Manual de Metodología para la Gestión de Riesgos

Versión	Fecha	Puntos Modificados
3	17/6/2021	• Se consignó en la sección "6.1 Generalidades" la autoevaluación de la GIR y su relación con el Plan de la GIR. • Se precisó en la sección "6.5.1 Definición y tipos de controles" que los controles son formalizados en documentos internos o externos que cuenten con la aprobación correspondiente. • Se agregó la sección "6.8 Mejora Continua" que contiene la frecuencia de actualización del apetito de riesgo.

Áreas Responsables	Nombres y Cargos
Elaborado: **Oficina de Planeamiento y Mejora Continua**	Amaru Aragón Especialista de Control de Gestión Miguel Tito Jefe de Planeamiento y Mejora Continua
Revisado: **Gerencia de Administración y Finanzas**	Andrés Millones Gerente de Administración y Finanzas
Homologado: **Oficina de Planeamiento y Mejora Continua**	Deymer Barturén Especialista en Calidad y Mejora de Procesos Miguel Tito Jefe de Planeamiento y Mejora Continua
Aprobado: **Gerencia General**	Edgar Román Gerente General (e)

INDICE

I. OBJETIVO

Establecer los métodos, las herramientas y las fuentes de información que deberán utilizarse para efectuar la Gestión Integral de Riesgos (en adelante GIR) en Activos Mineros S.A.C. (en adelante AMSAC).

II. ALCANCE

Esta metodología es aplicable a todas las áreas de la empresa, y debe ser utilizada para servir de guía para la planificación, identificación, valoración y respuesta a los riesgos que enfrenta AMSAC, así como para uniformizar los criterios de evaluación de los riesgos estratégicos, operacionales y de proyectos, financieros y de cumplimiento. Los riesgos asociados a normas específicas, tales como Seguridad y Salud en el Trabajo, Gestión Ambiental, Seguridad de la Información, podrán hacer uso de métodos propios de dicha gestión.

III. DOCUMENTOS DE REFERENCIA

La metodología está alineada a la normativa nacional indicada en la Sección 3 de la Política de Gestión de Riesgos, así como al Marco de Referencia Integrado COSO.

IV. VIGENCIA

Este documento entrará en vigencia a partir del primer día hábil después de la fecha de aprobación.

V. RESPONSABILIDADES

Los responsables de la gestión de riesgos son:

- Riesgos a nivel entidad: Comité Técnico de Riesgos y Alta Gerencia.
- Riesgos a nivel de procesos: Dueños de proceso, quienes usualmente ocupan un puesto gerencial o de jefatura y son conocedores del proceso de inicio a fin.
- Riesgos a nivel de proyectos: Administradores de contrato, jefes y gerentes de área responsables de la gestión de los proyectos a cargo de la empresa.

VI. METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS

6.1. Generalidades

La presente metodología es complementaria al Lineamiento de Gestión Integral de Riesgos para las empresas bajo el ámbito de FONAFE, así como de las disposiciones ulteriores que se emitan sobre la materia. En caso de aparente conflicto o contradicción, primará siempre lo dispuesto por FONAFE.

La revisión y/o actualización de los procesos se realiza al menos una vez al año, con la participación de los dueños de proceso; como resultado también se pueden actualizar las matrices de riesgo de la empresa, a nivel de procesos.

La metodología de Gestión de Riesgos de AMSAC considera los siguientes seis (6) componentes:

- Planificación de la gestión de riesgos
- Identificación de riesgos
- Valoración y priorización de los riesgos.
- Actividades de control.
- Respuesta al riesgo residual.
- Seguimiento y monitoreo

Anualmente se realiza la Autoevaluación de la Gestión Integral de Riesgos, para lo cual se utiliza la herramienta de evaluación aprobada por FONAFE. Como resultado, se identifican oportunidades de mejora, que se atienden con las actividades propuestas en el Plan de la GIR. El Comité Técnico de Riesgos propone el Plan de la GIR para su aprobación por el Directorio.

6.2. Planificación de la gestión de riesgos

La planificación de la GIR es la fase inicial para que las actividades sean implementadas de manera eficiente, oportuna y alineadas a las necesidades de AMSAC. Es requisito previo a la implementación de la GIR, lo siguiente:

- **Definición de objetivos a nivel entidad**
  Estos objetivos están alineados con la misión y visión y se encuentran en el Plan Estratégico Institucional y el Plan Operativo Institucional.
- **Mapeo de Procesos**
  AMSAC cuenta con un mapa de procesos de toda la organización, el cual ha sido elaborado conforme a los lineamientos de FONAFE.
- **Definición de objetivos a nivel de proceso y priorización de procesos**
  Las gerencias, en coordinación con los dueños de procesos definen los objetivos de los procesos, los cuales son registrados en las Fichas de Procesos. Posteriormente se seleccionan los procesos críticos, conforme a los lineamientos de FONAFE.
- **Determinación del apetito, tolerancia y capacidad de riesgo**
  El apetito, tolerancia y capacidad al riesgo es propuesta por el Comité Técnico de Riesgos y aprobada por el Directorio, en función a los objetivos del Plan Estratégico Institucional, lo cual representa el marco para la GIR.
  - Apetito de riesgo
    Es el nivel de riesgo que AMSAC decide asumir durante el proceso de consecución de sus objetivos y figura como la zona baja en el mapa de riesgos (verde). El apetito de riesgo se fija tomando en cuenta el nivel de riesgo tope que se acepta para no afectar el cumplimiento de los objetivos.
    Una vez definido el apetito de riesgo, se lleva a cabo la identificación de los riesgos a nivel entidad, por procesos y de proyectos, y en función a ello se procede a definir la tolerancia al riesgo y capacidad de riesgo de AMSAC.
  - La tolerancia al riesgo
    Es la desviación con respecto al apetito de riesgo; es decir la variación del nivel de riesgo que para AMSAC 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 AMSAC puede soportar sin que interfiera en su continuidad. Es representada por la zona alta y extrema en el mapa de riesgos (anaranjado y rojo).

  Estos elementos se expresan como riesgo residual, es decir, se evalúan después de aplicar los controles establecidos conforme a lo indicado en el numeral 6.4. de la presente Metodología.
  Para definir la tolerancia y capacidad de riesgo se evalúa la afectación a:
  - Objetivos de la empresa
  - Aspectos jurídicos y normativos
  - Operaciones de la empresa
  - Tecnologías de la información
  - Indicadores financieros
  - Reputación

6.3. Identificación de Riesgos:

Es el proceso de relevamiento y documentación del inventario de riesgos que puedan afectar el logro de los objetivos estratégicos, operacionales y de proyectos, financieros y de cumplimiento de AMSAC.

El primer paso en esta etapa es la identificación de los eventos, los cuales son situaciones o elementos potenciales de origen interno o externo que pueden afectar a la entidad, con consecuencias positivas (oportunidades) o negativas (riesgos). El Plan Estratégico Institucional cuenta con un análisis FODA, es decir un mapeo de fortalezas, oportunidades, debilidades y amenazas, que sirve para analizar en qué medida estos eventos afectan el cumplimiento de su misión. Los factores externos incluyen factores económicos, medioambientales, políticos, sociales y tecnológicos. Los factores internos reflejan las selecciones que realiza AMSAC e incluyen la infraestructura, personal, procesos y tecnología.

Posteriormente se identifican los riesgos que afectan a nivel Entidad, a nivel procesos y a nivel proyectos. Al primer nivel corresponderán los riesgos de carácter general o transversal a toda la empresa; mientras que, al segundo, aquellos riesgos específicos que afectan a un proceso en particular. Al tercer nivel corresponderán los riesgos propios de cada proyecto en su zona de influencia y su marco operativo y contractual.

Las técnicas para llevar a cabo el proceso de identificación de riesgos pueden ser:

- "Lluvia de ideas" en un taller de trabajo, en donde se convoque a los responsables y participantes clave de los procesos y proyectos, quienes mejor conocen acerca de los mismos.
- Por propuesta de las Gerencias (riesgos a nivel Entidad) revisados por el Comité Técnico de Riesgos.
- Por propuesta del dueño de proceso o del Responsable de GIR, revisado por el Comité Técnico de Riesgos.
- Por propuesta de los administradores de contrato o jefes de área, respecto de los proyectos que tienen bajo su gestión.

Como parte del proceso de identificación de riesgos, es necesario conocer qué es un riesgo y cuáles son los tipos de riesgo, así como la relevancia de conocer y priorizar los procesos en donde podrían presentarse los riesgos:

6.3.1. Definición y tipos de riesgos

- Riesgo:
  Incertidumbre o condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de AMSAC. También se dice que un riesgo es la amenaza que enfrenta una empresa cuando un evento o acción puede afectar adversamente su habilidad de alcanzar los objetivos corporativos y maximizar valor.

- Tipos de Riesgo:
  a. Por el objetivo que afecta el riesgo:
  - Riesgo Estratégico
    Es aquél que, de presentarse, puede afectar el logro de la misión o de los objetivos estratégicos de la empresa.
  - Riesgo Operativo
    Aquel riesgo que afecta el logro de los objetivos operacionales de la empresa, amenazando el uso eficaz y eficiente de los recursos. Incluye riesgos originados por errores o falta de capacidad de las personas que ejecutan los procesos y proyectos, fallas o ineficiencias de los procesos o proyectos, deficiencias en los sistemas de información, entre otros.
  - Riesgo Financiero
    Aquel riesgo que afecta el logro de los objetivos financieros de la entidad, tales como aquellos relacionados con la formulación y ejecución presupuestal, la elaboración y emisión de estados financieros, el manejo de la tesorería, la custodia de los activos, entre otros.
  - Riesgos de Cumplimiento
    Riesgos que impactan el cumplimiento de leyes y normas aplicables, además de la normativa interna (políticas, códigos, directivas, procedimientos, instructivos, entre otros), compromiso con la ética y compromiso ante la comunidad.

- Riesgos de Fraude
  Riesgos que impactan de manera negativa en la reputación de la empresa o que generan pérdidas económicas, siempre que sean causados por la acción de un colaborador con la intención de lograr un beneficio propio o de un tercero, relegando los intereses de AMSAC.

b. *Por su origen:*
   - Internos o endógeno
     Riesgos que se generan en los procesos internos.
   - Externos o exógenos
     Riesgos que provienen de eventos del ambiente externo.

c. *Por el nivel de la organización en el que se encuentran:*
   - Nivel entidad
     Riesgos que afectan a toda la empresa de manera transversal, pudiendo ocurrir en cualquier proceso particular.
   - Nivel de proceso
     Riesgos que afectan el logro de un proceso específico.
   - Nivel de proyectos
     Riesgos que afectan la gestión de un proyecto a cargo de AMSAC.

d. *Por su frecuencia:*
   - Rutinarios
     Riesgos que se podrían presentar constantemente.
   - No rutinarios
     Riesgos que se podrían presentar de manera poco frecuente.

Las fuentes potenciales de riesgos pueden ser, entre otras y sin limitarse a las indicadas a continuación, las siguientes:

- Procesos mal definidos, ineficientes o con errores
  - Procesos mal delimitados, sin un dueño de proceso a cargo.
  - Ineficiencias o “cuellos de botella” en los procesos.
  - Errores en las operaciones.
  - Error en la información que se genera en los procesos.
  - Falta de recursos para realizar las operaciones.
  - Falta de cumplimiento de los plazos del proceso.

- Carencia de políticas internas, o en caso de existir, que no estén actualizadas ni difundidas
  - Inexistencia de políticas internas.
  - Desalineamiento de las políticas internas respecto de la estrategia de la empresa.
  - Desactualización de las políticas internas.
  - Falta de difusión de las políticas internas.
  - Falta de supervisión del cumplimiento de las políticas internas.

- Errores del personal o personal poco capacitado o motivado
  - Personal no alineado a los conocimientos, competencias y habilidades requeridas para el puesto que ocupan.
  - Falta de capacitación constante al personal.
  - Falta de una línea de carrera para el personal.
  - Falta de un adecuado clima laboral.
  - Presencia de eventos de fraude y corrupción.
  - Alta rotación del personal.

- Debilidad de los sistemas de información
  - Inexistencia de un Plan Estratégico de Tecnología de Información y Plan de Continuidad, y supervisión de su cumplimiento.
  - Errores en la programación de los sistemas.
  - Problemas de calidad de información, ingreso de la información y actualización de la base de datos.
  - Fallas en la seguridad de la información.
  - Interrupción de la continuidad de los sistemas y comunicaciones.
  - Fallas en la interconexión de la oficina central y los proyectos.
  - Errores en el desarrollo de los sistemas.
  - Errores en la integración de los sistemas.
  - Falta de capacitación de los usuarios.
  - Inadecuada inversión en tecnología.

- Eventos externos
  - Cambios en la regulación o vacíos en la legislación.
  - Falta de estabilidad política, social o económica.
  - Entorno del sector en el que se desenvuelve la empresa.
  - Ocurrencia de desastres naturales.
  - Terrorismo, vandalismo o hurtos.
  - Crisis internacionales.
  - Fallas en los servicios críticos provistos por terceros.
  - Fallas en los servicios públicos.
  - Cambio climático y del medio ambiente.

6.3.2. Inventario y priorización de procesos

AMSAC realiza el inventario de procesos y la matriz de procesos conforme a lo indicado en E3.1.M1 Metodología para la Gestión por Procesos.

6.3.3. Inventario y priorización de proyectos

AMSAC realiza el inventario de proyectos conforme a una Metodología para la Gestión de Portafolio de Proyectos, alineada con la Programación Multianual de Inversiones del Invierte.pe.

6.4. Evaluación de los riesgos

Esta fase tiene como finalidad efectuar un análisis de los riesgos identificados en la etapa previa, para establecer una valoración o nivel de criticidad, tanto a nivel entidad, como a nivel de los procesos y proyectos, de acuerdo con los criterios de evaluación de riesgos.

El responsable titular de la GIR validará que cada 2 años, se actualicen las evaluaciones de riesgos de los procesos y controles de AMSAC. En el caso de los procesos críticos, estas actualizaciones se realizarán anualmente; mientras que, en el caso de los proyectos, estas se realizarán al menos trimestralmente.

El Comité Técnico de Riesgos es el responsable de aprobar la evaluación de los riesgos de cada proceso. Respecto de los proyectos, la aprobación de la evaluación la realizará el jefe de área.

Se evaluarán los riesgos desde 2 criterios: la probabilidad de ocurrencia y el impacto de la materialización de los eventos de riesgo, utilizando una combinación de factores cualitativos y cuantitativos.

a. Definición de los criterios de evaluación de riesgos

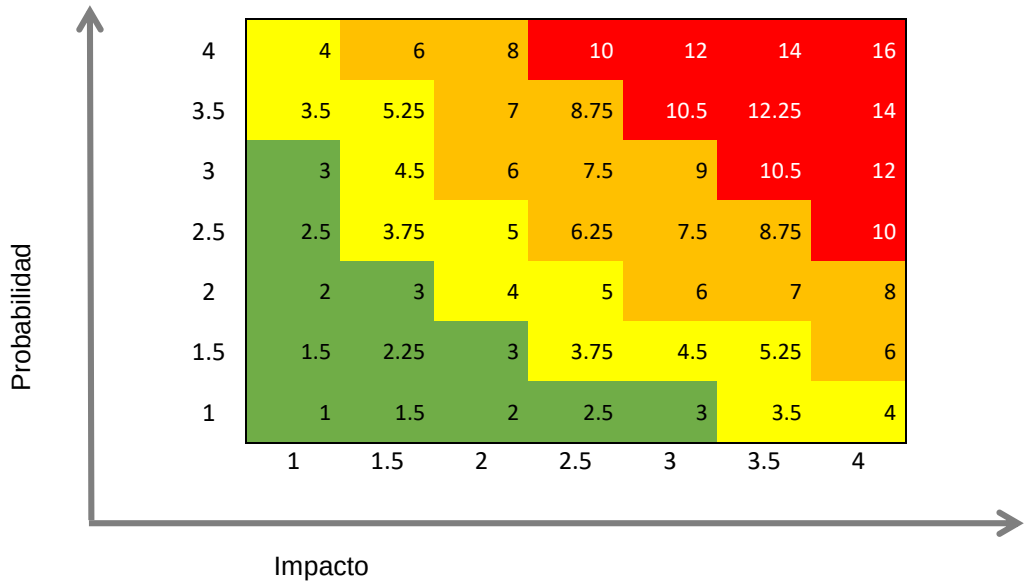
- **Probabilidad de ocurrencia**
  Es el nivel de posibilidad de que ocurra el evento de riesgo en el periodo de un año. Puede ser estimada en función a cuántas veces históricamente ha ocurrido el evento de riesgo en AMSAC o en la posibilidad de que ocurra en el futuro o por otros criterios cualitativos.

- **Impacto**
  Nivel o grado de exposición de AMSAC ante un riesgo, o cuantía de la pérdida que se pudiera generar si ocurriera el evento de riesgo. También se pueden considerar otros criterios cualitativos.

Se utilizará una escala de 4 niveles de evaluación de riesgos, tanto para el criterio de probabilidad, como para el de impacto, los cuales serán: extremo, alto, medio y bajo.

Se otorgará el valor de 1 al nivel “bajo”, el valor de 2 al nivel “medio”, el valor de 3 al nivel “alto” y el valor de 4 al nivel “extremo”. El cruce o multiplicación de las puntuaciones de ambos criterios dará el resultado final o nivel (severidad) del riesgo: extremo, alto, medio o bajo.

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



A continuación, se indica la descripción de las severidades al riesgo resultantes:

Severidad del Riesgo	Descripción
Extremo	Se requiere acción urgente. Planes de acción requeridos, implementados y reportados a la Alta Dirección.
Alto	Se requiere acción urgente. Planes de acción requeridos, implementados y reportados a las Gerencias y Jefaturas.
Medio	Se requiere atención importante. Planes de acción, implementados y reportados a las Gerencias y Jefaturas.
Bajo	Debe ser administrado con procedimientos normales de control.

b. Definición de los factores para la evaluación de riesgos

- **Factores cuantitativos**
  Son medidas o escalas numéricas que indican la magnitud de las consecuencias potenciales de la materialización de los riesgos, tanto a nivel de impacto, como de probabilidad de ocurrencia. Estas escalas se pueden modificar o ajustar ante el cambio del entorno económico, político, de inversión u otro de importancia de AMSAC.

- **Factores cualitativos**
  Son factores que utilizan escalas descriptivas para complementar los factores cuantitativos acerca de la magnitud de consecuencias potenciales de la materialización de los riesgos, tanto a nivel de impacto, como de probabilidad de ocurrencia. Tal como los factores cuantitativos, estas escalas se pueden modificar o ajustar ante el cambio del entorno económico, político, de inversión u otro de importancia de AMSAC.

A continuación, se detallan los factores cuantitativos y cualitativos referenciales para los criterios de impacto y probabilidad de ocurrencia de AMSAC, los que necesariamente se complementan con el juicio experto de quien evalúa el riesgo y quien lo aprueba:

IMPACTO				
Cuantitativos (expresado en soles)				
Criterios	**BAJO**	**MODERADO**	**ALTO**	**EXTREMO**
Potencial pérdida financiera	Impacto adverso menor igual a 3 UIT	Impacto adverso mayor a 3 UIT pero menor a 8 UIT	Impacto adverso mayor a 8 UIT pero menor a 25 UIT	Impacto adverso mayor a 25 UIT
Cualitativos				
Criterios	**BAJO**	**MODERADO**	**ALTO**	**EXTREMO**
Eventos de fraude	No se presentan eventos de fraude.	Se presentan eventos irregulares aislados, cometidos por personal de cargos operativos.	Se presentan eventos de fraude, cometidos por altos ejecutivos.	Se presentan eventos de fraude por colusión con proveedores u otros *stakeholders*.
Reputación / Pérdida de confianza	No se presentan daños en la reputación.	Daño en la reputación con alcance local, que podría originar desconfianza en ciertas entidades relacionadas.	Daño en la reputación con alcance local, pero con potencial de escalamiento si no se gestiona adecuadamente.	Daño en la reputación con alcance nacional o global, que origina la pérdida de confianza de las principales entidades relacionadas.
Incumplimiento ante reguladores	No se dan casos de incumplimiento de normativa externa legal, sectorial, laboral ni tributaria.	Casos aislados de incumplimiento de normativa externa legal, sectorial, laboral o tributaria, que podrían determinar llamada de atención o sanciones administrativas	Casos aislados de incumplimiento de normativa externa legal, sectorial, laboral o tributaria, que podrían determinar el pago de multas o indemnizaciones leves o moderadas.	Casos severos de incumplimiento de normativa externa legal, sectorial, laboral o tributaria, que decantan en el pago de multas o indemnizaciones elevadas.
Interrupción de operaciones	Interrupción de operaciones menor a 4 horas.	Interrupción de operaciones entre 4 y 8 horas.	Interrupción de operaciones entre 8 y 48 horas.	Interrupción de operaciones mayor a 48 horas.

Disponibilidad de información / Confiabilidad del sistema	No disponibilidad oportuna de información, pero que no afecta la continuidad del negocio.	No disponibilidad oportuna de la información crítica, aquella que: (i) es requerida por el regulador, o (ii) es estratégica para la empresa; lo cual conlleve a una breve interrupción (menor a 8 horas) de procesos clave.	No disponibilidad oportuna de la información crítica, aquella que: (i) es requerida por el regulador, o (ii) es estratégica para la empresa; lo cual conlleve a una interrupción mayor a 8 horas de procesos clave.	Pérdida de información crítica de la empresa o de terceros que no se pueda recuperar; lo cual conlleve a la interrupción de procesos clave o continuidad del negocio. Uso de un sistema no confiable.

PROBABILIDAD				
Cuantitativos				
Criterios	**BAJO**	**MODERADO**	**ALTO**	**EXTREMO**
Frecuencia de eventos	Remota: Históricamente el evento no ha ocurrido, pero podría ocurrir una vez al año; o menor al 5% de los casos.	Ocasional: El evento podría ocurrir 2 a 4 veces al año; o entre el 5% y 15% de los casos.	Probable: El evento podría ocurrir 5 a 12 veces al año, o con una periodicidad menor; o entre el 15% y 25% de los casos.	Frecuente: El evento podría ocurrir más de 12 veces al año; o mayor al 25% de los casos.

6.5. Actividades de Control

Las actividades de control, si bien forman parte de un componente diferente al de “Evaluación de Riesgos” del Marco de Referencia Integrado COSO y de la normativa de la Contraloría General de la República, están estrechamente asociadas a la identificación, valoración y respuesta a los riesgos.

El objetivo de esta etapa es identificar los controles existentes en AMSAC y diseñar e implementar los que sean necesarios para mitigar o reducir el riesgo, o para prevenir su ocurrencia o detectarla luego de ocurrido el evento del riesgo.

AMSAC deberá diseñar e implementar las acciones de control específicas que sean necesarias y evaluar al mismo tiempo que éstas sean efectivas en cuanto a su diseño y su operatividad, determinando si cubre de manera razonable el riesgo o no. De no cubrirlo de manera razonable, se deberán establecer nuevos controles o fortalecer los controles existentes que permitan compartir, mitigar o reducir el riesgo.

Los controles definidos serán consignados en la Matriz de Riesgos y Controles respectiva.

En algunos casos, una sola actividad de control afectará a un grupo de riesgos. En otros casos, será necesaria más de una actividad de control para mitigar un riesgo.

6.5.1. Definición y tipos de controles

- Control
  Se define Control como toda medida o actividad adoptada para mitigar el impacto y/o reducir la probabilidad de ocurrencia de los riesgos.

  El control se formaliza en un documento interno (procedimiento, ficha de proceso, manual, entre otros) o se encuentra contenido en algún documento externo (lineamiento de FONAFE, formato del reporte de alguna entidad regulatoria, entre otros) los cuales deben estar debidamente aprobados.

Al diseñar un control se debe tener consideración lo siguiente:

- Quién lo ejecutará: deberá tener un responsable claramente definido;
- Cuándo lo ejecutará: deberá tener una frecuencia o período de ejecución definido, dependiendo de la frecuencia con la que podría ocurrir el riesgo y sus características;
- Qué ejecutará: deberá tener actividades claramente definidas;
- Cómo lo ejecutará: deberá entenderse cómo el control mitiga el riesgo;
- Evidencia: deberá contemplar el dejar evidencia (electrónica o física) que permita en el tiempo hacer un seguimiento a la ejecución del control;
- Otros: ver si está documentado y comunicado dentro de la empresa.

- Tipos de Control
  - Según la oportunidad en que se ejecuta el control:

Clasificación	Descripción
Preventivo	Actividad que previene errores o mitiga riesgos antes de que afecten a AMSAC.
Detectivo	Actividad que identifica errores en la toma de decisiones o en el procesamiento dentro de un lapso aceptable.

  - Según la automatización en la aplicación del control:

Clasificación	Descripción
Automático	Actividad que es realizada internamente por un sistema.
Semi - Automático	Actividad que depende de la habilidad de la persona que lo ejecuta para prevenir o detectar errores incurridos utilizando información proveniente de un sistema.
Manual	Actividad que depende de la habilidad de la persona que lo ejecuta para prevenir o detectar los errores o riesgos que se presenten.

Para la identificación de controles se deberán tomar en cuenta las siguientes consideraciones:

- Existen controles clave y otros secundarios o parciales. El objetivo de la actividad es identificar los controles clave. Los controles clave tienen las siguientes características:
  - Cubre un riesgo crítico, o un conjunto de riesgos no necesariamente críticos.
  - Tienen que poder probarse a través de las evidencias que dejan.
  - Las revisiones de calidad son buenos controles clave, siempre y cuando sean realizadas con regularidad y siguiendo los mismos lineamientos.

- El control debe ser formal y repetible (realizado con una misma frecuencia y por un responsable definido).

- El control de los riesgos debe propender a que una persona no revise su propio trabajo. Para que sea un control debe haber independencia o actividades conflictivas adecuadamente segregadas.

- Un control implica el análisis, la revisión, la aprobación y/o la toma de acción respecto de la prevención o detección de un posible riesgo.

- Una actividad realizada de vez en cuando no es un control.

- Si no se deja evidencia de haber realizado el control, es como si el control no existiera.

6.5.2. Evaluación de las acciones de control

Esta etapa implica realizar la supervisión, seguimiento o evaluación de las acciones y/o controles para hacer frente a los riesgos, tanto a nivel entidad, como a nivel procesos y proyectos.

Es posible incluir nuevas acciones de control, o modificar las actuales, planteando recomendaciones que permitan una mejor gestión de riesgos.

Las evaluaciones de los controles se realizan en 2 niveles:

- Evaluación del diseño del control
  La evaluación del diseño del control consiste en determinar cuán bien definido está el control a nivel teórico; es decir, si la descripción del control cumple con las características antes descritas en el literal “a” del presente numeral, con lo cual debería logra mitigar el riesgo asociado, o una parte de él.

  Se deberá considerar la siguiente escala para determinar la calificación del diseño de un control:

Calificación del Diseños del Control	Características
Fuerte	Un control será considerado “fuerte” en su diseño, si la descripción del control cumple con las características antes descritas en el literal “a” del presente numeral y cuando a criterio del evaluador, se encuentre diseñado de tal forma que al ser aplicado cumpla el objetivo por el cual fue requerido.
Moderado	Un control será considerado “moderado” en su diseño, cuando se contemple en su descripción al menos los criterios que responden a las tres preguntas siguientes: ¿Qué?, ¿Cómo? y ¿Cuándo?, del literal “a” del presente numeral, y cuando bajo criterio del evaluador mitigue el riesgo al menos parcialmente.
Débil	Un control será considerado como “débil” en su diseño, cuando no se contemple en su descripción al menos dos de los criterios que responden a las tres preguntas siguientes: ¿Qué?, ¿Cómo? y ¿Cuándo?, del literal “a” del presente numeral.

- Evaluación de la efectividad operativa del control
  La evaluación de la efectividad operativa del control consiste en determinar cuán bien opera el control respecto del riesgo que mitiga/reduce; es decir, si funciona tal como fue diseñado por un lapso de tiempo determinado (por lo general, un año).

  Para probar la efectividad operativa de controles se deben seleccionar muestras, de acuerdo con la frecuencia en que se ejecuta el control.

  A continuación, se muestra una tabla con el tamaño de muestra a considerar:

Tamaño de muestra	
Frecuencia de la aplicación de control	**Tamaño de la muestra apropiada**
Anual	1
Trimestral	2
Mensual	2 a 5
Semanal	5 a 15
Diaria	20 a 40
Varias veces por día	25 a 60

De acuerdo a los resultados de la evaluación, se considerará si en relación a la efectividad si el control se cumple o no, de acuerdo con la siguiente tabla:

Calificación de la Efectividad Operativa del Control	Características
Fuerte	Un control será considerado "fuerte" en su efectividad operativa, cuando luego de haber sido probado, sobre la base de muestras selectivas, se considera que se está cumpliendo con el objetivo planificado en el diseño; es decir, mitiga gran parte el riesgo asociado.
Moderado	Un control será considerado "moderado" en su efectividad operativa, cuando luego de haber sido probado, sobre la base de muestras selectivas, se considera que mitiga parcialmente el impacto o la probabilidad de ocurrencia del riesgo.
Débil	Un control será considerado "débil" en su efectividad operativa, cuando luego de haber sido probado, sobre la base de muestras selectivas, éste no mitiga o reduce el efecto del riesgo, en términos de su impacto o probabilidad de ocurrencia.

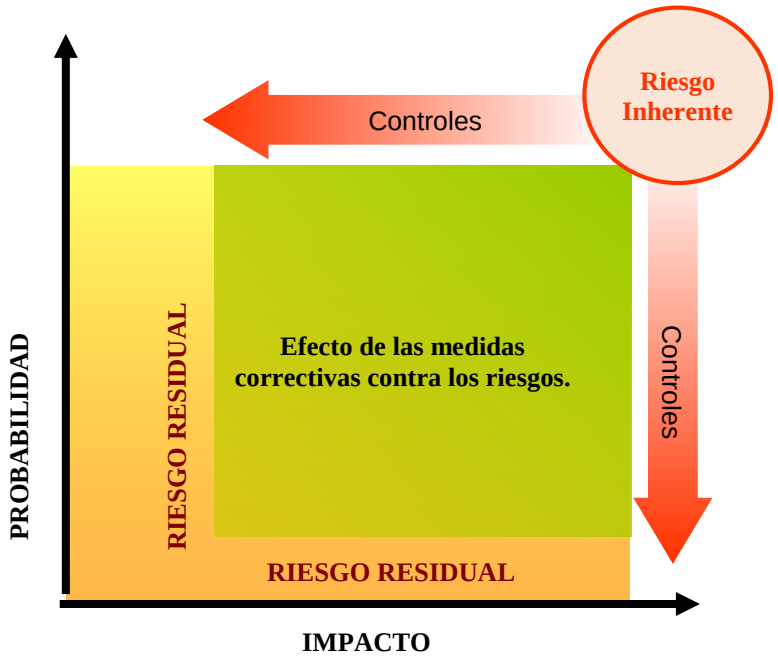
Para conocer la efectividad general de un control se debe considerar las calificaciones obtenidas tanto en el Diseño, como en la Efectividad operativa del Control, la siguiente tabla muestra la interrelación entre ambos niveles de evaluación y la calificación final resultante:

Escala de calificación del nivel general de los controles		
Diseño	Efectividad Operativa	Calificación Final de Controles
Fuerte	Fuerte	**Fuerte**
Fuerte	Moderado	**Moderado**
Moderado	Fuerte	**Moderado**
Moderado	Moderado	**Moderado**
Fuerte	Débil	**Débil**
Débil	**Fuerte**	**Débil**
Débil	**Moderado**	**Débil**
Moderado	**Débil**	**Débil**
Débil	**Débil**	**Débil**

6.5.3. Estimación y análisis del riesgo residual

El riesgo residual es la parte de riesgo inherente que queda remanente luego de haber implementado acciones de control para mitigarlo. Los riesgos residuales son objeto de revisiones periódicas para determinar si deben modificarse los perfiles de riesgo o la arquitectura de control.

A continuación, se presenta una representación gráfica del efecto de los controles en el riesgo inherente y riesgo residual.



a. Estimación del riesgo residual

Para calcular o estimar el riesgo residual se deberá tener en cuenta lo siguiente:

- Valoración de riesgo inherente
  Se deberá considerar la valoración del riesgo inherente como punto de partida para estimar el riesgo residual. En caso existan controles efectivos, el impacto o probabilidad de ocurrencia del riesgo inherente disminuirá, dando como resultado una disminución del nivel de riesgo (o severidad).
  En caso los controles asociados a los riesgos no sean efectivos, el riesgo residual será igual al riesgo inherente.

- Calificación y propósito del control
  En caso existan controles efectivos se mitigará el riesgo inherente, ya sea el impacto, la probabilidad o ambos criterios, dependiendo del diseño del control.

  A continuación, se muestra un cuadro referencial de la estimación del riesgo residual:

Calificación del Control	Efecto del Control
Fuerte	Disminuye máximo en 2 o más puntos el nivel del riesgo inherente.
Moderado	Disminuye máximo en 1 punto el nivel del riesgo inherente.
Débil	No disminuye el riesgo inherente. En este caso el riesgo inherente es igual al residual.

b. Análisis del riesgo residual

Luego de estimar los riesgos residuales, se deberá analizar si éstos se encuentran dentro de los límites de apetito y/o tolerancia al riesgo. Existen 2 posibilidades y son las siguientes:

- Riesgo residual se encuentra dentro de los niveles de riesgo aceptados (apetito y/o tolerancia al riesgo) por AMSAC:
  Se deberá realizar un análisis periódico de los factores internos y externos del riesgo residual (probabilidad e impacto del riesgo, efectividad del control y entorno) con la finalidad de examinar que el riesgo residual se encuentra efectivamente dentro de los niveles de riesgo aceptados por AMSAC. Se deberán continuar con las actividades de control vigentes.
- Riesgo residual no se encuentra dentro de los niveles de riesgo aceptados (apetito y/o tolerancia al riesgo) por AMSAC:
  Se deberá preparar un plan de acción para gestionar los riesgos residuales, ya sea fortaleciendo las medidas de control existentes o diseñando nuevos controles. El plan de acción podría considerar la siguiente información:
  - Descripción de la actividad de mejora
  - Proceso, riesgos y controles relacionados
  - Responsable de la implementación de la mejora
  - Lineamientos para la implementación
  - Fecha límite de ejecución de la actividad de mejora

6.6. Respuesta a los riesgos

Esta fase tiene como finalidad seleccionar una estrategia de respuesta o gestión de los riesgos, a fin de mitigar o reducir su impacto o probabilidad de ocurrencia, los cuales se concretan en planes de acción.
Las estrategias o respuestas a los riesgos se deberán seleccionar de acuerdo al nivel o severidad del riesgo, así como al apetito y/o tolerancia al riesgo que ha definido la Alta Gerencia.

a. Definición de las estrategias de respuesta a los riesgos

Las estrategias o respuestas al riesgo son acciones realizadas para lograr una gestión del riesgo dentro de los márgenes deseados (apetito y/o tolerancia al riesgo). AMSAC definirá una estrategia para cada riesgo evaluado previamente, seleccionando una de las siguientes opciones:

Tipo de respuesta a riesgos	Cuando seleccionarlo	Actividades
Evitar	Cuando el beneficio de implementar un control sea menor al costo del riesgo inherente y sus posibles consecuencias.	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.

Tipo de respuesta a riesgos	Cuando seleccionarlo	Actividades
Reducir o Mitigar	Cuando el beneficio de implementar un control sea mayor al costo del riesgo inherente y AMSAC se encuentre en la capacidad de realizar el tratamiento del riesgo.	Establecer controles para disminuir la probabilidad de ocurrencia del riesgo. Establecer controles para disminuir el impacto del riesgo.
Transferir	Cuando el beneficio de implementar un control sea mayor al costo del riesgo, debido a su especialización, infraestructura entre otros.	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. También, se puede realizar una transferencia parcial del riesgo, el cual consiste en compartir los riesgos, dando la responsabilidad a un tercero.
Retener	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 de AMSAC.	Conservar el riesgo en su presente nivel realizando una adecuada administración y monitoreo.
Explotar	Cuando se presente una oportunidad para AMSAC al momento en el que el riesgo se materialice, para lo cual se debe tener en cuenta el inventario de eventos positivos (oportunidades) a fin de hacer más eficiente la solución. Se verificara previamente, que el beneficio obtenido por esta acción sea mayor al costo de sus consecuencias para AMSAC.	No definir actividades de control con la finalidad de que el riesgo se materialice, para lo cual AMSAC, deberá diseñar mecanismos para obtener beneficios cuando las oportunidades se presenten.
Eliminar	Cuando es factible eliminar la causa raíz que ocasiona el riesgo, verificando previamente, que el beneficio obtenido por esta acción sea mayor al costo de sus consecuencia para AMSAC.	Eliminar la causa raíz que ocasiona el riesgo. Además, AMSAC deberá diseñar actividades que afronten consecuencias de su eliminación.

Al considerar la respuesta a los riesgos, se evalúa el efecto sobre la probabilidad y el impacto del riesgo, así como también la relación **costo-beneficio** de la implementación de los planes de acción, dentro de los grados de apetito y/o tolerancia al riesgo deseados.

Es importante considerar el efecto de las respuestas al riesgo. En algunos casos, una estrategia de respuesta al riesgo puede no ser la mejor o la más rentable para un determinado riesgo. No obstante, si esa respuesta al riesgo ayuda a gestionar otros riesgos, el beneficio para la entidad puede justificar la selección de esa opción en particular.

b. Planes de acción de respuesta al riesgo

Las estrategias de respuesta al riesgo definidas en la fase previa, deberán estructurarse en planes de acción que se encuentren documentados, con responsable, y la fecha de inicio y fin.

Los planes de acción deberán estar siempre asociados al menos a un riesgo con exposición no aceptada de acuerdo al apetito al riesgo, así como un riesgo podrá estar sujeto a varios planes de acción, a fin de lograr su mitigación.

La Gerencia y/o dueño de proceso son los encargados de la ejecución de los planes de acción, definición de los plazos y seguimiento y control de los mismos. El establecimiento del plazo de los planes de acción debe ser no mayor a 10 días hábiles posterior a su conocimiento, para asegurar una oportuna implementación de dichos planes.

El cumplimiento de los planes de acción debe ser revisado de manera continua y deben contar con el sustento correspondiente. Las posibles reprogramaciones de la fecha de implementación de los planes de acción, antes que el Responsable Titular los reporte como vencidos al Comité Técnico de Riesgos.

c. Indicadores de desempeño de la GIR (KRI)

Los indicadores de desempeño de la GIR (Key Risk Indicators – KRI) son métricas para el monitoreo de las respuestas a los riesgos, y cumplen las siguientes condiciones:

i. Identificación de riesgos que requieren de un KRI
- Aplicado a riesgos de severidad alta y procesos críticos.
- El Dueño del Proceso identifica y monitores el riesgo.
- El Dueño del Proceso completa la información del KRI en la matriz de riesgos.
- Los KRI deben ser evaluados mensualmente con el valor objetivo.
- Los KRI de los procesos críticos deben ser actualizados anualmente.

ii. Restricciones de un KRI
- Debe ser dinámico, o actualizable
- No redundante con otro indicador
- Medible, cuantificable y verificable
- De fácil implementación
- Auditable
- Revisados sobre una base de tiempo

iii. Monitoreo de las medidas de desempeño (KRI)
- Trimestralmente se realiza la evaluación de los KRI
- De existir alguna desviación del indicador, se analizará los motivos con el personal involucrado.
- Anualmente se identifica oportunidades de mejora en el diseño de los indicadores, con los dueños de proceso.

6.7. Monitoreo de la gestión de riesgos

El monitoreo consiste en realizar seguimiento a la gestión de riesgos y a las actividades de mejora consignadas en el plan de acción. El monitoreo estará a cargo de:

- Los “Dueños de Proceso”, como parte de su rol de responsable del logro de los objetivos y gestión de los riesgos del proceso.
- Los administradores de contrato, en su rol de responsables de la ejecución satisfactoria de los proyectos a cargo de AMSAC.
- El Comité Técnico de Gestión de Riesgos, como parte del seguimiento al Plan de Gestión Integral de Riesgos.

Los planes de acción definidos deben consolidarse y monitorear a través de un cronograma de implementación.

La actualización del apetito de riesgo, así como el seguimiento y evaluación del proceso de autoevaluación de riesgos, controles, planes de acción e indicadores de riesgos deben reportarse trimestralmente al Gerente General y al Comité Técnico de Riesgos; semestralmente al Directorio y a FONAFE. Los plazos de remisión de la información a FONAFE están definidos en la Directiva de Gestión.

6.8. Mejora continua

La mejora continua de procesos deberá considerar la evaluación de los aspectos relacionados al riesgo y la evaluación de la efectividad de los controles existentes e implementados.

Con base en los resultados del monitoreo y las revisiones, el Comité Técnico de Riesgos deberá tomar decisiones sobre la forma en que se podrían mejorar las políticas, procedimientos y el Plan de la GIR.

Los principales factores a tomar en consideración para realizar modificaciones en la Política son:

- Los resultados obtenidos en las autoevaluaciones y evaluaciones del desempeño de la GIR.
- Modificaciones en la normativa o mecanismos de reporte requeridos.
- Cambios en la estructura organizacional de la GIR.

El apetito de riesgo se revisa y actualiza por lo menos una vez al año en función de parámetros estratégicos, financieros y operativos.

VII. RIESGOS EN EL AMBIENTE DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

La gestión de los riesgos de los procesos relacionados a las Tecnologías de la Información y Comunicaciones se desarrolla siguiendo la presente Metodología.

La gestión de los riesgos de Seguridad de la Información se desarrolla conforme a la normativa vigente de AMSAC y de FONAFE, orientado por la NTP-ISO/IEC 27001:2014; siguiendo las siguientes etapas:

- Identificación de los Activos de información
- Análisis de los controles actuales
- Evaluación de los Riesgos de Seguridad de la Información
- Tratamiento de los Riesgos de Seguridad de la Información

El Oficial de Seguridad de la Información se asegura de la implementación progresiva de la gestión de riesgos y presenta periódicamente la evaluación de los avances en Seguridad de la Información.

VIII. RIESGO DE FRAUDE

Los riesgos de fraude se identifican y evalúan aplicando la metodología descrita en el presente documento.

AMSAC realiza una revisión anual de las áreas susceptibles a posibles actos de fraude, para garantizar que estén operando adecuadamente.

Los riesgos de fraude identificados deben ser comunicados oportunamente a la Gerencia, para dar respuesta adecuada.

La segregación de funciones en los cargos o equipos de trabajo debe contribuir a reducir los riesgos de error o fraude en los procesos, actividades o tareas.

AMSAC cuenta con canales de denuncia para usuarios externos e internos, de modo que sea posible detectar oportunamente los conflictos de interés y/o eventos de fraude que afecten a la empresa y el cumplimiento de sus objetivos.

8.1. Cómo gestionar los conflictos de interés

8.1.1. Autonomía

Con el fin de evitar los conflictos de interés en AMSAC, se establece la autonomía de los responsables de la Gestión Integral de Riesgos en la ejecución de las principales actividades de esta función, de acuerdo con lo establecido en la siguiente tabla:

Actividades	Responsabilidades		
	Propone y/o ejecuta	Visto Bueno	Aprobar
1. Definición del nivel de apetito, tolerancia y capacidad de riesgo.	Responsable Titular de la GIR	Comité Técnico de Riesgos	Directorio
2. Autoevaluación de riesgos y controles	Responsable del proceso	Responsable Titular de la GIR	Comité Técnico de Riesgos
3. Definición del indicador clave de riesgo	Responsable del proceso	Responsable Titular de la GIR	Comité Técnico de Riesgos
4. Definición de planes de acción	Responsable del proceso	Responsable Titular de la GIR	Comité Técnico de Riesgos
5. Definición del Plan de la GIR	Responsable Titular de la GIR	Comité Técnico de Riesgos	Directorio
6.Desempeño de la GIR	Responsable Titular de la GIR	Comité Técnico de Riesgos	Directorio

Estos criterios de autonomía, y segregación de funciones se aplican también en los procesos y actividades donde existe riesgo de fraude por conflicto de interés, los cuales se encuentran establecidos en los procedimientos respectivos.

8.1.2. Criterios para la solución de conflictos de interés

De acuerdo al Código del Buen Gobierno Corporativo de AMSAC, para la solución de conflictos de interés se debe priorizar un menor costo, mayor efectividad, eficacia e intereses sociales. En este contexto, se le debe brindar preferencia a mecanismos como los de conciliación y arbitraje. De igual manera, AMSAC difunde los temas considerados en el Código de Ética de manera continua a todo el personal, entre los cuales se encuentran los lineamientos a seguir en caso de conflictos de interés. Asimismo, se establece la necesidad de informar sobre cualquier conducta ilegal o no ética por parte del personal directo de la empresa.

8.1.3. Criterios para evitar los conflictos de interés

AMSAC implementa las siguientes medidas para evitar la generación de conflictos de interés:

- Mantener actualizados los documentos normativos internos, tales como; políticas, lineamientos, procedimientos, entre otros, para facilitar la toma de decisiones.
- Restricciones de contar con colaboradores que tengan relación de parentesco hasta el segundo grado de consanguinidad, segundo grado de afinidad y unión civil.

IX. GUIA PARA LA ADMINISTRACION DE RIESGOS EN LA MATRIZ DE RIESGOS:

Esta Guía tiene como objetivo facilitar a los colaboradores de AMSAC los conceptos básicos del contenido de la Matriz de Riesgos, así como la forma de llenado de la misma, para una mejor identificación, registro, control y seguimiento de cada uno de los Riesgos.

La Matriz de Riesgos es una herramienta de gestión que permite determinar objetivamente cuáles son los riesgos relevantes tanto a nivel Entidad, de los procesos críticos, de los proyectos, así como de Fraude.

De esta manera, la matriz de riesgos permite establecer de un modo uniforme y consistente el perfil de riesgo y permite profundizar en el propósito de establecimiento de planes de supervisión, a fin de que se ajusten a las características específicas de AMSAC.

Para un mejor desarrollo y control de la metodología, esta fase está sub dividida en cinco elementos claramente definidos, que se desarrollan a continuación:

a. Datos Generales del Riesgo:

En caso de matrices de riesgos a nivel entidad, las dos columnas descritas a continuación no serán necesarias. Éstas matrices iniciarán con la información descrita en el literal b del presente numeral, la información descrita a continuación sólo aplica a matrices de riesgos a nivel de procesos críticos:

- Código y Nivel:

Es el código del nivel de matriz, el cual puede ser: E (Entidad), P (Proceso), Y (Proyecto), F (Fraude).

- Nombre del proceso analizado:

Aplica solo para el matriz nivel de procesos.

- Código del Riesgo

Se identifica con la inicial del nivel de matriz y un número correlativo.

- Procesos impactados

Aplica solo para el matriz nivel de procesos.

b. Evaluación del Riesgo:

- Probabilidad:
  Una vez evaluada la probabilidad de ocurrencia del riesgo, se procede a seleccionar el valor de probabilidad correspondiente: 1, 2, 3, 4 (1= nivel “bajo”, 2= nivel “medio”, 3= nivel “alto”, y 4= nivel “extremo”).

- Impacto:
  Una vez evaluada el impacto del riesgo, se procede a seleccionar el valor de impacto correspondiente: 1, 2, 3, 4 (1= nivel “bajo”, 2= nivel “medio” y 3= nivel “alto, y 4= nivel “extremo”).

El listado de los valores, tanto para probabilidad como para impacto, se puede identificar abriendo las listas desplegables del campo “Probabilidad” o “Impacto”.

El nivel del riesgo, o severidad, se determina al multiplicar los valores de probabilidad e impacto. La herramienta está programada para que de forma automática el referido nivel del riesgo sea identificado, producto de los valores ingresados en los criterios de probabilidad e impacto.

c. Control

Contiene los siguientes campos:

- Descripción del control, y hace referencia al documento aprobado que lo especifica.
- Responsable del control
- Frecuencia del control
- Evidencia del control

d. Evaluación del riesgo residual

Se evalúa la probabilidad e impacto del riesgo, de forma posterior a la aplicación de los controles y se calcula la severidad.

e. Plan de acción:

- Descripción del plan de acción
- Responsable de realizar el plan de acción
- Fecha de Inicio de plan de acción
- Fecha de Fin del plan de acción