Especialista en Calidad y Mejora de Procesos
Firmado digitalmente por: DEYMER FRANK BARTUREN HUAMAN DNI:40658546 RUC:20103030791 Motivo: Doy V° B° Fecha: 24/11/2026 08:08:16-0500

Jefe de la Oficina de Planeamiento y Mejora Continua
Firmado digitalmente por: TITO ASCUE Miguel Armando FAU 20103030791 soft Motivo: Doy V° B° Fecha: 24/11/2026 08:33:00-0500

Gerente General(e)
Firmado digitalmente por: AGUILAR ONOFRE DANTE RUC:20103030791 Motivo: Soy el autor del documento Fecha: 24/11/2026 15:38:46-0500

Manual de Metodología para la Gestión de Riesgos

Versión	Fecha	Control de cambios
7	20/11/2026	• Se incorporó el concepto de Análisis de Impacto al Negocio (BIA) en los términos y definiciones y su aplicación en la identificación de riesgos de continuidad operativa. • Se incorporaron los roles y responsabilidades del Comité Técnico de Riesgos y de los dueños de procesos, precisando sus funciones y responsabilidades en la gestión de riesgos institucionales. • Se incorporó expresamente el Modelo de las Tres Líneas como marco de referencia para la gestión y supervisión de riesgos. • Se estableció que toda reprogramación de planes de acción para el tratamiento de riesgos deberá estar debidamente sustentada. • Se incorporaron cuadros con criterios para determinar la eficacia de los controles y rangos de calificación de sus niveles de eficacia. • Se actualizó el gráfico de clasificación de activos de información. • Se actualizó la matriz de ejemplos de tipos de eventos de pérdida.

Áreas Responsables	Nombres y Cargos
Elaborado: **Oficina de Planeamiento y Mejora Continua**	Amaru Aragón Mendieta Especialista en Control de Gestión
Revisado: **Oficina de Planeamiento y Mejora Continua**	Miguel Tito Ascue Jefe de la Oficina de Planeamiento y Mejora Continua
Homologado: **Oficina de Planeamiento y Mejora Continua**	Deymer Barturen Huamán Especialista en Calidad y Mejora de Procesos
Aprobado: **Gerencia General**	Dante Aguilar Onofre Gerente General (e)

Este documento es propiedad de Activos Mineros S.A.C. Queda prohibida su reproducción sin su autorización escrita.
Es una copia auténtica imprimible de un documento electrónico emitido por Activos Mineros S.A.C. Es responsabilidad del usuario asegurarse de que corresponde a la versión vigente publicada en la red interna y/o página web institucional.

Especialista en Control de Gestión
Firmado digitalmente por: ARAGON MENDIETA Amaru Lenin FAU 20103030791 hard Motivo: Doy V° B° Fecha: 23/11/2026 18:16:46-0500

ÍNDICE

I. OBJETIVO 4
II. ALCANCE 4
III. DOCUMENTOS DE REFERENCIA 4
IV. TÉRMINOS Y DEFINICIONES 4
V. VIGENCIA 5
VI. RESPONSABILIDADES 5
VII. RECURSOS NECESARIOS 7
VIII. METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS 7
8.1. Generalidades 7
8.2. Planificación de la gestión de riesgos 8
8.3. Identificación de eventos 9
8.4. Determinación del apetito, tolerancia y capacidad de riesgo 9
8.5. Identificación de Riesgos 10
8.6. Evaluación de los riesgos 11
8.7. Actividades de Control 15
8.8. Estimación y análisis del riesgo residual 16
8.9. Respuesta a los riesgos 17
8.10. Indicador clave de riesgo 18
8.11. Monitoreo de la gestión de riesgos 19
8.12. Mejora continua 20
IX. RIESGO DE CORRUPCIÓN (SOBORNO) Y FRAUDE 21
9.1. Criterios de identificación de riesgos de corrupción (soborno) y fraude 21
9.2. Evaluación del riesgo de corrupción (soborno) y fraude 22
9.3. Identificación de controles 23
9.4. Tratamiento al riesgo 23
9.5. Seguimiento y monitoreo continuo 23
X. GESTIÓN DE LOS CONFLICTOS DE INTERÉS 23
10.1. Autonomía 23
10.2. Criterios para la solución de conflictos de interés 23
XI. GESTIÓN DE RIESGOS DE CONTINUIDAD OPERATIVA 24
11.1. Identificación de riesgos de continuidad operativa 24
XII. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 25
12.1. Inventario de activos de información 25
12.2. Análisis de la exposición de los activos de información 28
12.3. Criterios de identificación del riesgo de seguridad de la información 29
12.4. Identificación de controles 31
12.5. Selección de controles que mitiguen los riesgos 32

XIII. GESTIÓN DE OPORTUNIDADES 33
13.1. Identificación de oportunidades. 33
13.2. Evaluación de oportunidades 33
13.3. Criterios de Evaluación de Oportunidades 33
13.4. Plan de tratamiento de oportunidades 35
13.5. Seguimiento y monitoreo continuo 35
XIV. EVENTOS DE PÉRDIDA 36
14.1. Identificación de eventos de pérdida 36
14.2. Registro de eventos de pérdida 36
14.3. Tipos de eventos de pérdida 36
14.4. Evaluación de eventos de pérdida 39
14.5. Recuperación del evento de pérdida 39
XV. CAMBIOS SIGNIFICATIVOS 39
15.1. Identificación de cambios significativos 39
15.2. Evaluación de cambios significativos 40
XVI. DESEMPEÑO DE LA GESTIÓN INTEGRAL DE RIESGOS (GIR) 40

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 AMSAC, y establece los criterios para la identificación, evaluación, tratamiento, monitoreo y reporte de los riesgos y oportunidades de la empresa. En ese sentido, la gestión de riesgos comprende los niveles de entidad, procesos y proyectos; así como en la gestión de los riesgos de continuidad operativa, corrupción (soborno), fraude y seguridad de la información. Los riesgos asociados a normas específicas, tales como Seguridad y Salud en el Trabajo Y Gestión Ambiental, podrán gestionarse mediante metodologías propias, en concordancia con el marco institucional de gestión integral de riesgos.

III. DOCUMENTOS DE REFERENCIA

- Resolución de Contraloría General N° 320-2006-CG que aprueba las Normas de Control Interno.
- Resolución de Contraloría General N° 409-2019-CG que aprueba la Directiva N° 011-2019-CG/INTEG “Implementación del Sistema de Control Interno en el Banco Central de Reserva del Perú, Petroperú S.A., Superintendencia de Banca y Seguros y AFP, Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado y entidades que se encuentren bajo supervisión de ambas”.
- Resolución Ministerial N° 320-2021-PCM, que aprueba los “Lineamientos para la Gestión de Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno”.
- Directiva Corporativa de Gestión Empresarial de FONAFE aprobada mediante Acuerdo de Directorio N° 003-2026/007-FONAFE y sus modificatorias.
- Código de Buen Gobierno Corporativo para las Empresas bajo el ámbito de FONAFE, aprobado por Acuerdo de Directorio N° 002-2025/007-FONAFE.
- Lineamiento Corporativo: “Lineamiento de Gestión Integral de Riesgos”.
- Manual Corporativo: “Guía para la Gestión Integral de Riesgos”.
- Manual Corporativo: “Metodología para la Gestión de Riesgos de Seguridad de la Información”.
- Política de Gestión Integral de Riesgos de AMSAC.

IV. TÉRMINOS Y DEFINICIONES

- Apetito: Nivel de riesgo que AMSAC 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.
- Análisis de Impacto al Negocio (BIA): Es un proceso sistemático mediante el cual se identifican los procesos y servicios críticos de la organización y se evalúan los impactos operativos, financieros, legales, regulatorios y reputacionales que podrían generarse ante su interrupción, determinando las prioridades y tiempos requeridos para su recuperación.
- Cambios significativos: Son cambios importantes que se producen cuando se eliminan o modifican procesos existentes, se crean nuevos procesos, o se implementan nuevas operaciones, productos, servicios, sistemas informáticos, inversiones, proyectos o reorganizaciones societarias y en general cualquier cambio que pueda afectar significativamente el logro de los objetivos de AMSAC o afectarla financieramente.
- Continuidad operativa: Disciplina que prepara a las organizaciones para responder de manera eficaz y eficiente ante la ocurrencia de eventos de crisis o desastres que tengan la potencialidad de interrumpir la operatividad normal de las mismas.

- Control: Medida o actividad implementada con la finalidad de reducir la probabilidad de ocurrencia y/o el impacto de un riesgo. Su ejecución debe realizarse de manera consistente, contar con un responsable definido y generar evidencia verificable.
- Evento: Un suceso o serie de sucesos que pueden ser internos o externos, originados por una misma causa, que ocurren durante el mismo periodo de tiempo.
- Evento de pérdida: Un evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional, que debe estar registrado contablemente.
- Indicadores clave de riesgo (KRI): Métricas usadas para obtener señales tempranas sobre el incremento de la exposición de las diversas áreas a los riesgos.
- Nivel de entidad: Nivel donde las actividades son ejecutadas por el Gerente General y Gerentes de línea.
- Nivel de procesos: Nivel donde las actividades son ejecutadas por los dueños de procesos y su personal clave.
- Oportunidad: Evento positivo relevante que debe ser aprovechado, previa evaluación, pues se tiene cierta certeza de que pueden contribuir al cumplimiento de los objetivos.
- Riesgo: Incertidumbre o condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos.
- Riesgo inherente: Aquel riesgo en su forma natural sin el efecto mitigante de los controles.
- Riesgo residual: Nivel resultante del riesgo después de aplicar los controles.
- Seguridad razonable: Es el nivel de certeza respecto al logro de los objetivos considerando que se produzcan hechos significativos o eventos de pérdida que no sean prevenidos o detectados oportunamente dada la incertidumbre inherente al futuro.
- Ciberseguridad: Es una práctica que garantiza la protección de los activos digitales que interactúan con el ciberespacio mediante la prevención, detección, respuesta y recuperación ante incidentes de seguridad que afecten su disponibilidad, confidencialidad o integridad.
- Activos digitales: Son recursos que existen de forma digitalizada en el ciberespacio y que alguien puede poseer.
- Confidencialidad de la Información: Indica que sólo acceden quienes están autorizados.
- Disponibilidad de la Información: Establece que debe existir garantía de acceso cuando sea requerido.
- Integridad de la Información: Establece que la información y su procesamiento son exactos y completos.

V. VIGENCIA

Este documento entrará en vigor a partir del primer día hábil después de la fecha de aprobación, derogándose su precedente Versión 06 de fecha 6.nov.2025.

VI. RESPONSABILIDADES

Los responsables de la gestión de riesgos son:

- Riesgos a nivel de entidad: Comité Técnico de Riesgos y Gerencia General.
- 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.
- Riesgos de corrupción (soborno) y fraude: Comité Técnico de Riesgos, Oficial de Cumplimiento y Gerencia General.
- Riesgos de continuidad operativa: Gerencia de Administración y Finanzas (Gestión) y Gerencia de Operaciones (Proyectos).

Las autonomías de los responsables de la GIR en la ejecución de las principales actividades de la GIR son:

Actividades	Responsabilidades		
	Propone y/o ejecuta	Visto bueno	Aprobar
1. Definición del nivel de apetito, tolerancia y capacidad de riesgo.	Responsable designado de la GIR	Gerencia General	Directorio
2. Autoevaluación de riesgos y controles	Dueño de Proceso	Responsable designado de la GIR	Gerente de área
3. Definición del indicador clave de riesgo	Dueño de Proceso	Responsable designado de la GIR	Gerente de área
4. Definición de planes de acción	Dueño de Proceso	Responsable designado de la GIR	Gerente de área
5. Definición del Plan de la GIR	Responsable designado de la GIR	Comité Técnico de Riesgos	Gerencia General
6. Desempeño de la GIR	Responsable designado de la GIR	Comité Técnico de Riesgos	Gerencia General

Los roles y responsabilidades en materia de la GIR son los siguientes:

6.1. Comité Técnico de Riesgos

- Gestionar la asignación del personal y recursos necesarios para la implementación de la GIR.
- Asegurar que se incluyan las capacitaciones de la GIR en el plan anual de capacitaciones de la empresa.
- Promover e implementar la cultura de la GIR.
- Recomendar acciones de mejora para la eficiencia y eficacia de la GIR.
- Supervisar la gestión de los riesgos clave de la empresa según lo definido en el apetito y tolerancia al riesgo.
- Alertar sobre nuevos riesgos y gestionar la evaluación de oportunidades.

6.2. Órganos Gerenciales

- Ser diligentes en la adopción de las medidas necesarias ante la desviación de los objetivos y metas programadas, detección de irregularidades, o de actuaciones contrarias a los principios de legalidad, economía, eficiencia y/o eficacia.
- Aprobar las matrices de riesgos y controles, los cronogramas de implementación de estrategias de respuesta al riesgo, las matrices de evaluación de controles, los KRI, y demás mecanismos de seguimiento, que le correspondan.
- Asegurarse de la contribución de los controles de riesgos al logro de los resultados de la gestión.
- Aprobar y realizar el seguimiento de las oportunidades aplicables a su área.
- Supervisar el fortalecimiento de la cultura de la GIR de su área, evaluando el desempeño de su personal a cargo frente a las actividades de capacitación y sensibilización.

6.3. Responsable designado de la GIR

- Brindar soporte en las actividades de evaluación de riesgos.
- Apoyar en la identificación de estrategias de respuesta al riesgo y definición de planes de acción.
- Coordinar la implementación del plan de acción y monitorear su cumplimiento.
- Apoyar en la evaluación e informe de los cambios significativos en el entorno empresarial.
- Brindar soporte en las actividades sobre oportunidades identificadas.
- En caso de ausencia del Responsable designado de la GIR titular, el responsable alterno de la GIR asume las funciones mencionadas. Asimismo, el Responsable designado de la GIR puede

solicitar apoyo al responsable alterno si lo considerase necesario para el desarrollo de la implementación de la GIR.

6.4. Dueño de proceso

- Implementar la cultura de GIR en los procesos bajo su responsabilidad.
- Desarrollar las actividades contenidas en el plan de la GIR donde corresponda.
- Reportar oportunamente la información de la GIR al Responsable designado de la GIR.
- Comunicar los cambios en sus procesos y los riesgos asociados al Responsable designado de la GIR.
- Administrar los riesgos de sus procesos sobre la base de los resultados de la evaluación de riesgos.
- Definir la severidad de los riesgos en coordinación con el Responsable designado de la GIR.
- Monitorear el cumplimiento de los planes de acción de la matriz de riesgos y controles, así como otros que pudieran requerirse, y reportar los resultados al Responsable designado de la GIR.
- Velar por la eficacia de los controles asociados a los riesgos de sus procesos.
- Reportar trimestralmente eventos de pérdida significativos.

VII. RECURSOS NECESARIOS

Anualmente, el Responsable designado de la GIR, con el visto bueno de la Gerencia General, comunica al Directorio los recursos requeridos para la implementación de planes de acción ligados a las estrategias de la GIR, así como otros elementos necesarios para su desarrollo, con el propósito de otorgarles relevancia especial.

VIII. METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS

8.1. Generalidades

La presente metodología complementa el Lineamiento de Gestión Integral de Riesgos para las empresas bajo el ámbito de FONAFE, y las disposiciones posteriores que se emitan sobre la materia. En caso de aparente conflicto o contradicción, primará siempre lo dispuesto por FONAFE.

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 Responsable designado de la GIR propone el Plan de la GIR, el cual contará con el visto bueno del Comité Técnico de Riesgos, para su aprobación por la Gerencia General.

8.1.1. Modelo de las Tres Líneas

Con la finalidad de fortalecer la gobernanza, la gestión integral de riesgos y el control interno, AMSAC adopta el Modelo de las Tres Líneas como marco de referencia para la gestión y supervisión de los riesgos institucionales.

Este modelo establece una distribución clara de roles y responsabilidades para la gestión, supervisión y aseguramiento de los riesgos, promoviendo la coordinación entre las áreas responsables de la ejecución de las actividades, las funciones de apoyo y monitoreo, y las

instancias de aseguramiento independiente. Su aplicación contribuye al fortalecimiento de la toma de decisiones, el cumplimiento de los objetivos institucionales y la mejora continua del desempeño organizacional.

- **Primera Línea:** Está conformada por los dueños de proceso, administradores de contrato, jefaturas y personal responsable de la ejecución de las actividades operativas.
  Son responsables de identificar, evaluar, tratar, controlar y monitorear los riesgos asociados a los procesos, proyectos y actividades bajo su responsabilidad.
- **La segunda línea**: Está conformada por el Responsable designado de la GIR titular, el Responsable alterno de la GIR, la Oficina de Planeamiento y Mejora Continua y las funciones de Cumplimiento, Integridad y Prevención.
  Tiene la responsabilidad de brindar metodologías, lineamientos, asesoramiento y monitoreo para asegurar una adecuada gestión de riesgos, así como realizar el seguimiento al cumplimiento de las políticas y disposiciones aplicables.
- **La tercera línea**: Está conformada por las instancias independientes que realizan evaluaciones o revisiones sobre la forma en que AMSAC gestiona sus riesgos, controles y mecanismos de gobierno, así como la identificación de oportunidades de mejora para fortalecer la gestión institucional.
  Estas funciones pueden ser ejercidas por órganos o entidades de control, auditoría o evaluación independientes, de acuerdo con su ámbito de competencia y la normativa aplicable.

Las tres líneas actúan de manera coordinada y complementaria, en el marco de sus respectivas funciones y responsabilidades, preservando la independencia de la tercera línea, contribuyendo al fortalecimiento de la gobernanza corporativa, la transparencia, el cumplimiento normativo y la gestión integral de riesgos,

8.2. 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. Para implementar la GIR, se deben cumplir los siguientes requisitos previos.

- **Definición de objetivos a nivel de 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 y jefaturas, 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.

- **Elaboración del Plan de la GIR**
  El Responsable designado de la GIR elabora el Plan de la GIR, con la finalidad de brindar seguridad razonable sobre la gestión de riesgos y promover el cumplimiento de sus objetivos que deben, a su vez, estar alineados al Plan Estratégico y Plan Operativo. El Plan debe contener, como mínimo, los siguientes elementos: actividades, responsables, plazos y recursos, entre otros.

Se debe evaluar si los recursos para desarrollar las actividades son con personal de AMSAC o si es conveniente contar con personal externo; de escoger la primera opción, es importante verificar si el personal seleccionado cuenta con el conocimiento y las competencias necesarias para llevar a cabo estas actividades o si requiere capacitación o entrenamiento.

8.3. Identificación de eventos

Los eventos 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, climatológicos, políticos, sociales y tecnológicos. Los factores internos reflejan las selecciones que realiza AMSAC e incluyen la infraestructura, personal, procesos y tecnología.

La identificación de dichos eventos que corresponden a peligros y riesgos es crucial para mitigar impactos negativos, aprovechar oportunidades estratégicas y asegurar la resiliencia a largo plazo de AMSAC.

8.4. Determinación del apetito, tolerancia y capacidad de riesgo

La propuesta de apetito, tolerancia y capacidad de riesgo es elaborada por el Responsable designado de la GIR y debe contar con el visto bueno de la Gerencia General para su aprobación por parte del Directorio; en función de los objetivos del Plan Estratégico Institucional, lo cual representa el marco para la GIR.

- **Apetito al 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 al riesgo se fija tomando en cuenta el **nivel límite de riesgo** que se acepta para no afectar el cumplimiento de los objetivos.
  Una vez definido el apetito al riesgo, se lleva a cabo la identificación de los riesgos a nivel de 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 al 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 8.8. 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

AMSAC establece la disposición de cero eventos de corrupción (soborno) y fraude, lo que se implementa a través de la adopción de medidas preventivas y detectivas para evitar o conocer de manera temprana la ocurrencia de dichos eventos.

La actualización del apetito, tolerancia y capacidad al riesgo se realiza con una periodicidad no mayor a 2 años.

8.5. 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.

Un riesgo es la amenaza que enfrenta la empresa cuando un evento o acción puede afectar negativamente su capacidad para alcanzar los objetivos estratégicos y 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.

Posteriormente se identifican los riesgos que afectan a nivel de 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 actividades de identificación de riesgos se pueden realizar a través de talleres u otras técnicas, al menos una vez al año, como parte de la revisión de las matrices de riesgos.

Las Gerencias y los dueños de proceso deben identificar y reportar potenciales riesgos, para lo cual cuentan con el apoyo del Responsable designado de la GIR.

Cabe señalar que la Matriz de Riesgos de Proyectos se desarrolla conforme se establece en el O1.6.PL1. Plan de Gestión de Riesgos de Proyectos de Remediación de Pasivos Ambientales Mineros, cuyo objetivo es establecer un marco que permita identificar, evaluar y atender los riesgos que puedan afectar el cumplimiento de los objetivos de los proyectos, definiendo estrategias de respuesta, responsabilidades y mecanismos de monitoreo a lo largo de su ciclo de vida.

8.5.1. Técnicas para la identificación de riesgos

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, mediante juicio de expertos.
- Por propuesta de las Gerencias (riesgos a nivel de entidad) revisados por el Comité Técnico de Riesgos.
- Por propuesta del dueño de proceso o del Responsable designado de la 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.

8.5.2. Forma de redacción y tipos de riesgos

- Redacción del Riesgo:
  El riesgo se describe con sus dos componentes: a) Consecuencia: Es el impacto de un riesgo al momento de materializarse; b) Causa: Es el motivo por el cual se presenta el riesgo.

- Tipos de Riesgo:

  a. Por el objetivo que afecta el riesgo:

- Riesgos estratégicos
  Son aquellos que, de presentarse, pueden afectar el logro de la misión o de los objetivos estratégicos de la empresa.

- Riesgos a nivel proceso
  Son los riesgos que afectan el logro de los objetivos operacionales de la empresa, amenazando el uso eficaz y eficiente de los recursos. Incluyen los riesgos originados por fallas en los procesos, proyectos o en la estructura organizacional.

- 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), como en la seguridad de la información (accesos lógicos, cambios a programas, etc.) de los sistemas.

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

- Riesgos de cumplimiento
  Riesgos que impactan en la capacidad de AMSAC para cumplir las 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 corrupción (soborno) y fraude
  Riesgos que impactan de manera negativa en la reputación de la empresa o que generan pérdidas económicas, siempre que sean causados por la conducta de un colaborador que incumple las obligaciones legales, con la intención de lograr un beneficio propio o de un tercero, relegando los intereses de AMSAC.

- Riesgos de continuidad operativa
  Riesgos que afectan la continuidad operativa de las actividades o funciones que se requiere recuperar y continuar operando ante eventos disruptivos.

8.6. 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 de entidad, como a nivel de los procesos y proyectos, de acuerdo con los criterios de evaluación de riesgos.

El Responsable designado de la GIR verificará que las evaluaciones de riesgos se actualicen al menos una vez al año a nivel de entidad, de corrupción (soborno) y fraude, de los procesos y controles de AMSAC; mientras que, en el caso de los proyectos, estas se realizarán al menos semestralmente. Esta actualización puede efectuarse junto con la revisión y/o actualización de los procesos, con la participación de los dueños de proceso.

Se evaluarán los riesgos considerando 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.

8.6.1. Definición de los criterios de evaluación de riesgos

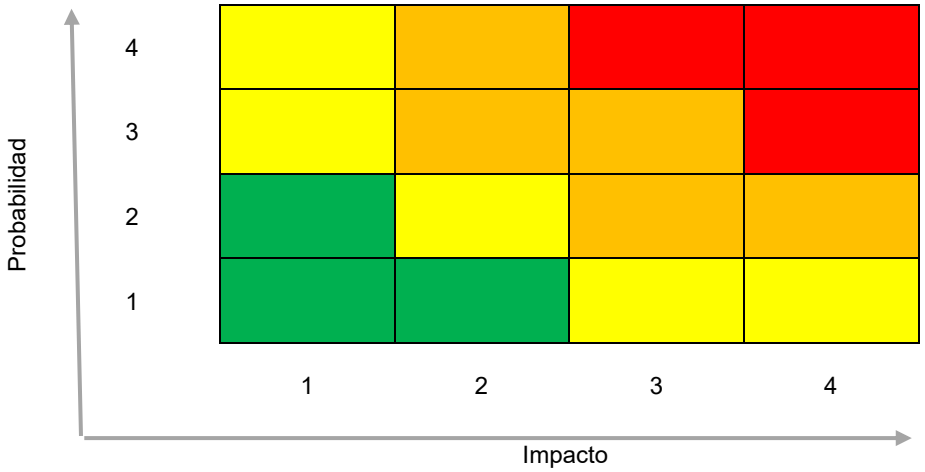
- **Probabilidad de ocurrencia**
  Es el nivel de posibilidad de que ocurra el evento de riesgo en el periodo de un año. Puede ser estimada en función de cuántas veces históricamente ha ocurrido el evento de riesgo en AMSAC o en la posibilidad de que ocurra en el futuro o por otros criterios cualitativos.

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

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 los niveles de severidad del 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.

8.6.2. Definición de los criterios 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 en términos 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 en términos 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 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**	**MEDIO**	**ALTO**	**EXTREMO**
Potencial pérdida financiera	Impacto adverso menor o igual a 1 UIT	Impacto adverso mayor a 1 UIT pero menor o igual a 8 UIT	Impacto adverso mayor a 8 UIT pero menor o igual a 15 UIT	Impacto adverso mayor a 15 UIT
Cualitativos				
Criterios	**BAJO**	**MEDIO**	**ALTO**	**EXTREMO**
Reputación/ Pérdida de confianza	No se presentan daños en la reputación.	Daño en la reputación conalcance local, que podría originar desconfianza en ciertas entidades relacionadas.	Daño en la reputación conalcance local, pero con potencial de escalamientosi 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 nitributaria.	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 dan lugar al pago de multas o indemnizaciones elevadas.
Disponibilidad de información / Confiabilidad del sistema	No disponibilidad oportuna de información, pero que no afecta la continuidad del negocio.	No disponibilidad oportunade la información crítica, aquella que: (i) es requerida por el regulador,o (ii) es estratégica para la empresa; lo cual conlleva 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 conlleva 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 conlleva a la interrupción de procesos clave o continuidad del negocio. Uso de un sistema no confiable.
Continuidad Operativa	No se interrumpenlos procesos y/o sin lesiones al personal	Se interrumpe en un tiempo considerable los procesos y/o hay lesiones leves en el personal	Se interrumpe en un tiempo considerable los procesos y/o hay lesiones graves al personal	Se interrumpe permanentemente los procesos y/o hay muerte de una persona

IMPACTO DE EVENTOS DE CORRUPCIÓN (SOBORNO) Y FRAUDE

Para la evaluación del impacto general de los posibles eventos de corrupción (soborno) o fraude, se consideran 4 impacto específicos: impacto económico, impacto legal, impacto reputacional e impacto en la continuidad, tal como se describe a continuación:

		Impacto económico	Impacto legal	Impacto reputacional	Impacto en la continuidad
	Ponderación	25%	25%	25%	25%
Apetito	1. Bajo	- Sin impacto económico	- Sin impacto legal	- Sin impacto reputacional	- Sin impacto en la continuidad.
Tolerancia	2. Medio	Impacto adverso menor o igual a 8UIT	- Actividad afectada sujeta o no a supervisión por parte de otra entidad. - Posibilidad de multa o sanción por falta leve. - La actividad afectadacon potencial o no de generar demandas o reclamaciones. - Posibilidad de demanda que afecta a algunos empleados de nivel operacional de la empresa.	- La exposición de la imagen es interna y puede ser limitada o con potencial para trascender externamente.	- Impacto puede ser absorbido (asimilado) por las actividades normales del negocio en 1 semana aproximadamente. - Los costos adicionales del impacto son mínimos. - Personal adicional podría ser necesario.
Capacidad	3. Alto	Impacto adverso mayor a 8 UIT pero menor o igual a 15UIT	- Multa o sanción por falta grave. - Posibilidad de demanda que afecta a los directores, gerentes o algún personal especializado de la empresa.	- La exposición de la imagen es interna y externa, presenta un potencial de impacto negativo por un plazo acotado (menos de un mes).	- Impacto potencial en la continuidad del negocio, productividad, en un horizonte mayor a 1 semana. El costo de interrupción es alto.
	4. Extremo	Impacto adverso mayor a 15UIT	- Multa o sanción por falta muy grave, cierre de las instalaciones, entre otras. - Posibilidad de demanda que afecta a múltiples áreas de la empresa.	- Exposición total de la imagen, con potencial de generar un mal manejo de situaciones de crisis y tener un impacto negativo por un tiempo prolongado (más de un mes).	- Interrupción total o significativa de las operaciones de la empresa por un período superior a 1 mes. El costo de interrupción es muy alto.

PROBABILIDAD

Cuantitativos

Criterios	BAJO	MEDIO	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 mayor al 15% y menor al 25% de los casos.	Frecuente: El evento podría ocurrir más de 12 veces al año; o igual o mayor al 25% de los casos.
Frecuencia de eventos de corrupción (soborno) o fraude	El evento no ha ocurrido (en los últimos tres años)	El evento podría ocurrir 1 o 2 veces al año	El evento podría ocurrir de manera mensual (entre 3 y 12 veces al año)	El evento podría ocurrir de manera semanal o diaria (más de 12 veces al año)
Continuidad Operativa	No se presentó o podría presentarse en 15 años o más	No se presentó o podría presentarse en 10 o 14 años	No se presentó o podría presentarse en 5 o 9 años	No se presentó o podría presentarse en 1 o 4 años

Para calificar la probabilidad e impacto, es necesario seleccionar el criterio general respectivo más idóneo según las características del riesgo. En caso de que 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.

Para determinar los niveles de probabilidad y de impacto de los riesgos, se pueden utilizar, sin ser limitativas, las mismas técnicas que se usan para la identificación de los riesgos. Se busca el consenso entre los participantes sobre los niveles de probabilidad y de impacto, considerando los valores del mapa de riesgos; en el caso que no haya consenso, se definirá mediante multivotación u otro método.

8.7. Actividades de Control

El objetivo de esta etapa es identificar los controles existentes en AMSAC y diseñar e implementar los que sean necesarios para reducir la criticidad del riesgo. AMSAC deberá diseñar e implementar las acciones de control específicas que sean necesarias y evaluar al mismo tiempo que éstas sean eficaces. Si se determinara que no son eficaces, 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.

8.7.1. Consideraciones para definir el Control

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 en 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 generar evidencia (electrónica o física) que permita en el tiempo hacer un seguimiento a la ejecución del control;

8.7.2. Tipos de Control

- Según la oportunidad en que se ejecuta el control:

Clasificación	Descripción
Preventivo	Actividad que ayuda a evitar la ocurrencia de un riesgo.
Detectivo	Actividad que permite identificar errores después de la materialización del riesgo.
Correctivo	Actividad que permite enmendar algo no deseado. Cuando se identifica un error o irregularidad, este permite corregir oportunamente el efecto no deseado.

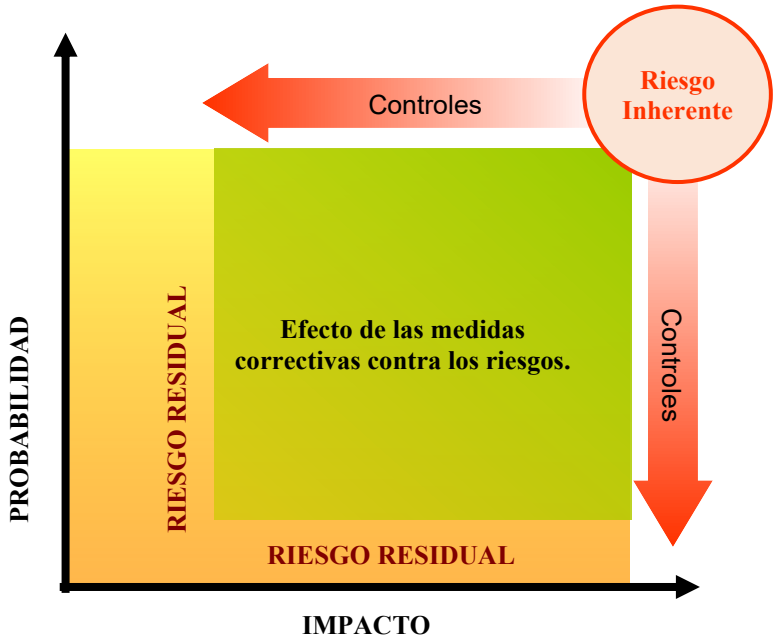
- Según la automatización en la aplicación del control:

Clasificación	Descripción
Automático	Control que es realizado internamente por un sistema.
Semiautomático	Control que depende de la habilidad de la persona para prevenir o detectarerrores cometidos utilizando información proveniente de un sistema.
Manual	Control que depende de la habilidad de la persona que lo ejecuta paraprevenir o detectar los errores que se presenten.

8.8. Estimación y análisis del riesgo residual

El riesgo residual es el nivel de riesgo que permanece después de aplicar los controles luego de haber implementado acciones de control.

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



8.8.1. 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 de que existan controles eficaces, el impacto o la 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 eficaces, el riesgo residual será igual al riesgo inherente.

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

8.8.2. 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, eficacia 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.

8.9. Respuesta a los riesgos

AMSAC define las estrategias de tratamiento, con la finalidad de mantener los riesgos dentro de los niveles definidos por el apetito al riesgo.

La selección de la estrategia de tratamiento al riesgo está a cargo de la Gerencia correspondiente, con la participación del Responsable designado de la GIR y los dueños de procesos.

8.9.1. 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	Cuándo 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.
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 factores.	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 el riesgo, dando la responsabilidad a un tercero.
Retener o Aceptar	Cuando el control (eficaz) relacionado con el 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.

Tipo de respuesta a riesgos	Cuándo seleccionarlo	Actividades
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 consecuencias 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.

8.9.2. Planes de acción de Tratamiento al riesgo

Las estrategias de respuesta al riesgo definidas en la fase previa deberán estructurarse en planes de acción que se encuentren documentados, con un responsable, una fecha de inicio y una fecha de término y evidencia que permita realizar el control de avance.

Los planes de acción deberán estar siempre asociados al menos a un riesgo con exposición no aceptada de acuerdo con el 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 cumplimiento de los planes de acción debe ser revisado de manera continua y deben contar con el sustento correspondiente. Para ello, los dueños de los procesos deben reportar al Responsable designado de la GIR y al Gerente General, el estatus de la implementación de los planes de acción programados, así como el planteamiento de las medidas correctivas en el caso de desviación de los plazos determinados.

Asimismo, toda reprogramación de un plan de acción deberá estar debidamente sustentada por el responsable de su ejecución, indicando las causas que la motivan, la justificación del nuevo plazo, sus implicancias sobre la exposición al riesgo y, de corresponder, las medidas temporales de mitigación, así como el nuevo cronograma previsto para su cumplimiento. La reprogramación deberá contar con la aprobación de la instancia que aprobó el plan de acción original y ser comunicada al Responsable designado de la GIR para su seguimiento.

8.10. Indicador clave de riesgo

Los indicadores clave de riesgo (Key Risk Indicators – KRI) deben cumplir las siguientes condiciones:

a. Identificación de riesgos que requieren de un KRI
- Aplicado a riesgos residuales de severidad alta, extrema y procesos críticos.
- El Dueño de Proceso identifica los riesgos que requieren un KRI, con el fin de monitorearlos.
- El Dueño de Proceso completa la información del KRI en la matriz de riesgos.
- Los KRI deben ser evaluados de manera semestral con el valor objetivo.
- Los KRI de los procesos críticos deben ser actualizados anualmente.

b. Restricciones de un KRI
- Debe ser dinámico o actualizable

- No redundante con otro indicador
- Medible, cuantificable y verificable
- De fácil implementación
- Auditable
- Sujeto a revisión periódica

c. Monitoreo de las medidas de desempeño (KRI)

- Semestralmente se realiza la evaluación de los KRI
- De existir alguna desviación del indicador, se analizarán los motivos con el personal involucrado.
- Anualmente, se identifican oportunidades de mejora en el diseño de los indicadores, con los dueños de proceso.
- El Responsable designado de la GIR informa semestralmente sobre los resultados de los indicadores de la GIR, así como de la implementación de las medidas correctivas a la Gerencia General.

8.11. 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 responsables 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 Riesgos, como parte del seguimiento al Plan de Gestión Integral de Riesgos.

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

8.11.1. Verificación de la eficacia de los planes de acción de tratamiento de los riesgos

La verificación de la eficacia muestra la forma como la implementación de las acciones ha beneficiado a AMSAC para lo cual se registra en la Matriz de Riesgos, la eficacia del plan de acción, la fecha de su verificación, el encargado de verificarlo, la evidencia encontrada, y de ser necesario comentarios.

8.11.2. Evaluación de los controles

Esta etapa comprende la evaluación anual de los controles establecidos para hacer frente a los riesgos, tanto a nivel de entidad como de procesos y proyectos. Su finalidad es determinar el nivel de eficacia de cada control mediante el levantamiento de información y la realización de pruebas que permitan verificar su diseño, ejecución y contribución a la reducción del riesgo.

Como resultado de la evaluación, se podrán identificar oportunidades de mejora, formular recomendaciones, incorporar nuevos controles o modificar los existentes, según corresponda.

A continuación, se presentan los criterios para determinar si un control es eficaz:

Criterio	Puntaje	Descripción
Diseño del Control	**0**	El control no existe o no guarda relación con el riesgo identificado. No se encuentra definido, documentado.

	1	El control existe y está relacionado con el riesgo; sin embargo, presenta debilidades en su diseño, tales como falta de responsable definido, periodicidad no establecida, ausencia de formalización, cobertura parcial del riesgo o limitaciones para prevenir o detectar oportunamente su materialización.
	2	El control está formalizado, cuenta con responsable, frecuencia y actividades claramente definidas, genera evidencia y responde adecuadamente al riesgo identificado.
Evidencia de la Ejecución	**0**	No existe evidencia que demuestre la ejecución del control o la evidencia disponible es insuficiente para acreditar su aplicación.
	1	Existe evidencia parcial de la ejecución del control; sin embargo, esta es incompleta, inconsistente o no permite verificar plenamente su cumplimiento.
	2	Existe evidencia suficiente, confiable, íntegra y verificable que demuestra la ejecución del control conforme a lo establecido.
Reducción del Riesgo	**0**	El control no contribuye a reducir la probabilidad o el impacto del riesgo, manteniéndose la exposición al mismo.
	1	El control contribuye parcialmente a reducir la probabilidad o el impacto del riesgo; sin embargo, persisten deficiencias que limitan su eficacia.
	2	El control reduce significativamente la probabilidad o el impacto del riesgo, mitigando de manera efectiva la exposición al riesgo evaluado.

La eficacia de cada control se determina mediante la evaluación de tres criterios: diseño del control, evidencia de su ejecución y reducción del riesgo. Cada criterio se califica de 0 a 2 puntos, de acuerdo con las características observadas durante la evaluación.

El puntaje total se calcula aplicando la siguiente fórmula:

Puntaje = (Diseño x Evidencia) + Reducción

Los rangos de calificación constituyen intervalos de puntaje que permiten clasificar el nivel de eficacia de los controles evaluados.

Puntaje Obtenido	Nivel de Eficacia	Interpretación
0-2	No eficaz[1]	El control no trata adecuadamente el riesgo o presenta deficiencias significativas en su diseño o ejecución, por lo que no cumple con el propósito previsto de prevenir, detectar o mitigar su materialización
3-4	Parcialmente eficaz	El control trata parcialmente el riesgo, debido a que existen situaciones o escenarios que no son prevenidos, detectados o mitigados oportunamente, lo que permite que el riesgo pueda materializarse.
5-6	Eficaz	El control trata adecuadamente el riesgo, conforme a su diseño, y permite prevenir, detectar o mitigar oportunamente las situaciones que podrían ocasionar su materialización.

8.12. Mejora continua

La mejora continua de procesos deberá considerar la evaluación de los aspectos relacionados con el riesgo y la evaluación de la eficacia de los controles existentes e implementados.

[1] Regla especial de calificación: Independientemente del puntaje obtenido, cuando el criterio de diseño del control o el de evidencia de su ejecución obtenga una calificación de cero (0), el control será considerado no eficaz para efectos de la estimación del riesgo residual. En consecuencia, su puntaje máximo será de dos (2) puntos.

El Responsable designado de la GIR recopila las lecciones aprendidas, a fin de proponer mejoras en la matriz de riesgos y controles, medir el desempeño y brindar seguridad razonable sobre la gestión de riesgos.

La auditoría interna realiza evaluaciones para asegurar la operación de la gestión de riesgos y su mantenimiento.

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 que deben considerarse para realizar modificaciones en la Metodología para la GIR 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.

IX. RIESGO DE CORRUPCIÓN (SOBORNO) Y FRAUDE

Los riesgos de corrupción (soborno) y fraude se identifican y evalúan por las gerencias y jefaturas (dueños de procesos), en coordinación con la Oficina de Planeamiento y Mejora Continua, aplicando la metodología descrita en el presente documento.

Los controles y planes de acción de tratamiento de los riesgos de corrupción (soborno) y fraude deben estar orientados a abordar al menos uno de los elementos del triángulo del fraude: i) oportunidad, mediante el establecimiento de controles como la debida diligencia respecto de agentes potenciales de corrupción (soborno) o fraude; ii) incentivo / presión, mediante la comunicación directa con los trabajadores por parte de los líderes para identificar y adoptar medidas frente a posibles factores desencadenantes de corrupción (soborno) o fraude; y iii) racionalización, mediante acciones de sensibilización en integridad, Código de ética, entre otros.

El Oficial de Cumplimiento, Integridad y Prevención de AMSAC realiza una revisión anual de los procesos / áreas sensibles a riesgos de corrupción (soborno) y fraude, para garantizar que se encuentren identificados y evaluados adecuadamente.

Los riesgos de corrupción (soborno) y fraude identificados deben ser comunicados oportunamente a las Gerencias, para brindar una respuesta adecuada.

La debida diligencia, el control posterior y la segregación de funciones en los cargos o equipos de trabajo deben contribuir a reducir los riesgos de error, corrupción (soborno) o fraude en los procesos, actividades o tareas.

AMSAC cuenta con canales de denuncias éticas para usuarios externos e internos, de modo que sea posible detectar oportunamente los conflictos de interés, eventos de corrupción (soborno), fraude o comportamientos antiéticos que afecten a la empresa y el cumplimiento de sus objetivos.

9.1. Criterios de identificación de riesgos de corrupción (soborno) y fraude

Los criterios para identificar los riesgos de corrupción (soborno) y fraude son los siguientes:

Riesgos de Corrupción (soborno)	
Tipo	**Definición**
Cohecho	Es la situación en la que un trabajador busca obtener dinero u otro beneficio a cambio de realizar u omitir una conducta funcional.

Colusión	Es la situación en la que un colaborador que interviene directa o indirectamente, por razón de su cargo, en cualquier etapa de las modalidades de adquisición o contratación de bienes, obras o servicios, concesiones o cualquier operación, concierta con los interesados para defraudar al Estado o entidad u organismo del Estado.
Tráfico de influencias	Es la situación en la que, invocando o teniendo influencias reales o simuladas, se recibe, se da o promete para sí o para un tercero, donativo o promesa o cualquier otra ventaja o beneficio con el ofrecimiento de interceder ante un funcionario que ha de conocer, esté conociendo o haya conocido un caso judicial o administrativo.
Negociación incompatible	Es la situación en la que un colaborador indebidamente, en forma directa o indirecta o por acto simulado se interesa, en provecho propio o de un tercero, por cualquier contrato u operación en que interviene debido a su cargo.
Abuso de autoridad	Es la situación en la que un colaborador, abusando de sus atribuciones, comete u ordena un acto arbitrario que cause perjuicio a alguien.
Cobro indebido	Es la situación en la que un colaborador, abusando de su cargo, exige o hace pagar o entregar contribuciones no debidas o en cantidad que excede a la tarifa legal.
Concusión	Es la situación en la que un colaborador, abusando de su cargo, obliga o induce a una persona a dar o prometer indebidamente, para sí o para otro, un bien o un beneficio patrimonial.
Enriquecimiento ilícito	Es la situación en la que un colaborador, abusando de su cargo, incrementa ilícitamente su patrimonio respecto de sus ingresos legítimos. Son indicios de enriquecimiento ilícito el aumento muy notorio del patrimonio o del gasto económico personal, en comparación a su declaración jurada de bienes y rentas y a sus ingresos actuales.
Malversación	Es la situación en la que un colaborador da al dinero o bienes que administra un uso definitivo diferente de aquel al que estaban destinados, afectando el servicio o la función encomendada.
Nombramiento, designación, contratación ilegal de cargo	Es la situación en la que un colaborador nombra, designa, contrata o encarga a persona en quien no concurren los requisitos legales para un cargo o acepta el cargo sin contar con los requisitos legales para dicho cargo.
Peculado	Es la situación en la que un colaborador se apropia o utiliza, en cualquier forma, para sí o para otro, caudales o efectos del Estado, cuya percepción, administración o custodia le están confiados por razón de su cargo. Este delito afecta el patrimonio del Estado.
Riesgos de Fraude	
Tipo	**Definición**
Apropiación de bienes	Ocurre cuando el colaborador recibe un bien (eficaz o no eficaz), en virtud de su cargo y lo incorpora a su propio patrimonio.
Reportes o cuentas fraudulentas	Es la manipulación deliberada de información financiera o no financiera de AMSAC, que se logra mediante la presentación intencionalmente errónea de cifras o de datos o alteración, creación u ocultamiento de información con el objeto de engañar al usuario de estos.
Contabilidad paralela	Es la situación en la que un colaborador, que con la finalidad de obtener una ventaja indebida, mantiene contabilidad paralela distinta a la exigida por la ley.

9.2. Evaluación del riesgo de corrupción (soborno) y fraude

9.2.1. Método para la definición de la probabilidad e impacto

La definición de la probabilidad y del impacto se realiza de acuerdo con lo dispuesto en el numeral 8.6. Para el impacto, se considera una combinación de impactos específicos, conforme a la siguiente tabla:

Tipo de riesgo	Factores que deben considerarse para evaluar el impacto
Riesgo de corrupción (soborno) y fraude	• Impacto negativo en el presupuesto (económico) • Finalización de la actividad organizacional (continuidad) • Afectación grave de la imagen y reputación (reputación) • Consecuencias legales (legal)

9.2.2. Nivel de Criticidad del riesgo

El nivel de criticidad se evalúa según lo establecido en el numeral 8.6.

9.3. Identificación de controles

AMSAC define controles preventivos en el proceso de selección de personal con el propósito de incorporar personas idóneas, mediante la aplicación del procedimiento de debida diligencia en aquellos puestos de mayor exposición al riesgo de fraude y corrupción (soborno); además se ejecuta el procedimiento de mitigación de riesgos de corrupción (soborno) y fraude en puestos y roles sensibles.

Los controles deben permitir hacer tratamiento a los posibles impactos que pueden ocasionar estos eventos tales como impacto económico, legal, reputacional o en la continuidad.

Cuando corresponda, el dueño de proceso debe adoptar acciones orientadas al fortalecimiento de los controles existentes, el diseño de nuevos controles, automatización de controles, incremento de medidas de seguridad, entre otras.

9.4. Tratamiento al riesgo

Una vez calificado el riesgo residual, se debe definir un plan de tratamiento que reduzca el nivel de impacto en el aspecto económico, legal, reputacional o en la continuidad; asimismo, se considera lo establecido en el numeral 8.9.

9.5. Seguimiento y monitoreo continuo

Se debe realizar el seguimiento y monitoreo de los planes de acción con el fin de evaluar su nivel de implementación; además adoptar medidas correctivas ante la posibilidad de deficiencias de controles o puntos de mejora para la ejecución de los procesos, con la finalidad de garantizar la mejora continua.

X. GESTIÓN DE LOS CONFLICTOS DE INTERÉS

10.1. Autonomía

Con el fin de evitar los conflictos de interés en AMSAC, que decantan en riesgos de corrupción o fraude, se establece la autonomía de los responsables de la Gestión Integral de Riesgos en la ejecución de las principales actividades de esta función.

10.2. Criterios para la prevención y tratamiento de conflictos de interés

a. Prevención de conflicto de intereses:
   - Los trabajadores considerados sujetos obligados deben presentar su declaración jurada de intereses ante la Contraloría General de la República, al inicio, periódicamente y al cese del vínculo con la entidad, dentro de los plazos previstos en la normativa aplicable.
   - Los trabajadores que participen en procesos de selección de personal, bienes, servicios u obras y otros procesos sensibles a riesgos de corrupción, fraude o conflicto de interés,

deben declarar expresamente la existencia o inexistencia de conflicto de intereses que pudieran afectar su imparcialidad y objetividad, mediante la suscripción de declaraciones juradas, antes de su participación en dichos procesos o actividades.

b. Tratamiento de conflictos de intereses: Cuando se identifique una situación de conflicto de intereses aparente, potencial o real, los trabajadores deben:
- Comunicar de manera inmediata a su jefe inmediato y al Oficial de Cumplimiento, Integridad y Prevención sobre la situación identificada, proporcionando la información necesaria para su evaluación.
- Abstenerse de participar en decisiones o actuaciones relacionadas con la situación identificada, hasta que la instancia competente evalúe y determine las medidas que correspondan.
- Cumplir las medidas dispuestas por las instancias competentes para prevenir, mitigar o resolver el conflicto de intereses, salvaguardando la imparcialidad, la transparencia y los intereses de la entidad.

XI. GESTIÓN DE RIESGOS DE CONTINUIDAD OPERATIVA

La gestión de continuidad operativa en AMSAC está dirigida por una estructura organizacional responsable de analizar el impacto de las interrupciones en la empresa, informar, dirigir, tomar decisiones cuando se generen interrupciones operativas y autorizar el financiamiento de los recursos necesarios para recuperar las operaciones continuas. Los alcances funcionales de la estructura organizacional se detallan en el Plan de Continuidad Operativa, que está alineado con las buenas prácticas y normas de continuidad operativa y Metodología establecida por FONAFE

11.1. Identificación de riesgos de continuidad operativa

11.1.1. Identificación de riesgo de continuidad operativa a nivel de entidad

El riesgo de continuidad operativa a nivel de entidad es el que afecta severa y simultáneamente a los recursos o componentes de los procesos de la empresa, los mismos que son transversales a todos los procesos. Para identificar los riesgos, se solicita información al personal clave que aplica controles a estos riesgos y se debe identificar cuál o cuáles recursos o componentes puede afectar el riesgo. La identificación y evaluación de los riesgos de continuidad operativa deberá considerar los resultados del Análisis de Impacto al Negocio (BIA), los procesos críticos y los tiempos objetivo de recuperación.

a. Recursos o componentes afectados

Recursos Humanos	Indisponibilidad del personal involucrado en la ejecución de los procesos de la empresa.
Infraestructura Física	Indisponibilidad de las instalaciones o ambientes físicos (incluyendo servicios básicos de energía eléctrica, agua, desagüe, etc.), donde se ejecutan los procesos de negocio de la empresa.
Recursos de Trabajo	Indisponibilidad de mobiliario, insumos y/o equipos necesarios para la operación (escritorios, sillas, computadoras, impresoras, teléfonos, etc.) de los procesos en la empresa.
Registros Vitales	Indisponibilidad de recursos relacionados con la información y/o documentación clave, indispensables para la realización de las operaciones de los procesos en la empresa.

Se podrá tomar en cuenta el catálogo de peligros detallado en el Plan de Continuidad Operativa de AMSAC.

11.1.2. Identificación de riesgo de continuidad operativa a nivel de procesos.

El riesgo a nivel de proceso es el que afecta la continuidad de las actividades o funciones de los procesos críticos priorizados que se requiere recuperar y continuar operando ante eventos disruptivos; y estos riesgos son identificados por los dueños de cada proceso.

Los procesos críticos priorizados se encuentran detallados en el Plan de Continuidad Operativa, el cual define las acciones y recursos necesarios para asegurar la recuperación y continuidad de las operaciones ante eventos disruptivos.

11.1.3. Evaluación de riesgos de continuidad operativa

La evaluación de los riesgos de continuidad operativa se realiza según lo indicado en el numeral 8.6 del presente documento.

11.1.4. Identificación de controles

La identificación de controles se realiza según lo indicado en el numeral 8.7 del presente documento.

11.1.5. Estrategias de respuesta y planes de acción de tratamiento al Riesgo

Se determina según lo indicado en el numeral 8.9 del presente documento.

XII. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de los riesgos de Seguridad de la Información, asociados a los riesgos en el ambiente de **Tecnologías de la Información y Comunicaciones**, se desarrolla conforme a lo establecido en la presente Metodología para la Gestión Integral de Riesgos, garantizando un tratamiento alineado al enfoque institucional y a las disposiciones vigentes.

La gestión de riesgos de Seguridad de la Información tiene como propósito identificar, evaluar y tratar aquellos eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información de AMSAC, considerada un activo estratégico para el cumplimiento de sus objetivos institucionales. Permite prevenir incidentes, establecer controles adecuados y garantizar la continuidad de las operaciones, de conformidad con los lineamientos de FONAFE y las mejores prácticas internacionales de gestión de riesgos.

12.1. Inventario de activos de información

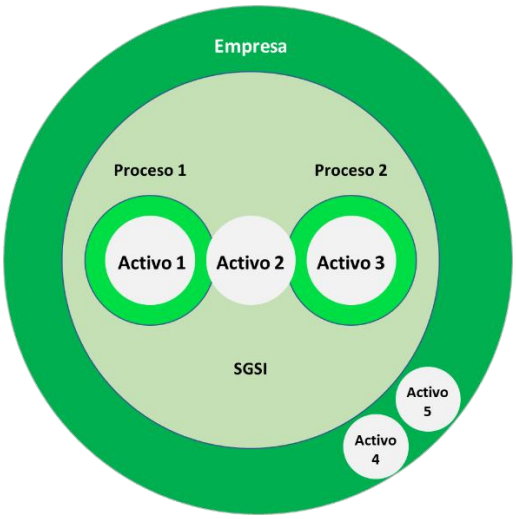
Para identificar los activos de la información[2], se sugiere que se ejecuten las siguientes actividades:

12.1.1. Identificación de los procesos que forman parte del alcance del SGSI

Los activos de la información que son de interés para la gestión de riesgos de seguridad de la información son aquellos que están contenidos en los procesos que forman parte del alcance del SGSI, detallados en el Manual del Sistema Integrado de Gestión

Gráfico: Relación entre activos de información y el alcance del SGSI

[2] AMSAC documenta la asignación de activos de información a los colaboradores de la empresa mediante el “Acta de Asignación de Activos de Información”.



12.1.2. Establecimiento de un modelo para valorar los activos de información

No todos los activos de información tienen la misma importancia, la identificación de los activos más críticos está en función del grado requerido de su confidencialidad, integridad y disponibilidad (CID) por AMSAC. Por ello, es necesario establecer una forma de valoración del activo de información.

A continuación, se describe la fórmula para valorar el activo de información (promedio o valor mayor) sobre la base de los principios de seguridad de la información tales como la confidencialidad, integridad y disponibilidad del activo de información:

$$Valor\ del\ Activo: \frac{(Confidencialidad + Integridad + Disponibilidad)}{3}$$

En la siguiente tabla se detallan ejemplos de rangos de valores y descripciones de cada nivel de valorización de los activos para riesgos de seguridad de la información y riesgos de privacidad

Tabla: Ejemplo de rangos de valores y descripciones de los activos de información para riesgos de seguridad de la información

Valor	Confidencialidad	Integridad	Disponibilidad
Extremo 4	La información asociada al activo —que puede incluir datos personales sensibles y documentación estratégica— es de carácter estrictamente confidencial y solo puede ser accedida por Directores, Gerentes o personal expresamente autorizado y con funciones especializadas. Su divulgación no autorizada podría comprometer la ejecución de procesos críticos institucionales, afectar el cumplimiento de mandatos legales o contractuales, exponer a la empresa a sanciones o demandas por vulneración de derechos de terceros, generar pérdida de confianza de entidades del Estado y de la ciudadanía, o deteriorar la imagen pública de AMSAC.	El activo de información no puede tolerar pérdida o alteración de sus componentes (físicos o lógicos o de información o de condición de servicio) ya que paralizaría o comprometería seriamente el desempeño de los procesos críticos de la empresa. Los cambios, autorizados y planificados, en los componentes se requieren o ejecutan rara vez (ninguna o una vez al año). Los cambios conllevan un sistema de aprobaciones de alto nivel en el que participan personas específicas.	El activo de información siempre debe estar disponible, pues su carencia afectaría el flujo de las actividades operativas de los procesos críticos de la empresa.
Alto 3	La información (que incluye datos personales) asociada al activo es restringida. Sólo personal clave o personal especializado puede acceder a ella, la divulgación comprometería el cumplimiento normativo (externo o interno), la reputación e imagen de la empresa y los requisitos de seguridad de las partes interesadas.	El activo de información puede tolerar alteración, planificada y autorizada (incluye las autorizaciones de los titulares de datos personales, de ser el caso), de sus componentes (físicos o lógicos o de información o de condición de servicio). Los cambios son autorizados y realizados por un pequeño grupo de personas. La	El activo de información no puede estar no disponible por más de dos horas, su carencia afectaría la operación de procesos críticos y operacionales.

Valor	Confidencialidad	Integridad	Disponibilidad
		alteración no autorizada podría ocasionar interrupciones no aceptables o resultados inconsistentes en los procesos de la empresa. Los cambios ocurren con poca frecuencia, de 2 a 4 veces por año.	
Medio 2	La información (que incluye datos personales) asociada al activo de información es de uso interno. Sólo el personal y proveedores autorizados pueden acceder a ella, su divulgación afectaría el cumplimiento normativo (externo o interno), la reputación e imagen de la empresa, los requisitos de seguridad de las partes interesadas involucradas y los procesos de las áreas involucradas.	El activo de información puede tolerar alteración, planificada y autorizada (incluye las autorizaciones de los titulares de datos personales, de ser el caso), de sus componentes (físicos o lógicos o de información o de condición de servicio). Los cambios ocurren con mucha frecuencia, más de 4 veces al año. Los efectos de una alteración no autorizada podrían generar degradaciones generales en los procesos no críticos o degradaciones menores en procesos críticos. Los efectos de una alteración no autorizada se pueden corregir con controles correctivos.	El activo de información no puede estar no disponible por más de un día, su carencia afectaría la operación de procesos operacionales o de soporte.
Bajo 1	La información (que incluye datos personales) asociada al activo de información está prevista para ser de acceso público. Cualquier parte interesada puede acceder a ella, pues no impacta a la organización.	El activo de información puede tolerar alteraciones controladas (registradas) de sus componentes (físicos o lógicos o de información o de condición de servicio) por parte de quienes cuenten con autorización asignada previamente para tal fin. Los cambios pueden ocurrir en cualquier momento	El activo de información puede estar no disponible por más de un día, su carencia afectaría una actividad menor de uno o varios procesos.

12.1.3. Identificación los activos de información

Luego se identifican los activos de información de cada uno de los procesos detallados en el alcance de implementación del SGSI.

12.1.4. Establecimiento de las categorías de activos de información

Definir las categorías de los activos de información (información, software, físicos, servicios, personal, datos personales entre otros) para, posteriormente, clasificar los activos de información identificados en el paso anterior.

A continuación, algunos ejemplos de categorías de activos de información.

- Activos de información: todo aquello que es información o contiene información y tiene valor para el proceso y/o empresa, incluyendo los datos personales que gestiona AMSAC.
- Activos de software: programas, sistemas de información, aplicaciones, entre otro aplicativo que contenga la lógica del proceso.
- Activos físicos: soporte físico que es relevante para el procesamiento, comunicación, almacenamiento y/u operación del activo.
- Servicios: conjunto de actividades internas o externas que brindan funcionalidades y requerimientos específicos.
- Personal: recurso humano que dispone información y/o experiencia importante que no se encuentra en algún otro medio.

Gráfico: Clasificación de activos de información



12.1.5. Documentar los activos de información

Los activos de información identificados se documentan, para ello, se establece que cada activo de información tenga los atributos estipulados en el Formato E3.1.M3.F2 Matriz de riesgos de Seguridad de la información de Activos.

AMSAC establece el criterio para seleccionar aquellos activos que serán analizados y evaluados. AMSAC establece que, si el valor de tasación del activo de información es extremo o alto, se considera un activo crítico y este debe pasar a la fase de análisis de riesgo. AMSAC puede cambiar esta definición en el momento que lo considere pertinente.

Tabla: Niveles de tasación de activos

Tasación	Rango
Extremo	3.50 - 4.00
Alto	2.50 - 3.49
Medio	1.50 - 2.49
Bajo	1.00 – 1.49

12.2. Análisis de la exposición de los activos de información

Para identificar las vulnerabilidades y amenazas actuales sobre los activos de información, se sugiere utilizar las técnicas para la identificación de riesgos: "Análisis de fortalezas y debilidades, oportunidades y amenazas" y "Diagrama de Ishikawa", o las establecidas en el numeral 8.5.1

12.2.1. Identificación de las vulnerabilidades del activo de la información

En este paso se identifican y registran las vulnerabilidades de los activos de información.

- Hardware: Mantenimiento insuficiente, almacenamiento no protegido, susceptibilidad al polvo y a la corrosión, copiado no controlado, cableado inadecuado, puertos inalámbricos no configurados o puertos físicos sin uso activos, entre otros.

- Software: Fallas conocidas en el software, falta de copias de respaldo, fallas en el cierre de sesión, falta de documentación, inadecuado manejo de contraseñas, indisponibilidad de los servicios de TI y ciberseguridad.
- Red: Tráfico sensible desprotegido, inseguridad de arquitectura de red, transferencia de contraseñas en texto plano, entre otros.
- Personal: Ausencia de personal, capacitación insuficiente en seguridad, falta de mecanismo de seguimiento, uso incorrecto de software y hardware, entre otros.
- Local: Ubicación en un área susceptible de inundación, red de energía inestable, falta de protección física del local y a los accesos a las instalaciones de la empresa, entre otros.

12.2.2. Identificación de las amenazas sobre los activos de información

Los activos de información están sujetos a muchas fuentes de amenazas que explotan sus vulnerabilidades. A continuación, se detallan algunos ejemplos de fuentes de amenazas:

- Desastres naturales: incendio, terremoto, avalancha, huaico, inundación, tornado, viento, volcán, tsunami, tormenta de invierno, tormenta solar, tormenta eléctrica/relámpago, entre otros.
- Humanas: divulgación de información por email, sabotaje, terrorismo, acciones de los hackers, ingeniería social, errores de mantenimiento, huelga, errores de usuario, uso de software pirata, corrupción o destrucción de la información, errores de programación o de software, suplantación de identidad de usuario, etc.
- Tecnológicas: fuga de información, virus y malware, caída de red, exceso de tráfico, falla de sistemas de información (hardware y software), errores en los servicios contratados externamente (incluidos los servicios de ciberseguridad), entre otros.

12.3. Criterios de identificación del riesgo de seguridad de la información

Para la gestión de riesgos de seguridad de la información y controles identificados, así como las calificaciones obtenidas producto de la evaluación de cada riesgo, se utiliza el Formato E3.1.M3.F2 Matriz de Riesgos de Seguridad de la Información de Activos.

12.3.1. Descripción del evento de riesgo de seguridad de la información

El evento de riesgo de seguridad de la información se construye considerando la relación entre la amenaza y la vulnerabilidad detectadas, de acuerdo con el enfoque definido en esta metodología.

En la siguiente tabla se muestra un ejemplo de cómo se construye la narración del riesgo o escenario de riesgo

Descripción del riesgo de seguridad de la información

Elemento	Narración de Riesgo de Seguridad de la Información
Activo de información	Archivos de configuración lógica de switches y router.
Amenaza a la confidencialidad	Acceso no autorizado a los archivos de configuración lógica de switches y router, por parte de atacantes internos y/o atacantes externos.
Vulnerabilidad	No se guardan los archivos de configuración lógica de switches y router con algún software de cifrado en los discos duros de los administradores
Descripción del riesgo (ejemplo de redacción del riesgo)	Que se genere paralización en la operación de la red o que se expongan datos y servicios debido al acceso no autorizado a los archivos de configuración lógica de switches y router o debido a que los archivos de configuración lógica de switches y router no están encriptados, lo cual, a su vez, podría generar una sanción económica

12.3.2. Identificación de los impactos sobre AMSAC

La estimación del impacto se basa en la pérdida cualitativa que se pudiera generar si se materializara el riesgo. Para este criterio se consideran factores de confidencialidad, integridad y disponibilidad.

En la presente metodología, se define el impacto como el nivel de afectación de la empresa o el proceso, respecto de los distintos factores relevantes con que cuenta la empresa. Se establecen factores relevantes en la tabla.

Tabla: Factores de riesgos de seguridad de la información

Factor a considerar para evaluar el impacto
Confidencialidad: la consecuencia del riesgo que afecta la confidencialidad permite que personas no autorizadas accedan a la información. **Integridad:** la consecuencia del riesgo que afecta la integridad permite alterar o corromper la información. **Disponibilidad:** la consecuencia del riesgo que afecta la disponibilidad impide acceder a la información cuando se requiera

En la siguiente tabla se detallan los tipos de impacto (confidencialidad, integridad y disponibilidad) y su efecto.

Ejemplo de correspondencia entre factores de riesgos de seguridad de la información, tipos de impacto y valorización del tipo de impacto.

Factor Valor	Bajo 4	Medio 3	Alto 2	Extremo 1
Impacto en la confidencialidad	Las amenazas y vulnerabilidades no exponen la confidencialidad del activo y se mantienen los accesos al personal autorizado	Las amenazas y vulnerabilidades exponen la confidencialidad del activo a personal no autorizado de una o algunas áreas	Las amenazas y vulnerabilidades exponen la confidencialidad del activo a todo el personal de la empresa con potencial de trascender externamente	Las amenazas y vulnerabilidades exponen la confidencialidad del activo a usuarios externos y público en general
Impacto a la Integridad	Las amenazas y vulnerabilidades no alteran o modifican los componentes físicos o lógicos del activo	Las amenazas y vulnerabilidades alteran o modifican menos de la mitad de los componentes físicos o lógicos del activo	Las amenazas y vulnerabilidades alteran o modifican más de la mitad de los componentes físicos o lógicos del activo	Las amenazas y vulnerabilidades alteran o modifican todos los componentes físicos o lógicos del activo
Impacto a la disponibilidad	Las amenazas y vulnerabilidades no afectan la disponibilidad del activo	Las amenazas y vulnerabilidades pueden generar indisponibilidad del activo entre 0.01 y 02 horas	Las amenazas y vulnerabilidades pueden generar indisponibilidad del activo entre 02 y 24 horas	Las amenazas y vulnerabilidades pueden generar indisponibilidad del activo por más de 24 horas

Se otorgará el valor de 4 al nivel “bajo”, el valor de 3 al nivel “medio”, el valor de 2 al nivel “alto” y el valor de 1 al nivel “extremo”.

12.3.3. Cálculo del nivel de exposición al riesgo inherente

Para efectos de esta metodología, el cálculo del impacto promedio es inversamente proporcional a los niveles de impacto en la confidencialidad, integridad y disponibilidad, esto debido a que dichos impactos permiten ver el grado de afectación en los niveles de CID del activo, como consecuencia de las amenazas, vulnerabilidades y el riesgo.

$$Impacto\ promedio = 5 - \frac{Impacto\ C + Impacto\ I + Impacto\ D}{3}$$

Por ejemplo, si el impacto en C+D+I es **3** en cada componente el valor del impacto promedio sería de **2**. A continuación, se muestra la aplicación de la fórmula para obtener el resultado:

$$Impacto\ promedio = 5 - \frac{3+3+3}{3} = 5 - \frac{9}{3} = 5 - 3 = \mathbf{2}$$

El nivel de exposición al riesgo es el producto del nivel de impacto y de la probabilidad de ocurrencia del riesgo. De esta forma, se calcula el nivel de exposición al riesgo, según el promedio indicado:

$$\begin{pmatrix} Nivel\ de \\ exposición \\ al\ riesgo \end{pmatrix} = (Nivel\ de\ Impacto\ promedio) * \begin{pmatrix} Probablilidad\ de \\ ocurrencia\ del\ riesgo \end{pmatrix}$$

La multiplicación de las puntuaciones de ambos criterios dará el valor que determinará el nivel de exposición al riesgo (severidad): extremo, alto, medio o bajo, tal como se muestra en el siguiente cuadro:

Tasación de riesgo	Valor	Prioridad de atención
Extremo	10.00 – 16.00	Inmediato (I)
Alto	5.00 – 9.99	Corto plazo (C)
Medio	2.50 – 4.99	Se acepta el riesgo
Bajo	1.00 – 2.49	Se acepta el riesgo

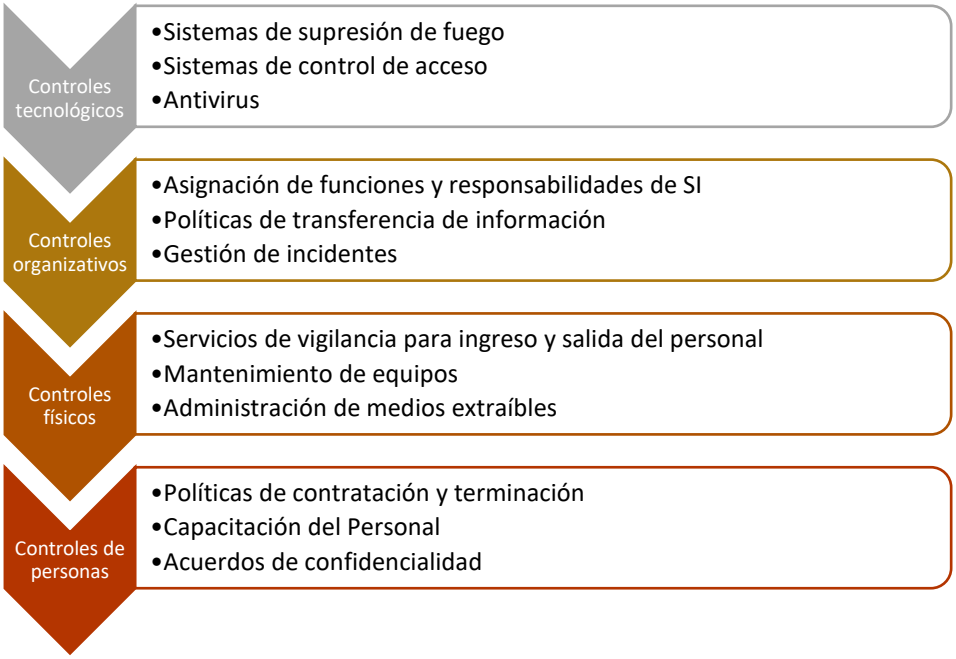
Una vez culminada la evaluación, se construye el mapa de riesgos a efectos de poder visualizar dónde se ubican los riesgos de seguridad de la información. El mapa de riesgos está alineado a lo establecido en el numeral 8.6.1.

12.4. Identificación de controles

Para la identificación de los controles actuales aplicables a los activos de información, se utiliza como referencia la siguiente tabla, la cual permite abordar las vulnerabilidades y amenazas que afectan dichos activos y sus atributos. En esta tabla se consideran los siguientes criterios:

- Clasificación: organizacional, de persona, físico o tecnológico.
- Oportunidad del control: preventivo, detectivo o correctivo.
- Responsable del control
- Automatización del control
- Objetivo de seguridad de la información: confidencialidad, integridad y/o disponibilidad
- Objetivo de ciberseguridad: gobernar, identificar, proteger, detectar, responder o recuperar.
- Capacidades operativas
- Dominios de seguridad
- Evidencia del control

Tabla: Tipos de controles por su clasificación

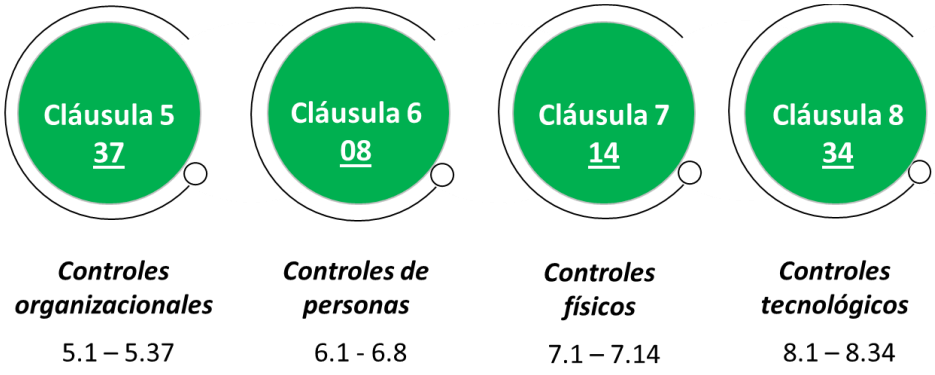


12.5. Selección de controles que mitiguen los riesgos

En los casos en los cuales se requiera de la implementación de un control, se recomienda realizar lo siguiente:

- En el gráfico se detallan los controles de la matriz de aplicabilidad elaborada sobre la base de la norma ISO/IEC 27002, en la cual se incluyen 4 grupos que contienen 93 controles.

Gráfico: Cláusulas del marco de controles ISO/IEC 27002



- Diseñar el control.
- Planificar la implementación del control.
- Documentar el control mediante el registro de los siguientes datos:
  - Responsable de la implementación.
  - Plazo de implementación (colocar fechas específicas o rangos de tiempo).
  - Qué: es la descripción del control, su composición.
  - Quién: el responsable de la gestión del control.

12.5.1. Documentación de las acciones para el tratamiento del riesgo

En el numeral 8.9 se establecen los criterios a tomar en cuenta para los planes de acción.

Para los riesgos de seguridad de la información, la Matriz de Riesgos incorpora las columnas del "Anexo A de la ISO 27001", con el fin de vincular los planes de acción con los controles de seguridad establecidos en dicho anexo.

- Objetivo de seguridad de la información: confidencialidad, integridad y/o disponibilidad
- Objetivo de ciberseguridad: gobernar, identificar, proteger, detectar, responder o recuperar.
- Capacidades operativas
- Dominios de seguridad

12.5.2. Verificación de la eficacia

La verificación de la eficacia consiste en validar si los planes de acción implementados cumplieron sus objetivos. Para la verificación de la eficacia, se recomienda utilizar los pasos establecidos en los numerales 8.11.1 y 8.11.2.

XIII. GESTIÓN DE OPORTUNIDADES

Para la gestión de oportunidades, se realizarán las siguientes actividades secuenciadas e interrelacionadas:

13.1. Identificación de oportunidades.
Se identifican y describen las oportunidades y sus atributos.

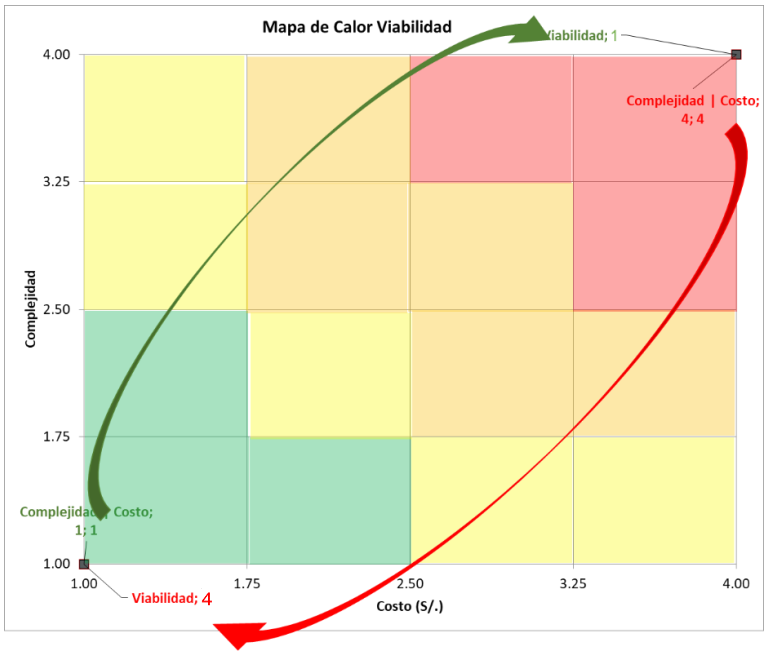
13.2. Evaluación de oportunidades
El Responsable designado de la GIR valida que, al menos cada 2 años, las evaluaciones de las oportunidades tengan actualizaciones, en función de la posibilidad de que estas se aprovechen oportunamente. Las oportunidades son evaluadas en función de su viabilidad (costo y/o complejidad para su implementación) y beneficio (beneficio económico y/o no económico para su implementación).

13.3. Criterios de Evaluación de Oportunidades
Los criterios de evaluación de la oportunidad se han establecido en las siguientes tablas:

Criterios de viabilidad

Nivel de Costo / Complejidad	Costo (Recurso Financiero)	Complejidad (Tiempo)
Bajo 1	< S/ 35,000	La oportunidad podría materializarse en menos de 2 meses
Medio 2	S/ 35,000 - menos de S/ 100,000	La oportunidad podría materializarse entre 2 y menos de 12 meses
Alto 3	S/ 100,000 - menos de S/ 250,000	La oportunidad podría materializarse entre 12 y menos de 24 meses
Muy Alto 4	S/ 250,000 o más	La oportunidad podría materializarse 24 meses o más

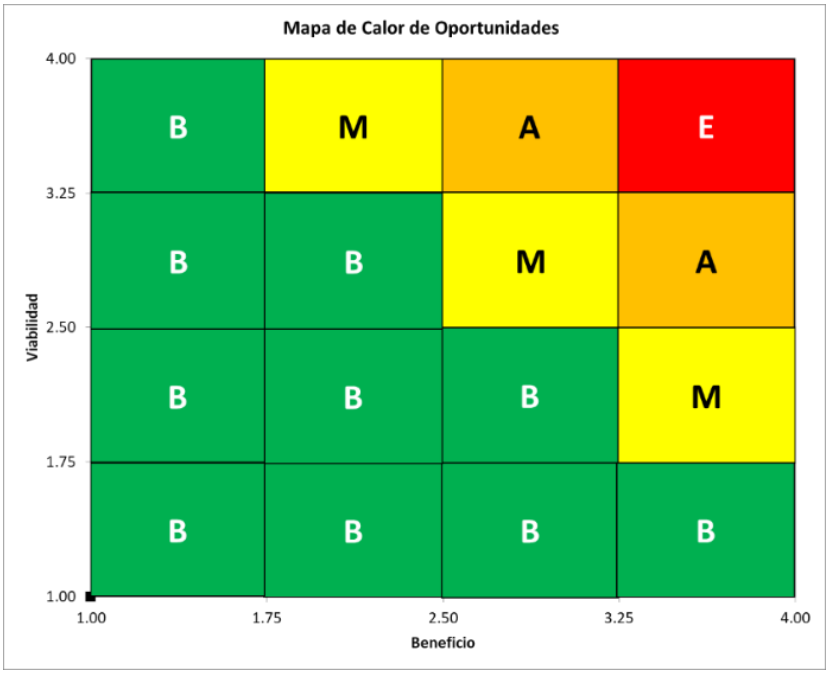
La viabilidad se calcula a partir del promedio del nivel de complejidad y del costo, de manera inversa, tal como se aprecia en el siguiente gráfico:



Niveles de beneficio

Nivel de Beneficio	Beneficio Económico
Bajo 1	Pueden presentarse uno o más de los siguientes criterios: El beneficio que puede generar en la empresa es bajo. El periodo de recuperación dela inversión es mayor de 6 años. Impacto bajo en la estrategia, en la operatividad de la empresa o en la calidad de los productos y servicios. Bajo interés de las partes interesadas. Mejora poco relevante del desempeño ambiental, de seguridad y salud en el trabajo u otro.
Medio 2	Pueden presentarse uno o más de los siguientes criterios: El beneficio que puede generar en la empresa es moderado. El periodo de recuperación de la inversión es mayor de 3 años y menor de 6 años. Impacto moderado en la estrategia, en la operatividad de la empresa o en la calidad de los productos y servicios. Moderado interés de las partes interesadas. Moderada mejora del desempeño ambiental, de seguridad y salud en el trabajo u otro.
Alto 3	Pueden presentarse uno o más de los siguientes criterios: El beneficio que puede generar en la empresa es alto. El periodo de recuperación de la inversión es mayor de 1 año y menor de 3 años. Fuerte impacto en la estrategia, en la operatividad de la empresa o en la calidad de los productos y servicios. Elevado interés de las partes interesadas. Alta mejora del desempeño ambiental, de seguridad y salud en el trabajo u otro.
Muy Alto 4	Pueden presentarse uno o más de los siguientes criterios: El beneficio que puede generar en la empresa es muy alto. El periodo de recuperación de la inversión es menor o igual a 1 año. Muy fuerte impacto en la estrategia, en la operatividad de la empresa o en la calidad de los productos y servicios. Muy elevado interés de las partes interesadas. Muy alta mejora del desempeño ambiental, de seguridad y salud en el trabajo u otro.

Una vez establecido el nivel de viabilidad y beneficio, se calcula la priorización de la oportunidad a partir del producto de ambos criterios. A continuación, se muestra el mapa de calor con las zonas que establecen los niveles posibles de priorización.



La zona superior derecha muestra las oportunidades con mayor nivel de priorización (extremo) mientras que la zona inferior izquierda señala las oportunidades con menor nivel de priorización (bajos), la zona intermedia comprende las oportunidades con nivel de priorización medio o alto.

Luego de priorizar la oportunidad, se identifica la estrategia de respuesta frente a las oportunidades, las cuales son:

Estrategia	Descripción
Explotar	Esta estrategia busca eliminar la incertidumbre asociada con una oportunidad haciendo que la oportunidad definitivamente se concrete. Explotar las respuestas directamente incluye asignar recursos.
Mejorar	Esta estrategia modifica el “tamaño” de una oportunidad, aumentando la probabilidad y/o los impactospositivos, e identificando y maximizando las fuerzas impulsoras clave de estas oportunidades. Busca facilitar o fortalecer la causa de la oportunidad, y dirigirse de forma proactiva a las condiciones que la disparan y reforzarlas, puede aumentar la probabilidad. También puede centrarse en las fuerzas impulsoras del impacto, buscando aumentar la susceptibilidad de la organización a la oportunidad.
Compartir	Esta estrategia implica asignar la propiedad a un tercero que está mejor capacitado para capturar la oportunidad en beneficio de la empresa. Entre los ejemplos de acciones para compartir se incluyen:formar asociaciones de riesgo conjunto, equipos, empresas con finalidades especiales o uniones temporales de empresas, que se pueden establecer con la finalidad expresa de gestionar oportunidades.
Aceptar	Esta estrategia indica que se ha decidido no aprovechar una oportunidad, o no ha podido identificar ninguna otra estrategia de respuesta adecuada.

13.4. Plan de tratamiento de oportunidades

Se define y documenta formalmente la actividad a ser implementada mediante el plan de acción, al responsable de realizarla, el plazo, los mecanismos de seguimiento y los recursos. Asimismo, se realiza una vez al año la verificación de la eficacia de los planes de acción.

13.5. Seguimiento y monitoreo continuo

El seguimiento de los planes de acción de oportunidades se reporta trimestralmente al Gerente General. La evaluación de la gestión de oportunidades se incluye en los informes del primer y segundo semestre remitidos a FONAFE.

XIV. EVENTOS DE PÉRDIDA

14.1. Identificación de eventos de pérdida

Todo evento que pudiera generar una pérdida económica, asociada a los riesgos detectados, debe ser documentado por el dueño de proceso donde ocurre la pérdida y reportado a través de la Matriz de Eventos de Pérdida, de manera trimestral, al Responsable designado de la GIR.

14.2. Registro de eventos de pérdida

El monto mínimo para el registro de eventos de pérdida en la matriz de eventos de pérdida es de 0,5 UIT vigente para el año en que se registra la pérdida contablemente.

No deben ser considerados como eventos de pérdida:

- Eventos que conducen a costos de oportunidad o ganancias no realizadas
- Eventos que causaron solamente daño reputacional.
- Eventos por desfase de registros contables que no signifiquen pérdidas reales. Un impacto por desfase de registros es una distorsión temporal al estado de pérdidas y ganancias de un periodo en particular, que es corregido totalmente cuando posteriormente se descubre. El estado de pérdidas y ganancias es cambiado de un periodo a otro.
- Los impactos por desfase de registro surgidos de eventos de riesgo operacional, no son reportados al Responsable designado de la GIR. Sin embargo, cualquier multa, sanción, penalidad o interés neto que resulte de este desfase es un evento de pérdida que debe ser reportado, debido a que genera una afectación permanente para el estado de pérdidas y ganancias.

Se debe clasificar el evento por su naturaleza principal y registrar sus consecuencias vinculadas, evitando contabilizar dos veces la misma pérdida.

Los eventos de pérdida tienen los siguientes estados:

- Evento en proceso: Para el caso de provisiones o cuando la contabilización del evento aún no ha concluido.
- Evento cerrado: Cuando la pérdida se ha ejecutado/pagado.

14.3. Tipos de eventos de pérdida

Los siguientes ejemplos no son limitativos y pueden ampliarse o ajustarse según las necesidades de AMSAC.

Tipos de Evento de Pérdida				
Nivel 1	**Definición**	**Cod.**	**Nivel 2**	**Ejemplos**
Fraude Interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas internas en las que se encuentran implicados trabajadores	**FI.1**	**Actividades no autorizadas**	Operaciones no autorizadas, según las disposiciones internas de AMSAC, por ejemplo:
				-Otorgamiento de buena pro a un proveedor que no cumple con todos los requisitos establecidos en los términos de referencia.
				-Operaciones no reveladas, no registradas, no informadas u ocultadas internamente.
				-La valoración intencionalmente errónea de inmuebles, muebles, otros tipos de activos en desuso a favor de un tercero.

Tipos de Evento de Pérdida				
Nivel 1	**Definición**	**Cod.**	**Nivel 2**	**Ejemplos**
	de AMSAC, y que tiene como fin obtener un beneficio ilícito.	**FI.2**	**Robo y fraude**	- Pérdidas generadas por malversación, robo, falsificación de documentos, alteración no autorizada de registros (físicos o digitales), soborno, apropiación indebida de activos, apropiación y/o uso de credenciales o accesos de otros trabajadores/proveedores, destrucción dolosa de activos, incluyendo los ataques informáticos internos, utilización de cheques sin fondos, evasión intencional de impuestos o uso indebido o no autorizado de los recursos de AMSAC.
Fraude Externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de un activo indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.	**FE.1**	**Robo y fraude**	- Pérdidas generadas por robo de activos, falsificación de documentos o presentación de documentos no vigentes para realizar operaciones con AMSAC, o daños inexistentes reportados en solicitudes de reclamo.
				- Pérdidas por apropiación de bienes o recursos institucionales mediante engaño o acceso no autorizado.
		FE.2	**Ciberseguridad y Seguridad de los sistemas**	- Daños por ataques informáticos (virus, hackers).
				- Robo y divulgación de información corporativa y personal que conducen a pérdidas monetarias y contingencias legales.
				- Robo de información a través de ingeniería social.
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre salud o seguridad en el trabajo, el pago de reclamos por daños personales, o casos relacionados con la diversidad o discriminación.	**RL.1**	**Relaciones laborales**	- Costos relacionados con eventuales demandas por incumplimientos de acuerdos laborales como el pago de la CTS.
				- Indemnización por despidos arbitrarios, vacaciones no gozadas.
				- Demandas judiciales por beneficios no otorgados u otorgados de forma incompleta al trabajador.
		RL.2	**Seguridad y salud en el trabajo**	- Indemnización a un trabajador por daños a su salud física y/o mental como consecuencia de sus actividades laborales.
				- Indemnización a un tercero por daños a su integridad física en las instalaciones de AMSAC.
				- Multas por incumplimientos a las normas relativas al acoso laboral u hostigamiento sexual.
				- Multas por incumplimientos a las normas de seguridad en Defensa Civil.
				- Multas por incumplimientos a la normativa laboral, detectadas en inspecciones laborales realizadas por el Ministerio de Trabajo.
		RL.3	**Diversidad y discriminación**	- Demandas por despidos improcedentes (que no correspondan a decisiones estratégicas u operativas y que responden a prácticas discriminatorias como, por ejemplo, el ser despedido por creencias religiosas.
				- Demandas por políticas de selección y contratación que discriminen a personas por su género, su simpatía a un determinado grupo político, entre otros.
				- Multas por inequidad remunerativa.
Prácticas empresariales relacionadas con los clientes, los productos y las operaciones	Pérdidas derivadas del incumplimiento involuntario o negligente de obligaciones frente a terceros, de la divulgación o gestión inadecuada de información, o de actuaciones que afecten la confianza en las relaciones institucionales de AMSAC.	**PE.1**	**Adecuación, divulgación de información y confianza**	- Demandas por abusos de confianza, entre otros.
				- Quebrantamiento de la privacidad de información sobre clientes, proveedores, trabajadores y contrapartes.
				- Pérdidas derivadas de información inexacta, incompleta o divulgada indebidamente sobre encargos, proyectos o resultados institucionales.
				- Costos o consecuencias económicas derivados de actuaciones que deterioren la confianza de las entidades con las que AMSAC se relaciona institucionalmente o de las comunidades beneficiarias, cuando exista una pérdida identificable.
		PE.2	**Prácticas empresariales improcedentes**	- Demandas o sanciones por la comisión o servir de medio para la comisión de actividades ilícitas relacionadas a blanqueo de dinero, evasión de capitales y financiamiento del terrorismo.
		PE.3	**Productos o servicios defectuosos**	- Costos de reparación, corrección o reproceso de estudios, expedientes técnicos, obras o servicios que no cumplan las especificaciones o requisitos contractuales y técnicos aplicables.
				- Pérdidas derivadas de deficiencias en las soluciones de remediación que impidan alcanzar los resultados técnicos o ambientales previstos.

Tipos de Evento de Pérdida				
Nivel 1	**Definición**	**Cod.**	**Nivel 2**	**Ejemplos**
				- Costos adicionales por ejecutar medidas correctivas o complementarias debido a deficiencias de calidad en las obras o soluciones implementadas.
				- Pérdidas derivadas de resultados de remediación que no mantengan la eficacia ambiental esperada en el tiempo, cuando se determine que ello responde a deficiencias atribuibles al diseño, ejecución o calidad de la solución.
				- Demandas o sanciones por entregar a los clientes productos o servicios con parámetros o atributos que no coinciden con el plan de cierre o estudio ambiental aprobado.
Daños a activos físicos	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.	**DA.1**	**Desastres y otros acontecimientos**	- Pérdidas de activos a causa de un terremoto, o por causas externas (vandalismo, terrorismo).
				- Daños a plantas de tratamiento, instalaciones, equipos, infraestructura de remediación y otros activos institucionales por desastres naturales o eventos externos.
				- Indemnizaciones por accidentes en las instalaciones de AMSAC a causa de un terremoto.
				- Daños a instalaciones o activos por incendios, inundaciones, huaicos, movimientos de tierra u otros eventos, cuando corresponda.
Interrupción en la continuidad operativa y fallos en los sistemas	Pérdidas derivadas de interrupciones en las operaciones, fallas en los sistemas o indisponibilidad de instalaciones, equipos y servicios esenciales necesarios para el funcionamiento institucional.	**CN.1**	**Interrupción de operaciones, instalaciones y sistemas**	- Pérdidas por interrupciones operativas y costos adicionales ocasionados por fallas en instalaciones, infraestructura, equipos, maquinaria o servicios esenciales para las operaciones y remediación.
				- Pérdidas generadas por interrupciones operativas ocasionadas por fallas de contratistas encargados de operar o mantener instalaciones, equipos o servicios esenciales.
				- Costos extraordinarios por restablecer operaciones interrumpidas, implementar medidas de contingencia o mantener temporalmente las actividades afectadas por fallas operativas o tecnológicas.
				- Pérdidas originadas por falta de procesamiento oportuno de transacciones o reprocesos de transacciones debido a fallas en el hardware, el software, en la comunicación de dispositivos o en los servicios de tecnología contratados.
				- Pérdidas generadas por la imposibilidad de continuar temporalmente o los sobre costos generados por mantener una operación que es afectada por conflictos sociales
Deficiencia en la ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes, tales como proveedores, clientes, entre otros.	**DP.1**	**Recepción, ejecución y mantenimiento de operaciones**	- Reprocesos, sobre carga operativa (validaciones, auditoría) o sanciones generadas por problemas de entrada de datos en las aplicaciones, mantenimiento de aplicaciones o componentes tecnológicos o error de carga.
		DP.2	**Seguimiento y presentación de informes**	- Multas, sanciones o costos adicionales por presentar fuera de plazo o con errores informes técnicos, financieros, presupuestales o de avance a las entidades competentes.
				- Multas o reparaciones por diferencias en declaraciones tributarias.
				- Multas por información financiera o hechos de importancia no comunicados oportunamente.
				- Pérdidas derivadas de errores u omisiones en reportes de ejecución de proyectos, rendición de cuentas o cumplimiento de encargos.
		DP.5	**Incumplimiento de normativa**	-Multas o sanciones generadas por el incumplimiento de la normativa, interna o externa, aplicable.
		DP.6	**Contrapartes institucionales**	- Pérdidas derivadas del incumplimiento de compromisos asumidos por una entidad participante en un convenio de colaboración para la ejecución de actividades de remediación ambiental, cuando ello genere costos adicionales o afecte la ejecución prevista.
				- Costos adicionales o pérdidas derivados del incumplimiento de compromisos de una de las partes en convenios de cooperación

Tipos de Evento de Pérdida				
Nivel 1	**Definición**	**Cod.**	**Nivel 2**	**Ejemplos**
				para proyectos de innovación, sostenibilidad ambiental o transferencia tecnológica.
				- Pérdidas derivadas de la falta de cumplimiento de compromisos de coordinación, aporte de recursos, provisión de información o ejecución de actividades asumidos por una contraparte en un convenio.
				- Costos legales, administrativos u operativos derivados de controversias con entidades u otras contrapartes institucionales respecto de la interpretación, ejecución o cumplimiento de convenios.
				- Pérdidas derivadas de actuaciones u omisiones no dolosas de una contraparte que afecten la ejecución de actividades conjuntas y obliguen a AMSAC a asumir costos adicionales o implementar medidas de contingencia.
		DP.7	**Proveedores y contratistas**	- La pérdida originada por errores en la ejecución de tareas internas que han sido tercerizadas (proceso de operaciones, etc.).
				- Pérdidas generadas por el incumplimiento contractual de un proveedor o contratista.
				-Pérdidas generadas por litigios con proveedores o contratistas (costos y costas).

14.4. Evaluación de eventos de pérdida

El Responsable designado de la GIR revisa y evalúa los sustentos de la identificación de los eventos de pérdida, y coordina con el área de Contabilidad respecto al monto reportado. Asimismo, consolida la matriz de eventos de pérdida con la información de todos los procesos para la ejecución de la matriz a nivel de entidad.

El Responsable designado de la GIR coordina con los dueños de proceso para realizar el seguimiento a los planes de acción que se consideren necesarios.

14.5. Recuperación del evento de pérdida

El Responsable designado de la GIR coordina con el dueño de proceso y/o área correspondiente el estado de las acciones que se han planificado o se están ejecutando para lograr la recuperación de la pérdida con la finalidad de registrar la recuperación o la provisión del evento de pérdida.

El monto de recuperación o provisión es registrado en la matriz de eventos de pérdida, además de ser comunicado al área contable para que ejecute el registro correspondiente.

XV. CAMBIOS SIGNIFICATIVOS

15.1. Identificación de cambios significativos

Los dueños de procesos deben informar oportunamente a la Oficina de Planeamiento y Mejora Continua los cambios significativos previstos o producidos que puedan afectar la situación financiera de AMSAC, el cumplimiento de sus objetivos o su perfil de riesgos (apetito), sin perjuicio de la revisión anual de dichos cambios. Los cambios significativos pueden incluir, entre otros, lo siguiente:

a. Cambios en las operaciones que se originen como consecuencia de modificaciones normativas significativas, financiamiento de proyectos y/o nuevos encargos.
b. Alianzas o contratos asociativos o en participación con otras entidades o convenios interinstitucionales, que impliquen el desarrollo conjunto de proyectos.
c. Proyectos o inversiones de envergadura mayor a 5,500 UIT.

d. Cambios significativos en la infraestructura tecnológica o sistemas informáticos
e. Subcontrataciones significativas.

Antes de la aprobación e implementación de cambios significativos, se deberá evaluar su impacto en el apetito y tolerancia de riesgos y en los controles vigentes, determinando, de corresponder, las medidas necesarias para gestionar los riesgos identificados.

15.2. Evaluación de cambios significativos

El Responsable designado de la GIR evalúa el informe de identificación de cambios significativos y coordina con los dueños de procesos la definición de los controles y/o planes de acción, cuando corresponda.

XVI. DESEMPEÑO DE LA GESTIÓN INTEGRAL DE RIESGOS (GIR)

Trimestralmente, el Responsable designado de la GIR revisa con los dueños de proceso el avance en la ejecución del Plan de la GIR, conforme al nivel de criticidad y perfil de riesgo adoptado.

Semestralmente, el Responsable designado de la GIR envía el informe ejecutivo que contiene el avance de la GIR, matriz de riesgos y controles, matriz de oportunidades y cumplimiento de los planes de acción al Gerente General para su revisión. El informe ejecutivo se debe remitir a FONAFE, en la fecha indicada en la Directiva Corporativa de Gestión Empresarial.

A su vez, producto de la evaluación anual de la GIR, se establece un Plan de fortalecimiento en función del nivel de madurez de la GIR que se desea alcanzar, en función a dicho plan se desarrolla la estrategia de implementación en sus principales procesos.

XVII. ANEXOS

- Formato E2.3.M1.F1 Cambios Significativos
- Formato E2.3.M1.F2 Matriz de Eventos de Pérdida
- Formato E3.1.M3.F2 Matriz de Riesgos de Seguridad de la Información para Activos