuesto por las prácticas líderes de la GIR y las características de las Empresas de la Corporación, se propone una agrupación

de seis (6) categorías (estratégicos, operacionales, de tecnologías de la información, de reporte, de cumplimiento y de fraude).

a. Riesgos estratégicos

Son los riesgos que tienen impacto directo en la Empresa a nivel de entidad debido a que afectan el cumplimiento de los objetivos corporativos y misión. Con la finalidad de facilitar su identificación, se puede tomar como base lo establecido en el plan estratégico, analizando aquellos aspectos que podrían tener efectos negativos en su cumplimiento.

b. Riesgos operacionales

Son los riesgos vinculados a la parte operativa de las Empresas de la Corporación. Incluye riesgos originados por fallas en los procesos o en la estructura organizacional, lo cual conlleva a ineficiencias o incumplimiento de compromisos. Con el fin de facilitar su identificación se puede tomar como base aquellos riesgos que comprometen la continuidad de negocio de las Empresas de la Corporación.

c. Riesgos de tecnologías de la información

Son los riesgos que tienen un impacto tanto en la gestión de las tecnologías de la información (activos, políticas, entre otras), así como en la seguridad de la información (accesos lógicos, cambios a programas, etc.) de los sistemas de la Empresa.

d. Riesgos de reporte

Son los riesgos asociados a los procesos de reporte, sean internos o externos, así como al de sus entregables.

e. Riesgos de cumplimiento

Son los riesgos que impactan en la capacidad de la Empresa para cumplir con los requisitos normativos internos y externos.

f. Riesgo de fraude

Son los riesgos asociados a las conductas que incumplen las obligaciones legales con la finalidad de obtener un beneficio (lavado de activos, etc.).

6.12 Técnicas para la identificación de riesgos

La identificación de riesgos es realizada a nivel de procesos y entidad. Las principales técnicas utilizadas para el proceso de identificación de riesgos son las siguientes:



a. Tormenta de ideas

El objetivo de esta técnica es obtener una lista completa de los riesgos de la Empresa con el propósito de aprovechar el conocimiento colectivo del grupo y desarrollar una lista de acontecimientos relacionados.

b. Técnica Delphi (metodología para buscar consensos entre los responsables de gestionar el riesgo)

Es una técnica que permite llegar a un consenso entre expertos en una materia. Los expertos en la GIR participan en esta técnica de forma anónima. Un facilitador emplea un cuestionario para solicitar ideas acerca de los riesgos importantes de la Empresa. Asimismo, la técnica Delphi ayuda a reducir sesgos en los resultados y evita que cualquier persona ejerza influencias impropias en el resultado.

c. Cuestionarios y/o encuestas

Los cuestionarios abordan una amplia gama de preguntas que los participantes deberán considerar, centrando su reflexión en los factores internos y externos que se han dado, o pueden dar lugar, a eventos negativos. Las preguntas pueden ser abiertas o cerradas, según el objetivo de la encuesta.

d. Entrevistas

Se entrevista a participantes experimentados e interesados en la materia de riesgos así como los funcionarios involucrados en los principales procesos. Las entrevistas son una de las principales fuentes de recopilación de datos para la identificación de riesgos.

e. Análisis de fortalezas y debilidades, oportunidades y amenazas

En este análisis se debe tomar en consideración los aspectos externos e internos con influencia sobre la consecución de los objetivos estratégicos de las Empresas de la Corporación, tales como factores económicos, factores políticos, factores regulatorios, factores sociales, capacidad de dirección, capacidad técnica, infraestructura, entre otros.

f. Diagramación Ishikawa

Esta técnica permite identificar las causas de los riesgos. El análisis de flujo de procesos implica normalmente la representación gráfica y esquemática de un proceso, con el objetivo de comprender las interrelaciones entre las entradas, salidas, tareas y responsabilidades de sus componentes. Una vez realizado este esquema, los acontecimientos pueden ser identificados y considerados frente a los objetivos del proceso.

Estas técnicas pueden ser aplicadas en el proceso de identificación de todos los tipos de riesgos mencionados en el punto anterior.

6.13 Riesgos múltiples

Los riesgos múltiples son aquellos que impactan a más de un procesos de la Empresa. En estos casos, se debe identificar los procesos que se encuentran afectados por estos riesgos, verificando que los controles a ser implementados guarden un alineamiento lógico entre los distintos procesos involucrados. Para ello, es importante que los dueños de proceso se reúnan periódicamente para alinear sus riesgos y controles.

Se debe tomar especial atención a los riesgos presentes en los procesos de soporte debido a que estos tienen un impacto directo en los procesos principales de la Empresa, lo cual puede resultar en riesgos múltiples.

6.14 Actividades de Control

La identificación y clasificación de los controles, es una de las actividades de gran importancia en la GIR debido a que permite identificar los esfuerzos realizados por la Empresa para el tratamiento de los riesgos.

a. Criterios para la identificación de controles

Un control es una actividad o serie de actividades que tiene como finalidad reducir la criticidad de un riesgo al cual se encuentra asociado. Es realizado de manera consistente, cuenta con un responsable asignado a su desarrollo y su ejecución es evidenciable.

b. Criterios para la documentación de controles

Los controles son incorporados en los procesos para garantizar que se mitiguen sus riesgos con el fin de cumplir con los objetivos del mismo.

Para definir y documentar controles se debe responder las siguientes preguntas:

- Cuándo: frecuencia definida e idónea según características del riesgo.
- Quién: deberá tener un responsable claramente definido.
- Qué: actividades claramente definidas.
- Cómo: debe entenderse cómo el control mitiga el riesgo.



- Evidencia: el control debe contemplar el dejar evidencia (electrónica o física) que permita en el tiempo hacer un seguimiento a su ejecución.
- Otros: ver si está documentado y comunicado dentro de la Empresa; evaluar si como está diseñado mitiga el riesgo

c. Clasificación de controles

Los controles se clasifican según la oportunidad en la que se ejecutan y el grado de automatización.

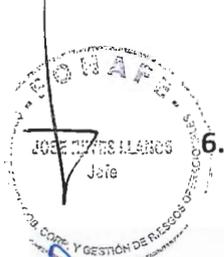
Según la oportunidad en la que se ejecutan los controles, se dividen en:

- Preventivo: Actividad de control que ayuda a evitar la ocurrencia de un riesgo
- Detectivo: Actividad de control que permite identificar errores luego de ocurrido el riesgo.

Según el grado de automatización de los controles, se dividen en:

- Manual: Control que depende de la habilidad de una persona (dueño o responsable de la actividad de control) para prevenir o detectar los errores ocurridos.
- Semiautomático: Control que depende de la habilidad de una persona para prevenir o detectar los errores ocurridos, utilizando información proveniente de un sistema
- Automático: Control que es realizado internamente por el sistema de información.

Independientemente de la clasificación de los controles, ellos apuntan a mitigar/reducir los riesgos (reales o potenciales) en beneficio de la Empresa, su misión y objetivos, así como la protección de los recursos propios o de terceros en su poder.



6.15 Matriz de riesgos y controles

Los riesgos y controles identificados, así como las calificaciones obtenidas producto de la evaluación de cada riesgo deben documentarse en la Matriz de Riesgos y Controles. Es importante contar con una Matriz de Riesgos y Controles a nivel entidad y otra a nivel de cada proceso.



6.16 Evaluación de riesgos

Una vez que se concluye la identificación de riesgos, éstos son evaluados en función a su criticidad y probabilidad de impacto, de modo que sea posible ubicar

a los riesgos más críticos. De esta manera se podrán orientar eficientemente los esfuerzos en el tratamiento de los riesgos.

6.16.1 Método para la definición de la probabilidad e impacto

Los riesgos son evaluados en función de dos variables: probabilidad (frecuencia de ocurrencia del riesgo) e impacto (severidad del riesgo o impacto económico).

Para estandarizar la criticidad de cada variable, se definen criterios generales de calificación. Estos criterios están sujetos a ser revisados y actualizados en el tiempo dependiendo de las necesidades de la Empresa.

La evaluación de riesgos cuenta con dos componentes: evaluación del riesgo inherente y evaluación del riesgo residual.

Riesgo inherente: Un riesgo inherente es aquel riesgo en su forma natural sin el efecto mitigante de los controles.

Riesgo residual: Un riesgo residual es aquel que permanece después de implementadas las actividades de control. La calificación obtenida al evaluar ambos estados del riesgo se registra en la Matriz de Riesgos y Controles.

6.16.2 Niveles y criterios de probabilidad e impacto

a. Impacto

El impacto es el nivel de exposición de la Empresa ante un riesgo; es decir la pérdida cuantitativa o cualitativa que se pudiera generar si se materializara el riesgo. Para este criterio se consideran factores financieros o monetarios, pero también factores cualitativos que no son valorizados monetariamente, tales como el impacto respecto de la reputación o imagen de las empresas de la Corporación, incumplimiento de normas o regulaciones, etc.

La definición de los criterios de probabilidad de impacto debe encontrarse alineada al apetito de riesgo.

A continuación se desarrollan algunos factores referenciales que pueden considerarse al momento de evaluar el impacto por cada uno de los tipos de riesgo, lo cual podrá ser de utilidad en la uniformización de la medición del impacto bajo distintos marcos metodológicos:



Tipo de riesgo	Factor a considerar para evaluar el impacto
Riesgos estratégicos	<ul style="list-style-type: none"> ▪ Impacto negativo en el cumplimiento de un objetivo a nivel entidad. ▪ Impacto negativo en las utilidades antes de impuestos.
Riesgos operacionales	<ul style="list-style-type: none"> ▪ Generación de ineficiencias en la utilización de recursos. ▪ Interrupción de las operaciones. ▪ Impacto negativo en el cumplimiento de los estándares de calidad de los servicios.
Riesgos de tecnologías de la información	<ul style="list-style-type: none"> ▪ Impacto negativo en el cumplimiento del Plan Estratégico de Tecnologías de la Información. ▪ Impacto negativo en un sistema informático que afecte la continuidad del negocio.
Riesgos de reporte	<ul style="list-style-type: none"> ▪ Impacto negativo en el cumplimiento de los procedimientos de reporte a entes reguladores. ▪ Calificación de opinión por parte de los auditores externos.
Riesgos de cumplimiento	<ul style="list-style-type: none"> ▪ Afectaciones a la normativa a la que se encuentra sujeta la Empresa. ▪ Generación de multas y/o penalidades.
Riesgos de fraude	<ul style="list-style-type: none"> ▪ Pérdidas económicas ligadas al evento de fraude. ▪ Impacto negativo en la reputación de la Empresa

Un ejemplo de la lógica a seguir en la formulación de las escalas para definir el nivel de impacto se presenta en la siguiente tabla:



Factor	1. Bajo	2. Medio	3. Alto	4. Extremo
% Utilidad Antes de Impuestos	1.1 Impacto que reduzca la utilidad antes de impuestos en menos del 5 %.	2.1 Impacto que reduzca la utilidad neta utilidad antes de impuestos entre 5% y menor al 10% del total de la utilidad antes de impuestos.	3.1 Impacto que reduzca la utilidad neta utilidad antes de impuestos entre 10 y menor o igual 15% del total de la utilidad antes de impuestos.	4.1 Impacto que reduzca la utilidad antes de impuestos en más del 15% del total de la utilidad antes de impuestos.

b. Probabilidad de ocurrencia

La probabilidad de ocurrencia es el grado de posibilidad de que ocurra un riesgo en un período. Puede ser estimada en función a cuántas veces históricamente ha ocurrido en la Empresa, o qué posibilidad existe de que ocurra en el futuro.

A continuación se presentan cuatro escalas que pueden ser utilizadas para definir los criterios de probabilidad de ocurrencia:

Escala	Probabilidad
1. Bajo	El evento no ha ocurrido pero podría presentarse al menos 1 vez en el año.
2. Medio	El evento podría ocurrir entre 3 o 4 veces al año.
3. Alto	El evento podría ocurrir de manera quincenal o mensual.
4. Extremo	El evento podría ocurrir de manera semanal o diaria.

Un riesgo inherente es aquel riesgo en su forma natural sin el efecto mitigante de los controles. Por su parte, un riesgo residual es aquel que permanece después de implementadas las actividades de control. La calificación obtenida al evaluar ambos estados del riesgo se registra en la Matriz de Riesgos y Controles

6.16.3 Tipos de riesgo de acuerdo a su criticidad

Los cuatro niveles de criticidad de los riesgos resultan de la combinación de los criterios de impacto y probabilidad de ocurrencia. Dichos niveles de criticidad son los siguientes:



- Riesgos extremos 
- Riesgos altos 
- Riesgos medios 
- Riesgos bajos 

6.16.4 Método para determinar el nivel de riesgo o severidad

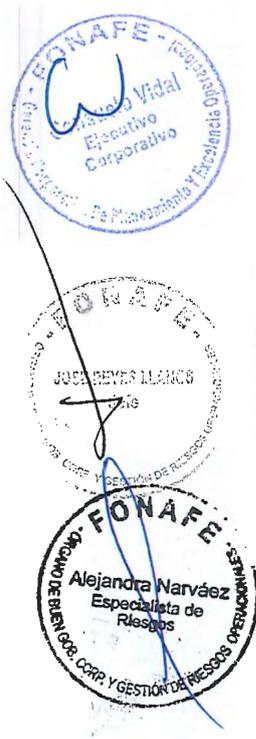
La combinación de las evaluaciones de impacto y probabilidad de ocurrencia representan un cruce dentro del mapa de riesgos que define la calificación del riesgo evaluado.

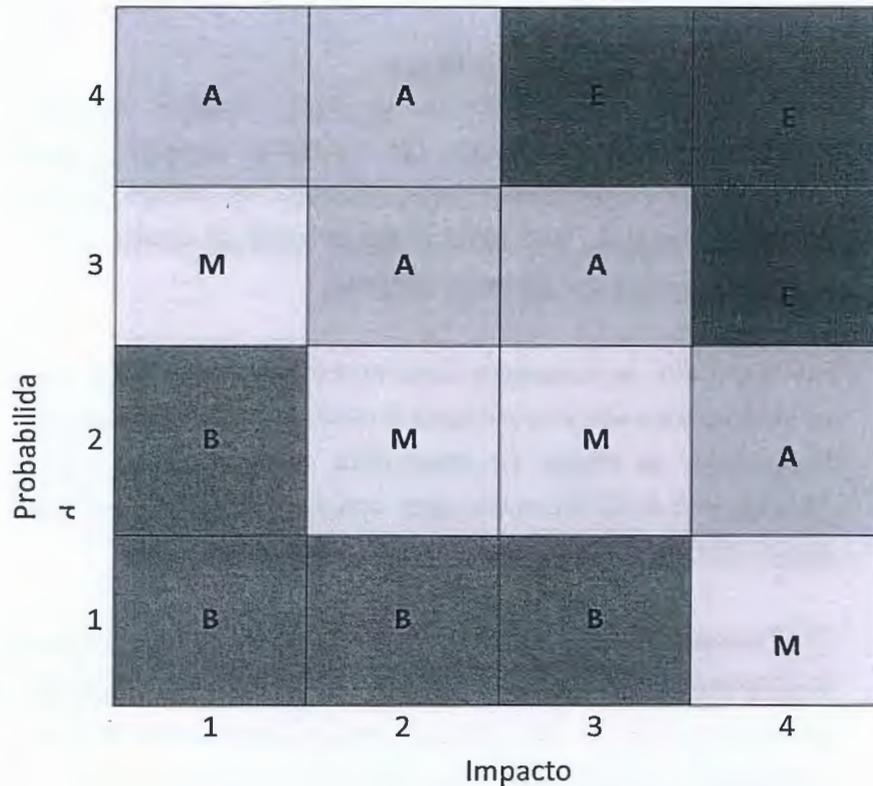
Cada uno de los riesgos identificados debe evaluarse según los criterios de calificación anteriormente mencionados, y en dos escenarios que consideren el riesgo inherente y el riesgo residual.

Para calificar la probabilidad e impacto, es necesario seleccionar el criterio general respectivo más idóneo según las características del riesgo. En caso el riesgo esté relacionado a más de un criterio general, se debe seleccionar el que esté intrínsecamente más relacionado con el riesgo o el criterio en el que se logre mayor calificación. Identificado el criterio general por variable, se procede a calificarlos según los cuatro niveles definidos. A partir de la calificación obtenida para la probabilidad e impacto, se ubican dichas coordenadas en el Mapa de Riesgos y se define la calificación total del riesgo.

6.16.5 Mapa de riesgos

En el mapa de riesgos se registran los resultados obtenidos de la evaluación de los riesgos inherentes y residuales.





La zona superior derecha muestra los riesgos más críticos (Extremos) mientras que la zona inferior izquierda señala los riesgos con menor criticidad (Bajos), la zona intermedia comprenden los riesgo con mediana-alta criticidad (Medios y Altos).

Se debe tener en cuenta que uno de los objetivos en la GIR es mantener la mayor parte de los riesgos en la zona inferior izquierda, donde son menos críticos.

6.17 Definición del plan de tratamiento al riesgo

Posteriormente a la identificación y evaluación de los riesgos, las Empresas de la Corporación deberán definir las estrategias de tratamiento de riesgos, con la finalidad de que los riesgos se mantengan dentro los niveles definidos por el apetito al riesgo.

Una característica inherente a los riesgos es que no pueden ser eliminados, por lo que las opciones giran en torno a diversas alternativas para administrarlos.

Una vez que se haya realizado la calificación del riesgo residual y de acuerdo al nivel de apetito de riesgo definido por la Empresa, se debe escoger el tratamiento a seguir para aquellos riesgos que se encuentran fuera del nivel de tolerancia de riesgo o que no cuenten con controles adecuados para su tratamiento.



6.17.1 Estrategias de respuesta al riesgo

Las respuestas pueden ser las de evitar, reducir, compartir, aceptar, explotar y eliminar el riesgo. Las Gerencias evalúan el efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios y debe seleccionar aquella que sitúe el riesgo residual dentro de los niveles de apetito de riesgo previamente definido.

Por lo general, las Empresas fallan en establecer una respuesta al riesgo de riesgos coordinado y consistente a nivel de toda la Empresa, lo cual lleva a la aparición de riesgos no detectados, la duplicación en la cobertura de riesgos, la evasión de estrategias coherentes para tratar riesgos, o sobre costos por controles excesivos para mitigar los riesgos.

Tradicionalmente, los tipos de repuesta al riesgo han girado alrededor de la contratación de seguros e implementación de actividades de control por parte de la gerencia. Sin embargo, es importante que estas medidas sean consideradas de un modo más amplio y vistas como una estrategia con el potencial de incrementar, disminuir o mantener niveles aceptables de riesgo.

La respuesta al riesgos reconoce que los riesgos tienen un ciclo de vida - antes, durante y después de la ocurrencia del hecho adverso- lo cual da lugar a que los riesgos puedan ser previstos o controlados apropiadamente a través de un planeamiento anti-contingencias, financiamiento o programas de recuperación de desastres, por ejemplo.

Cuando la respuesta al riesgo es manejada de manera efectiva, ésta puede proteger y aumentar el valor de la Empresa para los accionistas y grupos de interés. De acuerdo al nivel de riesgo identificado y evaluado, se podrá adoptar las siguientes estrategias de riesgo:

- Reducir
- Evitar
- Transferir
- Explotar
- Retener
- Eliminar

6.17.2 Razones para la selección de la estrategia de tratamiento al riesgo

La selección de la estrategia de tratamiento al riesgo debe estar a cargo del responsable de la implementación de la GIR con la participación de los dueños de procesos. Una vez seleccionadas las estrategias de tratamiento al riesgo, estas deben ser aprobadas por la dirección de la Empresa.

Antes de seleccionar las opciones de tratamiento a ser elegida, se debe considerar el escenario en el cual se deben seleccionar cada opción de tratamiento al riesgo.

Tipo de Tratamiento de Riesgos	¿Cuándo seleccionarlo?
Evitar	Se seleccionará esta alternativa, cuando el beneficio de implementar un control sea menor al costo del riesgo inherente y sus posibles consecuencias.
Reducir o Mitigar	Se seleccionará esta alternativa, cuando el beneficio de implementar un control sea mayor al costo del riesgo inherente y la empresa se encuentre en la capacidad de realizar el tratamiento del riesgo.
Transferir	Se seleccionará esta alternativa, cuando el beneficio de implementar un control sea mayor al costo del riesgo inherente y un tercero tenga una mayor capacidad para realizar el tratamiento del riesgo, debido a su especialización, infraestructura entre otros factores.
Retener	Se seleccionará esta alternativa, cuando el control (efectivo) relacionado al riesgo, no disminuya su criticidad y el riesgo deba permanecer monitoreado debido a que su alteración podría afectar la continuidad operativa del negocio.
Explotar	Se seleccionará esta alternativa cuando se presente una oportunidad para la empresa al momento en el que el riesgo se materialice, para lo cual se debe tener en cuenta el inventario de eventos positivos (oportunidades) de la empresa a fin de hacer más eficiente la solución.



Tipo de Tratamiento de Riesgos	¿Cuándo seleccionarlo?
	Se verificará previamente, que el beneficio obtenido por esta acción sea mayor al costo sus consecuencias para la Empresa.
Eliminar	Se seleccionará esta alternativa, cuando es factible eliminar la causa raíz que ocasiona el riesgo, verificando previamente, que el beneficio obtenido por esta acción sea mayor al costo sus consecuencias para la Empresa.

6.17.3 Razones para la selección de la estrategia de tratamiento al riesgo

De acuerdo a la estrategia de tratamiento del riesgo seleccionada, se deberán desarrollar las siguientes actividades.

Tipo de Tratamiento de Riesgos	Descripción
Evitar	Dejar de realizar la actividad que genera el riesgo debido a que el nivel de riesgo es inaceptable. Evitar implica generalmente rehacer el diseño del plan operativo o de negocios (v.g. no pescar ciertas especies debido a que existe un elevado nivel de riesgo de que se presenten variaciones en la estructura de costos que puedan generar grandes pérdidas para el Grupo).
Reducir o Mitigar	<p>Establecer controles para disminuir la probabilidad de ocurrencia del riesgo. (v.g. establecer un número de toma de muestras en la línea de producción con el fin de disminuir la probabilidad de que se obtenga harina de pescado de baja calidad o contaminada).</p> <p>Establecer controles para disminuir el impacto financiero del riesgo (v.g. disminuir la delegación de autoridad financiera en el control de gastos).</p>



Tipo de Tratamiento de Riesgos	Descripción
Transferir	Transferir a un tercero con la capacidad financiera o especialización necesaria para administrar adecuadamente el riesgo, o enfrentar las pérdidas originadas ante la ocurrencia de la adversidad (v.g. contratar seguros contra todo riesgo para las embarcaciones pesqueras). Los seguros transfieren el riesgo de pérdida financiera del asegurado al asegurador. Las transferencias parciales consisten en compartir los riesgos, dando la responsabilidad a un tercero.
Retener	Conservar el riesgo en su presente nivel realizando una adecuada administración y monitoreo (v.g. realizar gastos mayores a los presupuestados con el fin de cumplir con urgencias de extracción o producción).
Explotar	No definir actividades de control con la finalidad de que el riesgo se materialice, para lo cual la Empresa, deberá diseñar mecanismos para obtener beneficios de las oportunidades que se presenten.
Eliminar	Eliminar la causa raíz que ocasiona el riesgo. Además, la Empresa deberá diseñar actividades para afrontar las posibles consecuencias de la eliminación realizada.

Una vez establecidas las medidas, se define un responsable del seguimiento de su respectiva implementación. La persona nombrada evaluará la medida escogida con relación al costo/beneficio para proceder a elaborar el mapa de riesgos, el cual permitirá visualizar todo el proceso de valoración, análisis y manejo de los riesgos. Por último, se deben implementar las medidas seleccionadas, realizar nuevos ciclos de evaluación para determinar el nuevo riesgo residual y especificar la forma de monitoreo para la medida de tratamiento implementada.

6.17.4 Planes de acción de tratamiento al riesgo

Las estrategias de tratamiento al riesgo definidas en la fase previa deben estructurarse en planes de acción a implementar con el objetivo de materializar el efecto esperado de la estrategia seleccionada. La definición



de los planes de acción se realiza siguiendo el mismo flujo de responsabilidades aplicado en la definición de estrategias de tratamiento al riesgo. Es importante que se defina y documente formalmente la actividad a ser implementada mediante el plan de acción, al responsable de realizarla, y la fecha de inicio y fin.

El cumplimiento de los planes de acción debe ser revisado de manera continua. Para ello, los Dueños de los Procesos deben reportar a los Responsables titular/suplente de la GIR y al Gerente General de la empresa el estatus de la implementación de los planes de acción programadas, así como el planteamiento de las medidas de acción correctivas en el caso de desviación de los plazos determinados. En tal caso se debe identificar si existe algún factor crítico que dificulta su respectiva implementación. De ser un aspecto crítico, se deberá presentar un informe del caso al Comité técnico Riesgos y éste evaluará reportarlo al Directorio para que apruebe las medidas correctivas respectivas y permita se programe la fecha de implementación.

Se permitirá una sola reprogramación de la fecha de implementación de los Planes de Acción, antes que el Responsable Titular/Suplente los reporte como vencidos al Comité técnico de Riesgos.

Los responsables de la GIR solicitarán a las áreas el sustento físico y/o electrónico de la implementación del plan o planes de acción desarrollados.

El seguimiento de los planes de acción tiene los siguientes objetivos:

- Realizar seguimiento de los compromisos adquiridos por los responsables de la ejecución e implementación del plan de acción.
- Determinar el nivel de avance de la implementación de los planes de acción definidos.
- Identificar las causas de posibles retrasos en la implementación de los planes de acción.

6.17.5 Indicadores de desempeño de la Gestión Integral de Riesgos (KRI's)

Los indicadores de desempeño de la GIR (Key Risk Indicators - KRI's) son métricas financieras u operacionales que ofrecen una base razonable para estimar la probabilidad de ocurrencia y severidad de uno o más eventos de riesgo. Son de vital importancia para el desarrollo del plan de tratamiento del riesgo debido a que permite desarrollar un sistema de predicción y

seguimiento del tratamiento de los riesgos. Para que los KRI sean efectivos, deben ser monitoreados de manera continua.

a. Identificación de riesgos que requieren de un KRI

- Los KRI's son aplicados para los riesgos residuales de severidad igual o mayor a Alto y que estén relacionados a un proceso crítico.
- El Dueño del Proceso identifica los riesgos que requieren un KRI con el fin de monitorearlos de manera permanente, a través de la definición de Indicadores Claves de Riesgos.
- Luego de haber identificado los riesgos; el dueño del proceso procede a completar y validar la plantilla de documentación de KRI's, la cual envía al Responsable titular/Suplente de la GIR para su revisión.
- La plantilla debe contener información como: nombre, definición, fórmula del indicador, objetivos, tipo de indicador, fuente de información, periodicidad, responsable de la revisión. El formato se adjunta en el (Anexo 13). Además la información del KRI debe ser incluida en el Formato de registro de las estrategias de tratamiento al riesgo.
- Los KRI's definidos son evaluados mensualmente para monitorear la tendencia de los indicadores en el tiempo, y compararlos con el valor objetivo de los mismos, de tal manera que se pueda tomar oportunamente las acciones preventivas necesarias y cambiar una tendencia negativa del indicador.
- Los KRI's para los procesos críticos deben ser actualizados anualmente.

b. Las restricciones de un KRI

Existen ciertas restricciones que un KRI debe cumplir para que se sirva como un componente eficiente en el tratamiento del riesgo, las cuales son las siguientes.

- Ser dinámico: Debe reflejar los cambios y debe actualizarse con nueva información.
- No redundante: Si existe una alta correlación con otro indicador, solamente uno de ellos debe considerarse.
- Medible: Debe ser cuantificable y verificable. Asimismo, se debe establecer claramente la fórmula de cálculo del indicador con la finalidad de evitar errores en la medición.



- De fácil implementación: La obtención del indicador y su incorporación en la empresa debe ser asequible; es decir, se debe contar con dicha información en los sistemas de la empresa para su fácil obtención.
- Ser auditable: El indicador y la información con la que se obtiene, debe estar adecuadamente documentada.
- Revisados sobre una base de tiempo y deben permitir el monitoreo del comportamiento del riesgo dentro de los niveles de apetito y tolerancia establecidos, con el fin de poder tomar las acciones correctivas o preventivas de manera oportuna.
- Estar vinculado a los riesgos residuales que tengan una calificación de altos (críticos) identificados.

c. Las restricciones de un KRI

El valor meta considerado para KRI debe alinearse directamente con el riesgo que la empresa defina y se deben actualizar obligatoriamente con una periodicidad igual o menor periodicidad de la actualización del apetito, riesgo y capacidad al riesgo de la Empresa.

d. Monitoreo de las Medidas de desempeño (KRI's)

Trimestralmente, se debe llevar a cabo la evaluación de KRI's con el fin de determinar la necesidad de modificar estrategias de tratamiento y planes de acción. Para esto, se deben realizar las siguientes actividades:

- Evaluar que el nivel de los KRI's se encuentre dentro del valor definido. De no ser así, se deberá indagar los motivos que generaron esta desviación a través de entrevistas a los encargados de los procesos involucrados.
- Desarrollar reuniones con los responsables de monitorear los KRI y los Dueños de Procesos, con la finalidad de identificar oportunidades de mejora en el diseño de los indicadores así como para poder identificar la necesidad de implementará nuevos KRI, siguiendo los lineamientos previamente definidos.

6.18 Seguimiento y monitoreo continuo

6.18.1 Cronograma de seguimiento a los planes de acción

Los planes de acción definidos deben consolidarse y monitorearse a través de un cronograma de implementación utilizando la herramienta Gantt. Los

planes de acción asociados a riesgos residuales con mayor criticidad deben ser priorizados.

6.18.2 Evaluación de riesgo residual

El riesgo residual sirve como indicador para medir la efectividad de los controles, para lo cual, es necesario medir la variación entre el riesgo inherente y el residual; mientras un control disminuya más la criticidad de un riesgo será más efectivo.

Los riesgos son calificados en cuatro (4) niveles en función a su criticidad: Extremo, Alto, Moderado y Bajo. Asimismo, los controles son calificados en tres (3) niveles en función a su efectividad: Fuerte, Moderado y Débil.

La tabla que se presenta a continuación sirve para entender a modo de ejemplo la tendencia que podría presentarse entre la variación del nivel de un riesgo inherente con la variación del nivel de un riesgo residual dependiendo de la calificación del control:

Riesgo Inherente	Calificación del Control	Riesgo residual
Extremo	Fuerte	Moderado
Extremo	Moderado	Alto
Extremo	Débil	Extremo
Alto	Fuerte	Bajo
Alto	Moderado	Moderado
Alto	Débil	Alto
Moderado	Fuerte	Bajo
Moderado	Moderado	Moderado
Moderado	Débil	Moderado
Bajo	Moderado	Bajo
Bajo	Débil	Bajo

El mapa de riesgos debe ser actualizado de manera que refleje el efecto reductor de los controles sobre la probabilidad y el impacto del riesgo inherente.

6.18.3 Criterios para la evaluación de controles

La evaluación de los controles permite determinar el efecto de los mismos sobre los riesgos a los que se encuentran asociados. La evaluación de controles se realiza en dos niveles: (i) diseño del control (ii) efectividad del control.



Un control se considera deficiente en los siguientes casos:

Deficiencia en	Descripción
Diseño del control	<ul style="list-style-type: none"> - Si el diseño o la operación del control no permiten prevenir o detectar errores en un período de tiempo. - Si está faltando el control necesario para alcanzar el objetivo del control.
Efectividad del control	<ul style="list-style-type: none"> - Cuando un control apropiadamente diseñado no opera como está diseñado. - Cuando el responsable de realizar el control no posee la autoridad y calificación necesaria para realizarlo.

6.19 Actividades de reporte

Mensualmente, el responsable de la GIR en cada Empresa debe revisar con los responsables de los procesos el avance en la ejecución del Plan de GIR. De presentarse un retraso, el responsable de la implementación de riesgos deberá identificar su causa, considerando:

- Si se debe a una falta de recursos deberá elevar la solicitud a la Alta Dirección.
- Si se debe a ineficiencias en la gestión de los dueños de procesos. Deberá priorizar solucionar la causa de las mismas y las tareas pendientes.
- Si se debe a una mala estimación de las actividades, deberá gestionar el cambio del cronograma de implementación del Plan de GIR, el cual deberá ser aprobado por la Alta Dirección.

Posteriormente, deberá enviar el cronograma y avance del Plan de la GIR para la revisión y aprobación de la Alta Dirección.

Por otro lado, una vez concluida la evaluación, la autoevaluación o evaluación interna del nivel de madurez en GIR, los responsables de la implementación de riesgos en las Empresas de la Corporación y el Responsable de Riesgos de FONAFE deberán reunirse con el fin de compartir experiencias y generar sinergias entre sus organizaciones para mejorar el desempeño de riesgos.

Por último, anualmente el personal involucrado en el desarrollo de la GIR en cada una de las Empresas deberá reunirse internamente con la finalidad de detectar oportunidades de mejora en la política y metodología de riesgos.

NOTA: La Guía de Gestión Integral de Riesgos está basada en el Informe del "Sistema Efectivo de Análisis de Riesgos (SEAR)" y en los informes de "Acompañamiento en la Implementación del Sistema Efectivo de Análisis de Riesgos, con Contrato No. F-019-0-



13202 y No. F-035-0-13202 respectivamente, quienes fueron elaborados por el consultor Ernst & Young Asesores S. Civil de R. L.

