	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 1 de 32
	<b>Gestión Integral de Riesgos</b>	

## 1. INTRODUCCIÓN

Las empresas hoy en día, sin importar su origen o tamaño, enfrentan una serie de riesgos o amenazas que pueden afectar de forma directa o indirecta el desarrollo de sus actividades y el cumplimiento de sus objetivos. De allí, deviene la importancia de desarrollar un adecuado sistema de gestión de riesgos que le permita actuar de manera eficaz ante potenciales impactos y oportunidades que surgen del entorno interno y externo de la organización.

El presente documento contiene los lineamientos y criterios que orientarán el desarrollo de la Gestión Integral de Riesgos de SEDAPAL, tomando como referencia las mejores prácticas de los modelos de gestión de riesgos y normativa vigente que se encuentran descritas en el presente manual.

## 2. OBJETIVO


Establecer una guía metodológica para la implementación de la Gestión Integral de Riesgos de SEDAPAL, que facilite las actividades de gestión de riesgos que enfrenta y al cual es expuesta la empresa, proporcionando lineamientos, técnicas y herramientas, que permitan identificar, analizar, evaluar, y dar respuesta a los riesgos, con la finalidad de contribuir al fortalecimiento del gobierno corporativo de la empresa.

## 3. ALCANCE

Es de aplicación a todos los procesos y actividades de SEDAPAL.

## 4. DOCUMENTOS A CONSULTAR


- 4.1 Directiva Corporativa de Gestión Empresarial de FONAFE aprobada mediante Acuerdo de Directorio N° 003-2018/006-FONAFE y sus modificatorias.
- 4.2 Lineamiento Corporativo: Lineamiento de Gestión Integral de Riesgos.
- 4.3 Manual Corporativo: Guía para la Gestión Integral de Riesgos.
- 4.4 Manual para el Desarrollo de la Gestión por Procesos de Sedapal.
- 4.5 Manual de Organización y Responsabilidades General (MORG) de SEDAPAL.
- 4.6 Mapa de Procesos de SEDAPAL (niveles 0 y 1), aprobado con Acuerdo de Directorio.
- 4.7 Marco Integrado de Gestión de Riesgos 2017 - COSO ERM: Integrando la estrategia y el desempeño.
- 4.8 Plan Estratégico Institucional de SEDAPAL.
- 4.9 Resolución de Contraloría General N° 320-2006-CG que aprueba las Normas de Control Interno.
- 4.10 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 de 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.
- 4.11 Resolución de Secretaría de Integridad Pública N° 001-2023-PCM/SIP, que aprueba la "Guía para la gestión de riesgos que afectan la integridad pública".
- 4.12 Norma ISO 31001 – Gestión del Riesgo – Directrices.
- 4.13 Norma ISO 37001 – Sistema de Gestión Anti Soborno.
- 4.15 Norma ISO 9001 – Sistema de Gestión de Calidad.
- 4.16 Norma ISO 14001 – Sistema de Gestión Ambiental.
- 4.17 Norma ISO 45001 – Sistema de Gestión de la Seguridad y Salud en el Trabajo.
- 4.18 Norma NTP-ISO/IEC 17020 – Evaluación de la Conformidad. Requisitos para el funcionamiento de diferentes tipos de organismos que realizan la inspección.
- 4.19 Directriz para la aplicación de la norma NTP-ISO/IEC 17020 para Organismos de Inspección.
- 4.20 Norma NTP-ISO/IEC 17025 – Requisitos generales para la competencia de los laboratorios de ensayo y calibración.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 2 de 32
	<b>Gestión Integral de Riesgos</b>	

- 4.21** Resolución N° 001-2023-PCM/SIP, Guía para la gestión de riesgos que afectan la integridad pública.
- 4.22** Resolución SMV N° 006-2021-SMV-01, Lineamientos para la Implementación y Funcionamiento del Modelo de Prevención.

## 5. DEFINICIONES

- 5.1 Actividad de laboratorio:** Ensayo y/o muestreo, asociado con el subsiguiente ensayo.
- 5.2 Análisis del riesgo:** Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- 5.3 Apetito:** Es el nivel de riesgo que la Empresa decide asumir durante el proceso de consecución de objetivos. La determinación de este punto permite controlar y mantener los riesgos en los niveles deseados.
- 5.4 Autoevaluación:** Evaluación que tiene como fin conseguir el entendimiento de los procesos y/o procedimientos realizados, así como la identificación de los riesgos asociados a los mismos.
- 5.5 Cambios Significativos:** Es todo aquel cambio importante definido por la Empresa, que se produce cuando se elimina o modifica o crea nuevos procesos, operaciones, productos, servicios, sistemas informáticos, planes de negocio, inversiones, proyectos, reorganizaciones societarias y en general cualquier cambio importante que pueda afectar significativamente el perfil del riesgo de la Empresa o afectaría financieramente o afectar el logro de objetivos.
- 5.6 Capacidad:** Es el nivel máximo de riesgo que la empresa puede soportar en la persecución de sus objetivos.
- 5.7 Comité de evaluación de riesgos NTP ISO/IEC 17020:** Grupo conformado por el responsable del área que interviene en el proceso bajo evaluación y por lo menos un colaborador de la misma (de ser aplicable).
- 5.8 Conflicto de interés:** Situación en la que el juicio del individuo, concerniente a su interés primario, y la integridad de una acción tienden a estar debidamente influidos por un interés secundario, de tipo generalmente económico o personal.
- 5.9 Confidencial:** Que se hace o se dice en confianza o con seguridad recíproca entre dos a más personas.
- 5.10 Control:** Es una actividad que tiene como finalidad reducir la criticidad de un riesgo. Debe contar con un responsable designado para su ejecución, seguir una frecuencia determinada y dejar constancia de que se realizó la actividad de control.
- 5.11 Continuidad Operativa o de negocio:** capacidad de la empresa para enfrentar un riesgo interno o externo que pueda interrumpir el brindar los productos y/o servicios.
- 5.12 Directorio:** Es el órgano colegiado a cargo de la dirección de la empresa.
- 5.13 Dueño del proceso:** Persona formalmente identificada para asumir la responsabilidad global de un proceso y, por lo tanto, cuanta con las atribuciones y el poder de decisión necesario como para garantizar que el proceso sea efectivo.
- 5.14 Eficacia:** La verificación de la eficacia consiste en la evaluación de los procedimientos del control o plan de acción con la finalidad de comprobar si son coherentes y permiten conseguir los objetivos en función de lo establecido en las normativas correspondientes.
- 5.15 Estrategia de riesgo:** Es el tratamiento que se le brinda a un riesgo y tiene como propósito mantener el nivel de criticidad dentro de los niveles aceptados por la Empresa.
- 5.16 Evaluación del riesgo:** Proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel del riesgo respecto de los estándares predeterminados, niveles de riesgo objetivo u otro criterio.
- 5.17 Evaluación de la conformidad:** Demostración de que se cumplen los requisitos especificados relativos a un producto, proceso, sistema, persona u organismo.
- 5.18 Evento:** Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por una misma causa, que ocurren durante el mismo período de tiempo.


	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 3 de 32
	<b>Gestión Integral de Riesgos</b>	

- 5.19 Exposición del riesgo:** Medida que representan el grado de posibilidad de ocurrencia de un evento negativo o adverso, así como el impacto del mismo en la Empresa al momento de materializarse.
- 5.20 Gestión Integral de Riesgos:** Proceso de identificación, medición, control, monitoreo, evaluación, retroalimentación y optimización de todas las situaciones que representan riesgos para empresa, así como la identificación, evaluación y tratamiento de oportunidades.
- 5.21 Gobierno Corporativo:** Es el conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la empresa, como son los tres poderes dentro de una sociedad: Los accionistas, Directorio y Alta Administración.
- 5.22 Indicadores de riesgo:** Métricas usadas para obtener señales tempranas sobre la exposición creciente de los riesgos a las que estén expuestas las diversas áreas de la Empresa.
- 5.23 Integridad Pública:** La integridad pública es la actuación coherente con valores, principios y normas, que promueve y protege el desempeño ético de la función pública, de modo que los poderes y recursos confiados al Estado se dispongan hacia los fines que se destinaron, asegurando que el servicio público a la ciudadanía esté orientado al interés general y a la generación de valor público.
- 5.24 Impacto:** Se define como el nivel o grado de exposición ante la posibilidad de materialización de un riesgo.
- 5.25 Imparcialidad:** Presencia de objetividad<sup>1</sup>.
- 5.26 Mapa de Riesgos:** Gráfico que ilustra el impacto y la probabilidad de ocurrencia de los riesgos.
- 5.27 Nivel de entidad:** Nivel donde las actividades son ejecutadas por el Gerente General o Gerente de Línea.
- 5.28 Nivel de procesos:** Nivel donde las actividades son ejecutadas por los dueños de procesos y su personal clave.
- 5.29 Nivel de Riesgo:** Grado de exposición al riesgo, expresado en términos del producto de la probabilidad e impacto.
- 5.30 Parte Interesada:** Conjunto de personas naturales y /o jurídicas que por sus características comunes pueden verse significativamente afectados; o afectar positivamente o negativamente en el desarrollo de las actividades de cada organización u organización.
- 5.31 Personal clave:** Personal de la empresa que forma parte del proceso.
- 5.32 Plan de acción:** Conjunto de acciones enfocadas en abordar el riesgo u oportunidad.
- 5.33 Probabilidad:** Nivel de posibilidad de que ocurra el evento de riesgo en un período determinado.
- 5.34 Proceso:** Es el conjunto de actividades relacionadas de manera lógica que, cuando se llevan a cabo utilizan los recursos de la organización para lograr resultados específicos transformando elementos de entrada en elementos de salida (por ejemplo, un producto o servicio).
- 5.35 Riesgo:** Incertidumbre o condición en que existe la posibilidad de que un evento ocurra o impacte negativamente sobre los objetivos de la Empresa<sup>2</sup>.
- 5.36 Riesgo inherente o inicial:** Aquel riesgo en su forma natural sin el efecto mitigante de los controles.
- 5.37 Riesgo residual:** Riesgo remanente después de los controles y/o tratamiento del riesgo.
- 5.38 Tolerancia:** Desviación del nivel del riesgo que la empresa quiere aceptar.
- 5.39 Tratamiento de riesgos:** Proceso de selección y puesta en aplicación de medidas para gestionar el riesgo.

1 NOTA 1: Objetividad significa que no existen conflictos de intereses o que se han resuelto a fin de no influir negativamente en las actividades posteriores del organismo de inspección.

NOTA 2: Otros términos que son útiles para transmitir el elemento imparcialidad son: independencia, ausencia de conflictos de intereses, ausencia de sesgos, ausencia de prejuicios, neutralidad, equidad, actitud abierta, ecuanimidad, desapego, equilibrio.

2 NOTA: Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 4 de 32
	<b>Gestión Integral de Riesgos</b>	

## 6. DISPOSICIONES GENERALES

### 6.1 Enfoque para la Implementación de la Gestión Integral de Riesgos

El enfoque para la implementación de la Gestión Integral de Riesgos recoge el modelo COSO ERM 2017 (*Risk Management—Integrating with Strategy and Performance*), el cual consta de cinco componentes que se detallan a continuación, y sobre el cual la empresa toma como referencia para su implementación, así como para la evaluación del desempeño de la Gestión Integral de Riesgos, que se realiza anualmente.

**Gráfico N° 01** Componentes del Modelo de Gestión Integral de Riesgos



**Fuente:** COSO ERM 2017.


### 6.2 Objetivos de la Gestión Integral de Riesgos

Se tiene como objetivos de la Gestión Integral de Riesgos, los siguientes:

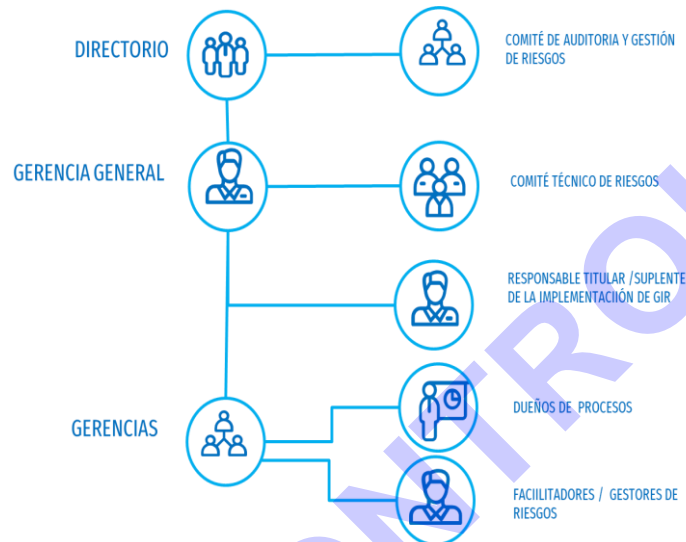
- Estandarizar las definiciones y criterios para el proceso de gestión de riesgos, y facilitar la toma de decisiones.
- Generar valor para los Grupos de Interés.
- Administrar los eventos futuros que crean incertidumbre.
- Responder adecuadamente ante los eventos producidos, para reducir pérdidas inesperadas.
- Transformar datos de riesgos en información y conocimiento para la toma de decisiones.
- Lograr la confiabilidad en la información generada por SEDAPAL, incluyendo reportes e informes tanto internos como externos.
- Cuidar y resguardar los recursos y bienes del Estado contra cualquier forma de pérdida, deterioro, uso indebido y actos ilegales, así como contra todo hecho irregular o situación perjudicial que pudiera afectarlos.
- Contribuir al desempeño del sistema de gestión.
- Fomentar e impulsar la práctica de valores institucionales y generar una cultura de riesgos a través de todo SEDAPAL.

### 6.3 Estructura Organizacional de la Gestión Integral de Riesgos

La estructura Organizacional de la Gestión Integral de Riesgos, representa la forma de asegurar el correcto funcionamiento de los componentes de la Gestión Integral de Riesgos a lo largo del tiempo, a través de la asignación de un esquema de responsabilidades consistentes con las características de SEDAPAL, siendo fundamental establecer claramente el involucramiento y la responsabilidad de todos los trabajadores en la gestión del riesgo. El siguiente gráfico detalla la estructura de gobierno y responsabilidades para la Gestión Integral de Riesgos:

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 5 de 32
	<b>Gestión Integral de Riesgos</b>	

**Gráfico N° 02** Estructura Organizacional para la Gestión Integral de Riesgos



## 6.4 Responsabilidades de la Gestión Integral de Riesgos

### 6.4.1 Directorio

Es la máxima autoridad jerárquica, de carácter colegiado y, como tal es el principal responsable evaluar las políticas de seguimiento, control y manejo de riesgos.

#### 6.4.1.1 Responsabilidades


- Establecer y asegurar una efectiva GIR.
- Impulsar la toma de decisiones de la GIR de la Empresa.
- Conformar el Comité de Auditoría y Gestión de Riesgos.
- Supervisar el adecuado funcionamiento de la GIR directamente y/o a través del Comité de Auditoría y Gestión de Riesgos o el que haga sus veces.
- Aprobar la política de riesgos, incluyendo los niveles de apetito y tolerancia de riesgos.
- Aprobar el plan de Gestión Integral de Riesgos y monitorear su ejecución.

### 6.4.2 Comité de Auditoría y Gestión de Riesgos

El Comité de Auditoría y Gestión de Riesgos o el que haga sus veces, debe asistir al Directorio en sus funciones de supervisión por medio de la revisión de los procesos contables, de auditoría, del Sistema de Control Interno y de la Gestión Integral de Riesgos.

#### 6.4.2.1 Responsabilidades

- Impulsar y supervisar la toma de decisiones y la ejecución de la estrategia de la GIR de la Empresa.
- Generar y liderar la cultura basada en riesgos.
- Proponer a Directorio la política de riesgos, incluyendo los niveles de apetito y tolerancia de riesgos.
- Proponer a Directorio el Plan de la Gestión Integral de Riesgos y monitorear su ejecución,
- Monitorear la evolución de la criticidad de los riesgos plasmada en el mapa de riesgos, y evaluar el progreso de las estrategias, así como recomendarlas de darse el caso.
- Velar por el alineamiento entre los objetivos y actividades de la GIR con el plan estratégico de la Empresa.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 6 de 32
	<b>Gestión Integral de Riesgos</b>	

- g. Evaluar anualmente el desarrollo de la GIR de la Empresa y el desempeño del personal involucrado, y presentar los resultados a FONAFE de acuerdo a lo estipulado en la Directiva Corporativa de Gestión Empresarial de FONAFE.
- h. Tomar conocimiento y evaluar el impacto a nivel de entidad de los eventos de pérdida, así como, de ser el caso, tomar las acciones que consideren necesarias.
- i. Asistir a Directorio en sus funciones de supervisión por medio de la revisión de los procesos contables, de auditoría, del sistema de control interno y de la GIR.
- j. Contar con un reglamento que regule políticas y procedimientos necesarios para el cumplimiento de las funciones del comité.

#### **6.4.3 Comité Técnico de Riesgos**

El Comité Técnico de Riesgos es el encargado de poner en marcha las acciones necesarias para la adecuada implementación de la GIR y su eficaz funcionamiento, a través de la mejora continua en la Empresa.

##### **6.4.3.1 Responsabilidades Generales**


- a. Proponer la política de la GIR y presentarla al Comité de Auditoría y Gestión de Riesgos para su posterior presentación a Directorio para aprobación.
- b. Proponer plan para la GIR al Comité de Auditoría y Gestión de Riesgos, para su posterior presentación a Directorio para aprobación.
- c. Proponer, revisar la metodología de riesgos.
- d. Gestionar la asignación del personal y recursos necesarios para la implementación de la GIR.
- e. Promover el cumplimiento rol del dueño del proceso.
- f. Aprobar la información de la GIR que la Empresa publique o comparta con entidades externas.
- g. Asegurar que se incluyan las capacitaciones de la GIR en el plan anual de capacitaciones de la empresa.
- h. Promover la cultura basada en riesgos de la empresa.
- i. Apoyar en el proceso de evaluación de la GIR alcanzando de manera oportuna los resultados e información requeridos relacionados a la misma.
- j. Recomendar acciones de mejora para la eficiencia y eficacia de la GIR.

##### **6.4.3.2 Responsabilidades específicas en relación a los riesgos.**

- a. Proponer el apetito, tolerancia y capacidad del riesgo.
- b. Gestionar riesgos claves de empresa según lo definido en el apetito y tolerancia al riesgo.
- c. Monitorear la evolución de la criticidad de los riesgos plasmada en el mapa de riesgos, y evaluar el progreso de las estrategias.
- d. Alertar sobre nuevos riesgos.
- e. Aprobar criterios y técnica para la evaluación de riesgos.
- f. Dar visto bueno a las matrices de riesgos y controles, los cronogramas de implementación de estrategias de respuesta al riesgo, las matrices de evaluación de controles, los KRI'S, y demás mecanismos de seguimiento.
- g. Aprobar el plan de acción propuesto por los responsables titulares / suplentes de la GIR para la implementación y fortalecimiento de la GIR.
- h. Establecer las estrategias que ayuden a la empresa a mitigar los riesgos a los que se encuentra expuesta, proponiendo medidas de control que contribuyan al logro de los objetivos de la Empresa.

##### **6.4.4 Gerente General**

- a. Máximo responsable en dirigir la implementación de la GIR de acuerdo con las normativas aprobadas por el Directorio, velando por su adecuado seguimiento y cumplimiento al interior de la Empresa.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 7 de 32
	<b>Gestión Integral de Riesgos</b>	

- b. La puesta en práctica de las políticas y medidas acordadas por el Directorio relacionadas a la GIR.
- c. La conducción y evaluación del funcionamiento del Comité Técnico de Riesgos.
- d. La supervisión del fortalecimiento de la cultura de la GIR dentro de la Empresa.
- e. Proporciona liderazgo y organiza la función de la GIR.

#### **6.4.5 Órganos gerenciales**

- a. Cuidar y velar la corrección, rendimiento y resultados de los procesos, actividades y operaciones que se realizan bajo su ámbito de competencia.
- b. Ser diligentes en la adopción de las medidas necesarias ante cualquier evidencia de desviación de los objetivos y metas programadas, detección de irregularidades, o de actuaciones contrarias a los principios de legalidad, economía, eficiencia y / o eficacia.
- c. Asegurarse de la contribución de controles de riesgos al logro de los resultados de la gestión.
- d. Realizar el seguimiento de las oportunidades aplicables a su gerencia.
- e. Supervisar el fortalecimiento de la cultura de la GIR de su gerencia, de su personal a cargo, desarrollando actividades de fortalecimiento de la cultura GIR, evaluando el desempeño de su personal a cargo frente a las actividades de capacitación y sensibilización de su personal.
- f. Atender las consultas y verificar la implementación de las recomendaciones formuladas por los órganos encargados de la GIR.
- g. Determinar las medidas correctivas y preventivas por los eventos de pérdida identificados.

#### **6.4.6 Responsable titular / suplente**

##### **6.4.6.1 Responsabilidades Generales**

- a. Brindar soporte al Comité Técnico de Riesgos en la elaboración del plan para la GIR y en su ejecución.
- b. Apoyar en la elaboración de la política de la GIR.
- c. Brindar soporte en la aplicación del Manual de Gestión Integral de Riesgos.
- d. Apoyar en la elaboración de la información de la GIR que la empresa publique, difunda o comparta con las entidades externas.
- e. Brindar soporte en las actividades de capacitación en la GIR.
- f. Brindar soporte al Comité Técnico de Riesgos en el reporte de resultados y entrega de información requeridos de la GIR.

##### **6.4.6.2 Responsabilidades específicas en relación al riesgo.**


- a. Apoyar en la definición del apetito, tolerancia y capacidad al riesgo.
- b. Brindar soporte en las actividades de evaluación de riesgos al dueño de proceso.
- c. Mantener actualizada la matriz de riesgos y reportar su estado al Comité Técnico de Riesgos.
- d. Apoyar la identificación de estrategias de respuesta al riesgo y definición de planes de acción.
- e. Coordinar con el dueño del proceso la implementación del plan de acción y monitorear su cumplimiento.
- f. Apoyar en la evaluación e informe de los cambios significativos.

#### **6.4.7 Dueño de Proceso**

El dueño del proceso es quien está a cargo de los procesos de la Empresa, y son responsables de los riesgos y oportunidades que estos implican.

##### **6.4.7.1 Responsabilidades generales**

- a. Implementar la cultura de GIR en los procesos bajo su responsabilidad.
- b. Asegurar la aplicación del presente manual en los procesos bajo su responsabilidad.
- c. Apoyar al responsable titular / suplente de la GIR en el desarrollo de las actividades contenidas en el plan de la GIR donde corresponda.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 8 de 32
	<b>Gestión Integral de Riesgos</b>	

- d. Apoyar al Comité Técnico de Riesgos con la información requerida para la evaluación de la GIR.
- e. Reportar oportunamente la información de la GIR al responsable titular / suplente.

#### **6.4.7.2 Responsabilidades específicas en relación a riesgos**

- a. Definir la tolerancia al riesgo en coordinación con el responsable titular / suplente de la GIR.
- b. Comunicar los cambios en sus procesos y los riesgos asociados al responsable titular / suplente de la GIR.
- c. Velar por la efectividad de los controles asociados a los riesgos de sus procesos.

#### **6.4.8 Gestores de Riesgos**

- a. Personal designado por equipo que brindan apoyo técnico (según metodología) en el proceso de identificación, evaluación y tratamiento del riesgo de los procesos al cual pertenecen; así como también, a los Sistemas de Gestión implementados actualmente en la empresa.

Para el caso del Comité de Seguridad y Salud en el Trabajo. A través del equipo de seguridad e higiene ocupacional (ESHO), el comité SST toma conocimiento en la identificación, evaluación de riesgos, determinación de control que el Equipo Seguridad e Higiene Ocupacional, determinada para el Sistema de Gestión de Seguridad y Salud en el Trabajo.

#### **6.4.9 Responsabilidades específicas:**

Respecto a la NTP ISO/IEC 17020 y NTP ISO/IEC 17025 cuentan con coordinadores de calidad para la gestión de riesgos.

### **6.5 Relación de la Gestión Integral de Riesgos con los sistemas de gestión implementados en la empresa.**

#### **6.5.1 Sistema de Gestión de la Calidad (ISO 9001)**

Los riesgos asociados al sistema de gestión de calidad se gestionan considerando las disposiciones contenidas en el presente manual.

#### **6.5.2 Sistema de Gestión Ambiental (ISO 14001)**

Los riesgos asociados al sistema de gestión de Gestión Ambiental se gestionan considerando las disposiciones contenidas en el presente manual, y también otras normativas vinculadas a su naturaleza.

#### **6.5.3 Sistema de Gestión de Seguridad y Salud en el Trabajo (ISO 45001)**

Los riesgos asociados al sistema de gestión de Seguridad y Salud en el Trabajo se gestionan considerando las disposiciones contenidas en el presente manual, y también otras normativas vinculadas a su naturaleza.

#### **6.5.4 Sistema de Gestión NTP ISO/IEC 17020 - Evaluación de la Conformidad**

Los riesgos asociados a las actividades de Inspección se gestionan considerando las disposiciones contenidas en el presente manual. La aplicabilidad del mismo se describe en el numeral 6.6.


#### **6.5.5 Sistema de Gestión ISO 17025 - Laboratorios de ensayo y de calibración**

Los riesgos asociados a las actividades de laboratorios de ensayo y calibración se gestionan considerando las disposiciones contenidas en el presente manual.

#### **6.5.6 Sistema de Gestión de riesgos que afectan la integridad**

La gestión de riesgos asociados a los riesgos que afectan la integridad, se gestiona con su propia normativa específica (Resolución N° 001-2023-PCM/SIP, Guía para la gestión de riesgos



	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 9 de 32
	<b>Gestión Integral de Riesgos</b>	

que afectan la integridad pública y Resolución SMV N° 006-2021-SMV-01, Lineamientos para la Implementación y Funcionamiento del Modelo de Prevención).

Este sistema incluye el soborno, lavado de activos, financiamiento del terrorismo, corrupción, conducta funcional antiética, y fraude en cualquiera de sus modalidades.

#### **6.5.7 Sistema de Gestión de Riesgos de Seguridad e Información**

La gestión de riesgos asociados a los riesgos que afectan a la seguridad de la información, se gestiona con sus lineamientos específicos establecidos en el SGSIPR0001 Procedimiento Metodología de Evaluación de Riesgos de Seguridad de la Información.

#### **6.5.8 Gestión de Riesgos de otros sistemas de gestión**

El manejo de riesgos de otros sistemas de gestión no establecidos en el presente manual se gestionan de acuerdo a su propia normativa específica.

Para el caso del proceso de producción y distribución del producto agua potable, y vinculados se aplica la "Metodología para el Análisis de Evaluación de los Riesgos" establecida en la "Directiva Sanitaria para la formulación, aprobación y aplicación del plan de control de calidad (PCC) por los proveedores de agua para consumo humano". Para los procesos asociados a la producción y distribución del producto agua potable cumplen con la metodología establecida del presente Manual.

### **6.6. Gestión de riesgos para la NTP ISO/IEC 17020**


#### **6.6.1 Disposiciones generales de la Gestión de riesgos para la NTP ISO/IEC 17020**

- a) El personal del Organismo de Inspección de Medidores de agua potable realiza las actividades de inspección con imparcialidad, para lo cual en señal de conformidad firma el GCFO132 Formulario Declaración Jurada de Protección de la Imparcialidad, Independencia y confidencialidad, que indica que el personal está libre de cualquier presión comercial, financiera interna y externa indebida y de otras presiones que pudieran afectar adversamente la calidad e imparcialidad de su trabajo; asimismo, se asegura la independencia del personal, precisándose que las actividades de la estructura organizacional del Organismo de Inspección son realizadas por distintas personas, para tal efecto en los procedimientos se establecen las responsabilidades de cada integrante del Organismo de Inspección. La renovación del GCFO132 es anualmente.
- b) Identifica de manera continua su imparcialidad, la cual incluye los riesgos derivados de las actividades de inspección y/o de las relaciones del personal. La revisión de la DGMMR0038 Matriz de Riesgos y Controles se realiza como mínimo una vez por año o cuando se identifiquen nuevas oportunidades o situaciones de riesgo que afecten la imparcialidad y/o el sistema integrado de gestión, dicha revisión y/o actualización la dirige la Coordinadora de ISO/IEC 17020 (CC-EGCM), para lo cual se convoca al Comité de evaluación de riesgos para revisar si la DGMMR0038 Matriz de Riesgos y Controles, la cual refleja el estado actual de los riesgos a la imparcialidad de modo efectivo.
- c) Las acciones de control pueden ser modificadas en función a la efectividad de las mismas.

### **7. DISPOSICIONES ESPECÍFICAS**

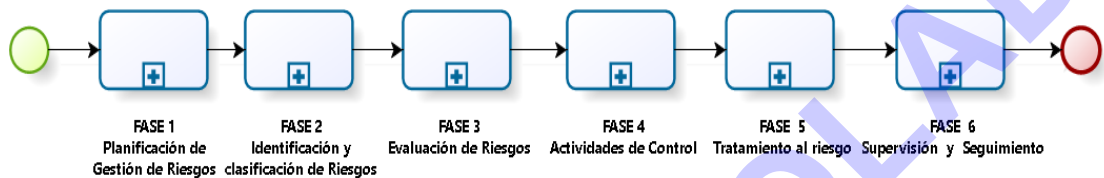
#### **7.1 Metodología para la Gestión Integral de Riesgos**

La metodología está basada en el marco del COSO-ERM (Committee of Sponsoring Organizations Enterprise Risk Management), la cual ha sido complementada y adecuada a las características propias de SEDAPAL, presentando seis fases: i) Planificación, ii) Identificación y clasificación,

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 10 de 32
	<b>Gestión Integral de Riesgos</b>	

iii) Evaluación, iv) Actividades de Control, v) Tratamiento al riesgo y vi) Supervisión y Seguimiento, tal como se muestran en el siguiente gráfico:

**Gráfico N° 03 Fases de la Gestión Integral de Riesgos**



### 7.1.1 Fase 1: Planificación de la Gestión de Riesgos

La planificación es la fase inicial en el desarrollo de la gestión de riesgos de SEDAPAL y es fundamental para que las actividades sean implementadas de manera eficiente, oportuna y alineadas a sus necesidades. Para un mejor desarrollo y control de la metodología, esta fase está sub dividida en cuatro etapas claramente definidas, que se pasan a desarrollar:

a. Etapa 1- Mapeo de Procesos

El mapeo de los procesos es fundamental para lograr un mayor entendimiento del negocio y sus operaciones, identificar los riesgos, e implementar y monitorear los controles de una manera más eficiente. Los procesos existentes deben agruparse en las siguientes categorías: i) Estratégicos, ii) Misionales y iii) De soporte. La metodología a usar en esta etapa se encuentra descritas en el DGMMMA002 Manual para el Desarrollo de la Gestión Por Procesos.

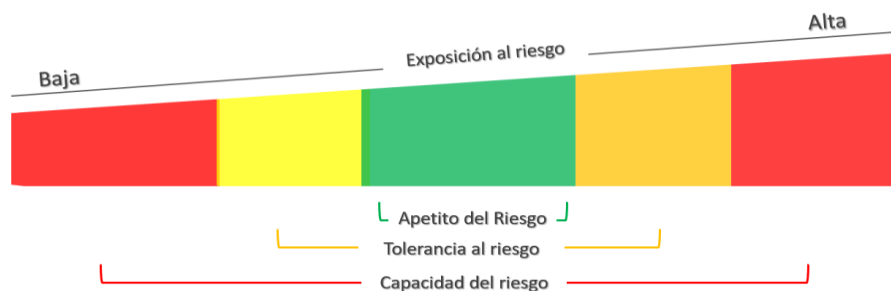
b. Etapa 2- Definición de Objetivos

Los objetivos están alineados a la Misión y Visión de SEDAPAL, y son comunicados a todo el personal. La gestión de riesgos se orienta en función a los objetivos definidos a nivel entidad y por procesos, por lo cual es una condición imprescindible tenerlos claramente identificados. Los objetivos a nivel de la empresa se encuentran definidos en el Plan Estratégico Institucional y los objetivos de los procesos están definidos en las fichas de los procesos.


c. Etapa 3- Definición del apetito, tolerancia y capacidad al riesgo

El proceso de definición del apetito de riesgo se basa en un enfoque de arriba hacia abajo también conocido como Modelo Top-down, el cual consiste en establecer el apetito de riesgo desde la Alta Dirección, alineándose con los objetivos a nivel Empresa y comunicarlo a todo el personal de SEDAPAL, alineando la gestión de riesgos a éste.

**Gráfico N° 04 Apetito al riesgo**



Fuente: Definición e Implantación del Apetito de Riesgo (Instituto de Auditores Internos de España)

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 11 de 32
	<b>Gestión Integral de Riesgos</b>	

El apetito de riesgo es el nivel de riesgo que SEDAPAL decide aceptar, aquel con el que se siente cómoda; la tolerancia será la desviación respecto a este nivel. Por otro lado, la capacidad de asumir riesgos es el nivel máximo de riesgo que SEDAPAL puede soportar en la persecución de sus objetivos, sin condicionar su sostenibilidad. Así, la tolerancia sirve como alerta para evitar que SEDAPAL llegue al nivel establecido por su capacidad, algo que pondría en peligro la sostenibilidad y existencia del negocio.

El Directorio define los niveles de apetito, tolerancia y capacidad de riesgo a nivel Empresa, los cuales deben ser actualizados por lo menos una vez al año, de acuerdo a los objetivos y recursos, entre otras variables.

Los niveles de apetito, tolerancia y capacidad de riesgo deben ser propuestos por el Comité de Riesgos, en concordancia con las responsabilidades descritas en el presente Manual.

d. Etapa 4- Priorización y Selección de Procesos Críticos

La priorización de procesos permite identificar los procesos críticos de la Empresa y organizar la designación de esfuerzos de la gestión de riesgos en función a la criticidad de las operaciones. Se identifican con la metodología descrita en el manual DGMMMA002 Manual para el Desarrollo de la Gestión Por Procesos.

### 7.1.2 Fase 2.- Identificación y Clasificación de Riesgos

La identificación y clasificación de riesgos es fundamental para hacer frente a las situaciones que afecten el cumplimiento de los objetivos de la entidad y los procesos. La información se registra y documenta en el DGMFO0038 Formulario Matriz de Riesgos y Controles.

Esta fase está sub dividida en tres etapas: i) Identificación de eventos, ii) Identificación de riesgos y iii) Evaluación del Riesgo.

a. Etapa 1 – Identificación de eventos

Se entiende como evento a una situación o elemento potencial de origen externo o interno que afecte a la entidad, el cual puede tener consecuencias positivas o negativas.

Los eventos negativos son el punto de partida para poder identificar los riesgos que afronta SEDAPAL. Es importante mapearlos pues permite desarrollar una cultura de prevención en la gestión de riesgos.

Los eventos positivos son relevantes para tener conocimiento de aquellas oportunidades que deben ser aprovechadas por SEDAPAL pues contribuyen al cumplimiento de objetivos.

b. Etapa 2 – Identificación de Riesgos

Es el proceso en el que, entendiendo el contexto de la empresa, se identifican las amenazas que enfrenta SEDAPAL cuando un evento o situación puede afectar adversamente su habilidad de alcanzar sus objetivos y maximizar valor. (\*)

Según el DGMFO0038 Formulario Matriz de Riesgos y Controles, es importante identificar las entradas donde se originan los riesgos. Para ello se tendrá en cuenta el siguiente cuadro:

***Tabla N° 02 Procedencias y su descripción***

Procedencia del evento	Descripción de la Procedencia
FODA (Contexto de la organización).	Nombre de la amenaza y/o debilidad identificada. <u>Si es una amenaza se considera como factor externo y si es una debilidad como factor interno</u>
Partes Interesadas.	Nombre de la Parte Interesada.

Procedencia del evento	Descripción de la Procedencia
Auditorías (Resultados de auditorías internas o externas).	Tipo y Número de Auditoría
Aspectos Ambientales (ISO 14001).	Nombre del Aspecto Ambiental.
Requisitos Legales y otros requisitos (ISO 14001, ISO 45001).	Nombre del Requisito Legal y/u otro requisito.
Sistema de Gestión de Calidad SGC (ISO 9001)	Nombre del elemento del sistema de gestión de calidad
Sistema de Antisoborno SGAS (ISO 37001)	Nombre del elemento del sistema de gestión anti soborno
Sistema de gestión Ambiental SGA (ISO 14001)	Nombre del elemento del sistema de gestión ambiental
Sistema de gestión SST (ISO 45001)	Nombre del elemento del sistema de gestión SST
Riesgo SST	Nombre del Riesgo SST
<u>Actividades de laboratorio (ISO 17025)</u>	<u>Nombre de la actividad o de los procesos del laboratorio.</u>
<u>Actividades de laboratorio (ISO 17020)</u>	<u>Nombre de la actividad o de los procesos del Organismo de Inspección.</u>

- Luego de identificar la procedencia del evento, es necesario realizar la descripción del riesgo. (\*)
- Luego de la identificación se debe **documentar** los riesgos en DGMMR0038 Matriz de Riesgos y controles. Ver tabla N° 03 Tipos de riesgos y ejemplos de eventos.

**Factor de origen interno:**

Son elementos, características o comportamientos que puedan generar un riesgo y que se encuentran dentro de la gestión de la empresa, de los procesos y Equipos.


1. Estrategia (decisiones relacionadas a segmentación de clientes y mercados; diversificación actividades; inversiones; adquisiciones grandes etc.).
2. Organización (renovación de plantillas; cambios organizativos; fusiones y adquisiciones; gobierno corporativo; responsabilidad social corporativa).
3. Operativos (producción y distribución, actividades de laboratorio, investigación, desarrollo e innovación; capital intelectual; sistemas de información; gestión de residuos, sistema de gestión de SST).
4. Capital humano (cumplimiento legal, responsabilidad de directivos, seguridad laboral, infidelidad de empleados, productividad; retención del talento, etc).

**Factor de origen externo:**

Son elementos, características o comportamientos que puedan generar un riesgo y que se encuentran fuera de la gestión de la empresa, en el entorno externo.

1. Legales (legislación local, nacional e internacional).
2. Naturales/ambientales (cambio climático; contaminación; gestión de residuos).
3. Políticos.
4. Financieros (tipos de interés, tipos de cambio, políticas crediticias, fluctuaciones de precios).
5. Mercados (cambios de hábitos de consumo, etc.): Macroeconómicos, Demográficos (tasa de crecimiento de la población, etc.).


- Los tipos y eventos de riesgos, tienen el propósito de identificar el tipo de riesgo según los eventos que se presenten. Tomar como referencia el siguiente cuadro que se detalla a continuación:

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 13 de 32
	<b>Gestión Integral de Riesgos</b>	

*Tabla N° 03 Tipos de riesgos y ejemplos de eventos*

TIPO DE RIESGO		SUBTIPOS	EVENTOS DE RIESGO - EJEMPLOS
FINANCIEROS	CRÉDITO		<ul style="list-style-type: none"> <li>• Incumplimiento de pago</li> <li>• Cartera morosa</li> <li>• Incobrabilidad</li> </ul>
	MERCADO		<ul style="list-style-type: none"> <li>• Crisis internacional</li> <li>• Tasas de Interés</li> <li>• Tipo de Cambio</li> </ul>
	LIQUIDEZ		<ul style="list-style-type: none"> <li>• Restricciones presupuestarias</li> <li>• Descalce de activos y pasivos</li> <li>• Capital de Trabajo</li> </ul>
NO FINANCIEROS	ESTRATÉGICO		<ul style="list-style-type: none"> <li>• Inestabilidad política</li> <li>• Legislación y/o regulaciones</li> <li>• Inversión en la infraestructura</li> </ul>
	REPUTACIONAL		<ul style="list-style-type: none"> <li>• Opinión pública</li> <li>• Manejo de medios</li> <li>• Mala Imagen corporativa</li> </ul>
	OPERACIONAL	OPERACIONAL	<ul style="list-style-type: none"> <li>• Procesos inadecuados</li> <li>• Fallas de personal</li> <li>• Fallas u obsolescencia de equipos</li> <li>• Eventos externos (ejm: desabastecimiento de insumos)</li> </ul>
		CONTINUIDAD OPERATIVA	<ul style="list-style-type: none"> <li>• Humanos intencionados</li> <li>• Incumplimiento regulatorio</li> <li>• Industriales y ambientales</li> <li>• Naturales</li> <li>• Tecnológicos</li> </ul>
	SEGURIDAD DE INFORMACIÓN	<ul style="list-style-type: none"> <li>• Disponibilidad de datos y sistemas</li> <li>• Integridad de datos</li> <li>• Confidencialidad de la información</li> </ul>	

TIPO DE RIESGO		SUBTIPOS	EVENTOS DE RIESGO - EJEMPLOS
		FRAUDE Y CORRUPCIÓN	<p>Fraude:</p> <ul style="list-style-type: none"> <li>• Fraude documentario.</li> <li>• Fraude comercial.</li> <li>• Fraude informático.</li> <li>• <u>Fraude contractual.</u></li> <li>• <u>Proselitismo político.</u></li> <li>• <u>Lavado de Activos. y Financiamiento del Terrorismo.</u></li> <li>• <u>Inconducta Funcional</u></li> </ul> <p><u>Corrupción:</u></p> <ul style="list-style-type: none"> <li>• <u>Soborno (cohecho).</u></li> <li>• <u>Conflicto de Intereses.</u></li> <li>• <u>Colusión.</u></li> <li>• <u>Peculado de Uso.</u></li> <li>• <u>Otros delitos contra la administración y fe pública.</u></li> </ul>
		MEDIO AMBIENTE	<ul style="list-style-type: none"> <li>• Emisiones de gas</li> <li>• Emisión de residuos</li> <li>• Derrames</li> </ul>
		<u>IMPARCIALIDAD</u>	<ul style="list-style-type: none"> <li>• <u>Ausencia objetividad</u></li> <li>• <u>Conflictos de intereses</u></li> <li>• <u>Ausencia de sesgos</u></li> <li>• <u>Favoritismo</u></li> <li>• <u>Ausencia de Neutralidad</u></li> <li>• <u>Actitud interesada</u></li> </ul>
		PROYECTOS	<ul style="list-style-type: none"> <li>• Retrasos en el cumplimiento de plazos</li> <li>• Falta de recursos presupuestales</li> <li>• Falta de claridad en el alcance</li> <li>• Modificaciones en las operaciones</li> </ul>
		SEGURIDAD Y SALUD OCUPACIONAL	<ul style="list-style-type: none"> <li>• Estrés Laboral</li> <li>• Falta de ergonomía</li> <li>• Físicoquímicos</li> <li>• Peligros Locativos</li> <li>• Sistema de Gestión de SST (Seguimiento de objetivos, programa de auditoría, seguimiento de acciones, entre otros elementos que forman parte de la gestión de SST)</li> </ul>
		TECNOLOGÍAS DE LA INFORMACIÓN	<ul style="list-style-type: none"> <li>• Obsolescencia de Hardware y Software</li> <li>• Filtración de datos y fuentes de información</li> <li>• Vulneración de la seguridad de la información</li> </ul>

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 15 de 32
	<b>Gestión Integral de Riesgos</b>	

TIPO DE RIESGO		SUBTIPOS	EVENTOS DE RIESGO - EJEMPLOS
		CUMPLIMIENTO	<ul style="list-style-type: none"> <li>• Sanciones legales</li> <li>• <u>Compliance Laboral.</u></li> <li>• <u>Compliance Penal.</u></li> <li>• <u>Compliance Integridad Pública.</u></li> <li>• <u>Compliance Prevención del Lavado de Activos y el Financiamiento del Terrorismo.</u></li> <li>• <u>Derechos Humanos</u></li> <li>• Demandas (*)</li> </ul>

A efectos de identificar las exposiciones al riesgo de SEDAPAL, se aplican una o más técnicas que se encuentran descritas en el Anexo 1 del presente Manual. (\*)

- d) Etapa 3: Descripción del Riesgo:  
Se debe redactar el riesgo de la siguiente forma:

Evento + Consecuencia + Causa

La consecuencia está ligada al impacto y la causa a la probabilidad de ocurrencia.

### 7.1.3 Fase 3.- Evaluación de Riesgos

Luego de realizar la identificación de riesgos, éstos son evaluados para determinar la criticidad de los riesgos en base a su probabilidad de impacto, y definir un tratamiento adecuado, priorizando esfuerzos hacia los riesgos más críticos.


Los riesgos son evaluados en función a dos variables: Probabilidad (frecuencia de ocurrencia del riesgo, asociado a la causa) e impacto (severidad del riesgo o impacto económico, asociado a la consecuencia).

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

- **Riesgo Inherente:** es aquel riesgo sin efecto de mitigante de los controles.
- **Riesgo residual:** es aquel riesgo que permanece después de la implementación de los controles.

Debe entenderse que luego de la evaluación del riesgo inherente (sin efecto de los controles), corresponde determinar el riesgo residual, a través de la evaluación de los controles existentes.

- a. Etapa 1: Determinación de la Probabilidad: La probabilidad de ocurrencia es el grado de posibilidad de que ocurra un riesgo en un período. Puede ser estimada en función a cuántas veces históricamente el riesgo ha ocurrido, o qué posibilidad existe de que ocurra en el futuro.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 16 de 32
	<b>Gestión Integral de Riesgos</b>	

***Tabla N° 04 Determinación de la probabilidad***

V a l o r	NIVEL	PROBABILIDAD
1	Bajo	<ul style="list-style-type: none"> <li>- Probabilidad de ocurrencia baja, casi nula (raro) y/o</li> <li>- <u>No ha ocurrido hace 5 años o más.</u></li> </ul>
2	Medio	<ul style="list-style-type: none"> <li>- Probabilidad moderada, ocurrencia periódica y/o</li> <li>- <u>Eventos similares han ocurrido dentro de los últimos 3 a 5 años.</u></li> </ul>
3	Alto	<ul style="list-style-type: none"> <li>- Es muy probable ocurre con frecuencia y/o.</li> <li>- <u>Eventos similares han ocurrido entre 1 y menos de 3 años.</u></li> </ul>
4	Extremo	<ul style="list-style-type: none"> <li>- Probabilidad elevada, ocurre muchas veces y/o</li> <li>- <u>Eventos similares ya han ocurrido / ocurre con bastante frecuencia, 1 en menos de un año.</u></li> </ul>


Como parte del despliegue de la metodología, se aplica para la evaluación de riesgos, las variables (\*) de probabilidad señaladas anteriormente para todos los sistemas de gestión de riesgos, sin perjuicio de ello, en cada uno de estos se puede analizar la información histórica con el propósito de definir escalas cuantitativas de frecuencia que complementen.

b. Etapa 2: Determinación del Impacto o severidad: El impacto es el nivel de exposición de SEDAPAL ante un riesgo, puede ser cuantitativo como cualitativo, y puede medirse según los escenarios descritos en el siguiente cuadro.

- Cuantitativo: Aspecto financiero o económico.
- Cualitativo: Regulatorio, continuidad del negocio, reputacional, seguridad y salud ocupacional, Antisoborno, Fraude, Corrupción y Soborno, Lavado de Activos y Financiamiento del Terrorismo, seguridad de la información, medioambiente e imparcialidad.


Cabe precisar que cuando el riesgo presenta más de un impacto asociado, se aplica preferentemente aquel que corresponda al tipo de riesgo por su naturaleza, donde el impacto sea más relevante. Para el caso de los riesgos identificados de la ISO/IEC 17025, en el tipo de riesgo operacional considerar preferentemente el impacto a la continuidad de la operación.




	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 17 de 32
	<b>Gestión Integral de Riesgos</b>	

**Tabla N° 05 Determinación del Impacto**

Valor	Nivel	Financiero (*)	Regulatorio (Multas / Sanciones)	Continuidad Operativa	(*) Reputacional (Imagen)	Seguridad y Salud Ocupacional (SSO)	Seguridad de la Información	Medio Ambiente	Imparcialidad
<b>1</b>	<b>Bajo</b>	Potencial pérdida de utilidad operativa menor e igual S/. 21 Millones	No existe posibilidad de multa o sanción. La(s) actividad(es) afectada(s) no está(n) sujeta(s) a supervisión por parte de otra Organización.	<p>El impacto puede ser absorbido (asimilado) por las actividades normales del negocio en 1 hora. Los costos adicionales del impacto son mínimos</p> <p><u>No se ve afectado los objetivos estratégicos de la empresa y/o</u>  <u>No se ve afectado el desempeño de los procesos y/o</u>  <u>No hay afectación en la imagen o reputación y/o</u>  <u>Sin lesiones en el personal.</u></p>	La exposición de la imagen es únicamente interna y limitada.	No existe impacto negativo en la SSO del personal. Las partes interesadas no perciben que el riesgo es irrelevante. Se genera baja o nula influencia en el objetivo del Sistema de gestión SSO	Cuando la pérdida o falla de un determinado activo no impacta la rentabilidad, operatividad, el cumplimiento legal, imagen y las dimensiones de seguridad de la información de la empresa.	El impacto no es percibido o no sería percibido por la comunidad.	<p>No tiene potencial para provocar pérdidas al laboratorio o a sus clientes, no siendo las infracciones susceptibles de ser prácticas causadoras de daños relevantes en la imagen y la operabilidad del mismo.</p> <p><u>Si el evento llegara a presentarse, tendría un bajo impacto o efecto sobre algunas actividades del Organismo de Inspección.</u></p>
<b>2</b>	<b>Medio</b>	Potencial pérdida de utilidad operativa mayor a S/. 21 Millones pero menor o igual a S/. 42 Millones.	Posibilidad de multa o sanción.	El impacto afecta la productividad del negocio en un horizonte de 1 semana aproximadamente.	La exposición de la imagen es interna con potencial para trascender externamente.	Existe un leve impacto en la SSO de las partes interesadas, tanto que se encuentran directa e indirectamente relacionados con el evento. Las partes	Cuando la pérdida o falla de un determinado activo impacta seriamente, operatividad, el cumplimiento legal, imagen y las dimensiones de	El impacto afecta o afectaría únicamente a la Empresa, es percibido como importante por las partes	<p>Puede ocasionar pérdidas para el laboratorio y perturbar su normal funcionamiento.</p> <p><u>Si el evento llegara a presentarse, tendría</u></p>


	<b>MANUAL</b>	<b>Código : DGMMMA0004</b> <b>Versión : 09</b> <b>Aprobado : GG</b> <b>Fecha : 2024.08.27</b> <b>Página : 18 de 32</b>
	<b>Gestión Integral de Riesgos</b>	

				Personal podría ser necesario. <u>Podría afectar moderadamente los objetivos estratégicos de la empresa y/o</u> <u>Se interrumpe parcialmente el desempeño de los procesos y/o</u> <u>Afecta moderadamente la imagen o reputación y/o</u> <u>Lesiones leves en el personal.</u>		interesadas perciben moderadamente el riesgo. Se genera mediana influencia en el objetivo del sistema de gestión SSO	seguridad de la información de la empresa.	interesadas aisladas.	<u>un moderado impacto o efecto sobre los objetivos del Organismo de Inspección, o compromete varias actividades.</u>
3	Alto	Potencial pérdida de utilidad operativa mayor a S/. 42 Millones pero menor o igual a S/. 63 Millones	Posibilidad de multa o sanción por falta grave.	Impacto potencial en la continuidad del negocio, productividad; en un horizonte mayor a 1 mes. El costo de interrupción es alto.	La exposición de la imagen es interna y externa, presenta un potencial de impacto alto.	Impacto medio - alto en la SSO de las partes interesante que se encuentran directa e indirectamente relacionados con el evento. Impacto en las condiciones de trabajo.  Situación perceptible en toda la organización como importante. Se genera alta influencia en el objetivo del Sistema de gestión de SSO o evitará el logro del objetivo previsto de la organización.  El impacto del riesgo afecta al desempeño y sostenibilidad del	Cuando la pérdida o falla de un determinado activo impacta drásticamente la rentabilidad, operatividad, el cumplimiento legal, imagen y las dimensiones de seguridad de la información de la empresa.	El impacto se manifiesta o se manifestaría fuera de la Empresa. Es percibido por la comunidad como algo importante.	Puede ocasionar pérdidas significativas para el laboratorio y/o la violación grave de los principios asociados a los intereses de los clientes, debilitando la credibilidad del laboratorio.  <u>Si el evento llegara a presentarse, tendría un alto impacto, comprometiendo los objetivos del Organismo de Inspección o la continuidad de las operaciones o paralización de los procesos de soporte. Ocasiona rehacer los trabajos para volver a la situación</u>

	<b>MANUAL</b>	<b>Código : DGMMMA0004</b> <b>Versión : 09</b> <b>Aprobado : GG</b> <b>Fecha : 2024.08.27</b> <b>Página : 19 de 32</b>
	<b>Gestión Integral de Riesgos</b>	

						Sistema de gestión de SSO.		anterior y conlleva altos costos de recursos para reparar la situación.	
4	Extremo	Potencial pérdida de utilidad operativa mayor a S/. 63 Millones	Posibilidad de multa o sanción por falta muy grave, cierre de las instalaciones, entre otras.	<p>Interrupción total o significativa de las operaciones de la empresa. El costo de interrupción es muy alto.</p> <p><u>No se pueden cumplir con los objetivos estratégicos de la empresa y/o</u></p> <p><u>Se interrumpe en un tiempo considerable los procesos y/o</u></p> <p><u>Afecta severamente la imagen o reputación y/o</u></p> <p><u>Lesiones graves en el personal</u></p>	Exposición total de la imagen, mal manejo de situaciones de crisis, que podría tener un impacto negativo por tiempo prolongado.	<p>Alto impacto en la SSO de las partes interesadas, pérdida de personal, entre otros.</p> <p>Situación adversa percibible en toda la organización y partes interesadas. se genera queja de partes interesadas, reclamos, multas, denuncias, Cierre de la empresa.</p> <p>Se genera alta influencia en el objetivo del Sistema de gestión SSO o evitará el logro del objetivo previsto.</p> <p>El impacto del riesgo afecta al desempeño y sostenibilidad del Sistema de gestión de SSO.</p>	<p>Cuando la pérdida o falla de un determinado activo impacta irreversiblemente la rentabilidad, operatividad, el cumplimiento legal, imagen y las dimensiones de seguridad de la empresa.</p>	<p>El impacto sobrepasará el nivel de respuesta por parte de la empresa necesitando ayuda del gobierno.</p>	<p><u>Puede ocasionar la cancelación de la acreditación.</u></p> <p><u>Si el evento llegara a presentarse, tendría un trágico impacto, comprometiendo los objetivos del Organismo de Inspección o la continuidad de las operaciones por paralización de los principales procesos o la cancelación de la acreditación.</u></p>

Se precisa que, la medición del impacto cualitativo de Fraude, Corrupción y Soborno, Lavado de Activos y Financiamiento del Terrorismo, se realiza a través de la normativa específica pertinente.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 20 de 32
	<b>Gestión Integral de Riesgos</b>	

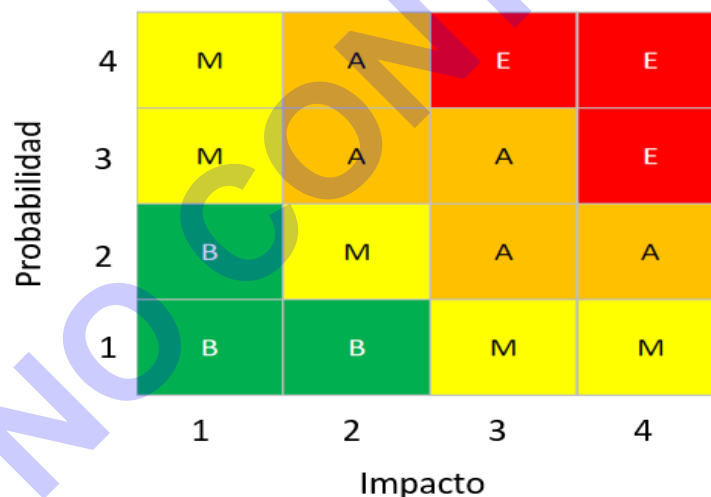
c. Etapa 3: Nivel de criticidad del riesgo

La criticidad de un riesgo es la medida que surge de la combinación de sus niveles de probabilidad e impacto. Dicho resultado ubica al riesgo en los niveles de riesgo, bajo, moderado, alto o extremo de acuerdo al mapa de calor de riesgos que se expone a continuación. La información es registrada en el formulario Matriz de riesgos y controles.

**Nivel de criticidad del riesgo:** Probabilidad x impacto

Según el valor de probabilidad e impacto, se ubica en el mapa de calor de riesgos a fin de definir la criticidad del riesgo y el tratamiento a seguir. Los niveles de riesgo se dan en base al producto entre "Probabilidad" e "Impacto". Ver Gráfico N° 05 Mapa de Calor.

***Gráfico N° 05 Mapa de calor del riesgo***




Fuente: Basado en el Manual Metodológico "Guía para la Gestión Integral de Riesgos"

De acuerdo a su criticidad, los riesgos pueden ser:

- Riesgos bajos (1-2)
- Riesgos medios (3-4)
- Riesgos altos (6-9)
- Riesgos extremos (12-16)

**d. Acciones a considerar según el nivel del riesgo.**

En función a la criticidad del riesgo se seleccionará una prioridad de respuesta al riesgo, la cual se enmarca dentro de las siguientes acciones:

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 21 de 32
	<b>Gestión Integral de Riesgos</b>	

**Tabla N° 06 Acciones según el nivel del riesgo**

NIVEL DE RIESGO	ACCIONES
<b>Riesgo Bajo<sup>1</sup></b>	Se gestiona con procedimientos. Los riesgos son controlados con seguimiento. (*)
<b>Riesgo Medio</b>	Debe ser gestionado con procedimientos de control, con atención periódica, seguimiento semestral.
<b>Riesgo Alto</b>	Se requiere priorización de atención de las Gerencias. Planes de Tratamiento requeridos, implementados y reportados a las Gerencias y Alta Dirección. (*)
<b>Riesgo Extremo</b>	Se requiere priorización de atención de las Gerencias. Planes de Tratamiento requeridos, implementados y reportados a las Gerencias y Alta Dirección. (*)

<sup>1</sup> Cuando el nivel del riesgo llegue a su nivel más bajo (área verde), los riesgos se controlan y monitorean a fin de mantenerlos en el mismo nivel.

**7.1.4 Fase 4.- Actividades de Control** La identificación y clasificación de controles consiste en la identificación de los esfuerzos realizados por SEDAPAL para procurar que los riesgos se encuentren dentro del nivel de apetito de riesgo.

- a. Etapa 1 - Criterios para la determinación de controles.  
 Un control es una actividad que tiene como finalidad reducir la criticidad de un riesgo al cual se encuentra asociado. La descripción, la frecuencia y responsable del control son descritos en el DGMFO0038 Formulario Matriz de Riesgos y Controles.

Para la frecuencia y el responsable tener en cuenta que:


- Frecuencia del control: Representa la periodicidad en la que el control se ejecuta.
- Responsable del control: Es aquel colaborador que ejecuta directamente la actividad de control.

- b. Etapa 2 – Clasificación de controles  
 Los controles se clasifican según sus atributos, los cuales determinan su fortaleza, estos son:
- La oportunidad en la que se ejecutan.
  - El grado de automatización.
  - Objetivo del control.
  - Definición del control.
  - Operatividad y Autoevaluación del control.

Para cada atributo de los controles se presentan los siguientes cuadros a fin de clasificarlos adecuadamente.

**Tabla N° 07 Oportunidad del Control**

Clasificación	Descripción
Preventivo	Actividad de control que ayuda a evitar la ocurrencia de un riesgo.
Correctivo	Actividad de control que permite identificar errores luego de ocurrido el riesgo.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 22 de 32
	<b>Gestión Integral de Riesgos</b>	

***Tabla N° 08 Grado de Automatización del Control***

Clasificación	Descripción	
Automático	Control que es realizado internamente por el sistema de información.	3
Semi automático	Control que depende de la habilidad de una persona para prevenir o detectar los errores ocurridos, utilizando información proveniente de un sistema.	2
Manual	Control que depende de la habilidad de una persona (dueño o responsable de la actividad de control) para prevenir o detectar los errores ocurridos.	1

(\*)

***Tabla N° 09 Definición del Control***

Definición	
No se han definido actividad, periodicidad, evidencia y responsable; <u>no existe segregación de funciones.</u>	1
Se han definido parcialmente actividad, periodicidad, evidencia y responsables; <u>existe segregación de funciones</u>	2
Se han definido actividad, periodicidad, evidencia y responsables, <u>existe segregación de funciones</u>	3


***Tabla N° 10 Operatividad y Autoevaluación del Control***

Nivel de Control Criterios	Débil	Moderado	Fuerte
Operatividad	1. Históricamente se presentan continuas desviaciones del control.	2. Históricamente se presentan muy pocas desviaciones del control.	3. Históricamente no se han presentado desviaciones del control.
Autoevaluación del control	1. El control nunca ha sido autoevaluado.	2. El control ha sido autoevaluado con alguna frecuencia.	3. El control es autoevaluado regularmente y no ha sido objeto de observación por ningún área de control.

- c. Etapa 3 – Evaluación de efectividad de controles y actualización de controles.  
El riesgo residual sirve como principal indicador para medir la efectividad de los controles, midiendo la variación entre el riesgo inherente y el residual.

Para la evaluación de los controles, se consideran los criterios de diseño y ejecución. Un control se considera deficiente en los siguientes casos:

- Diseño del Control
  - ✓ Si el diseño del control no permite prevenir o detectar errores.
  - ✓ Si el control en su estado actual no alcanza el objetivo para el que fue creado.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 23 de 32
	<b>Gestión Integral de Riesgos</b>	

- ✓ Si el control no tiene asignado a más de un responsable, no existe segregación de funciones.
- Ejecución del control
  - ✓ Cuando un control apropiadamente diseñado no opera como está diseñado.
  - ✓ Cuando el responsable de realizar el control no posee la autoridad y/o calificación necesaria para realizarlo.

Para evaluar el diseño del control se consideran 03 aspectos: i) Oportunidad ii) Automatización, iii) Definición. Considerar los puntajes de las tablas N° 07, N° 08 y N° 09. (\*)

El resultado de la suma de los atributos se obtiene la calificación del diseño según el siguiente cuadro:

**Tabla N° 11 Calificación del Diseño**

Calificación del Diseño	
De 0 a 3	Débil
De 4 hasta 6	Moderado
De 7 hasta 8	Fuerte

Para evaluar la ejecución del control se consideran 02 aspectos: i) operatividad y, ii) Autoevaluación del control, descritas en el cuadro N° 10.

El resultado de la suma de los atributos se obtiene la calificación de la operatividad y autoevaluación de control:


**Tabla N° 12 Calificación de la ejecución**

Calificación de la Ejecución	
De 0 a 2	Débil
De 3 hasta 4	Moderado
De 5 hasta 6	Fuerte

La utilización de la información de los cuadros previos permite obtener el resultado de las características de los controles evaluados.

Para el Sistema Integrado de Gestión, la eficacia del control se determina en la Etapa 3 - Evaluación de efectividad de controles y actualización de controles.

La calificación total del control se determina de los resultados obtenidos en la evaluación del diseño y ejecución, tal como se presenta en el siguiente cuadro:

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 24 de 32
	<b>Gestión Integral de Riesgos</b>	

**Tabla N° 13 Tabla del Diseño y Ejecución del Control**

Evaluación de Controles			
Diseño	Ejecución	Diseño-Ejecución	Resultados del Control
1. Débil	1. Débil	1. Débil - 1. Débil	<b>1. Débil</b>
1. Débil	2. Moderado	1. Débil - 2. Moderado	<b>1. Débil</b>
1. Débil	3. Fuerte	1. Débil - 3. Fuerte	<b>1. Débil</b>
2. Moderado	1. Débil	2. Moderado - 1. Débil	<b>1. Débil</b>
2. Moderado	2. Moderado	2. Moderado - 2. Moderado	<b>2. Moderado</b>
2. Moderado	3. Fuerte	2. Moderado - 3. Fuerte	<b>2. Moderado</b>
3. Fuerte	1. Débil	3. Fuerte - 1. Débil	<b>1. Débil</b>
3. Fuerte	2. Moderado	3. Fuerte - 2. Moderado	<b>2. Moderado</b>
3. Fuerte	3. Fuerte	3. Fuerte - 3. Fuerte	<b>3. Fuerte</b>

**Tabla N° 14 Objetivo del Control**

Objetivo	Nivel
El control mitiga el riesgo solo en probabilidad	Débil (P)
El control mitiga el riesgo solo en impacto	Moderado (I)
El control mitiga el riesgo (impacto + probabilidad)	Fuerte (P+I)


Finalmente, los resultados deben evaluarse analizando si los controles están dirigidos a mitigar solo la probabilidad, solo impacto o ambos, considerando la evaluación de la tabla N° 13 y N° 14:

**Tabla N° 15 Resultados de Diseño y Ejecución con Objetivo del Control**

Resultados del Control	Nivel Objetivo del Control	Calificación final del control
Débil	Débil (P)	Débil (P)
Débil	Moderado (I)	Moderado (I)
Débil	Fuerte (P+I)	Moderado (P+I)
Moderado	Débil (P)	Débil (P)
Moderado	Moderado (I)	Moderado (I)
Moderado	Fuerte (P+I)	Fuerte (P+I)
Fuerte	Débil (P)	Moderado (P)
Fuerte	Moderado (I)	Moderado (I)
Fuerte	Fuerte (P+I)	Fuerte (P+I)

Nota: Para la evaluación de los controles en lo que respecta al diseño – ejecución, esto podrá realizarse una vez que se hayan implementado o ejecutado los controles, y se evidencien documentalmente. Asimismo, pueden ser publicados en la plataforma informática dispuesto para tal fin, y ser monitoreados por el área responsable del control.



	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 25 de 32
	<b>Gestión Integral de Riesgos</b>	

Luego de la aplicación de los controles podrá realizarse la evaluación del riesgo residual.

d. Etapa 4 – Evaluación del riesgo residual

Un riesgo residual es el riesgo restante luego de haber aplicado los controles. El nivel de riesgo al que está sometido SEDAPAL nunca puede erradicarse totalmente, es importante alinear el mismo a la tolerancia al riesgo definida por la Empresa.

***Cuadro N° 15 Tabla Evaluación de Riesgo Residual***

<u>Calificación final del control</u>	<u>Probabilidad</u>	<u>Impacto</u>
<u>Débil (P)</u>	<u>0 nivel hacia abajo</u>	<u>0 nivel hacia la izquierda</u>
<u>Moderado (P+I)</u>	<u>1 nivel hacia abajo</u>	<u>1 nivel a la izquierda</u>
<u>Moderado (P)</u>	<u>1 nivel hacia abajo</u>	<u>0 nivel a la izquierda</u>
<u>Moderado (I)</u>	<u>0 nivel hacia abajo</u>	<u>1 nivel a la izquierda</u>
<u>Fuerte (P+I)</u>	<u>2 niveles hacia abajo</u>	<u>2 niveles a la izquierda</u>

- Cálculo cuando existe más de un control


***Tabla N° 16 Cuadro Cálculo Controles***

<u>Controles</u>	<u>Probabilidad</u>	<u>Impacto</u>
<u>Control 1</u>	<u>0 nivel hacia abajo</u>	<u>0 nivel hacia la izquierda</u>
<u>Control 2</u>	<u>1 nivel hacia abajo</u>	<u>1 nivel a la izquierda</u>
<u>Control 3</u>	<u>1 nivel hacia abajo</u>	<u>0 nivel a la izquierda</u>
<u>Control n</u>	<u>0 nivel hacia abajo</u>	<u>1 nivel a la izquierda</u>
<u>Evaluación del nivel del riesgo</u>	<u>Promedio (Control 1, Control 2, control 3,...Control n)</u>	<u>Promedio (Control 1, Control 2, control 3,...Control n)</u>

Considerar para el cálculo redondear a un número entero inferior próximo.

Finalmente, los resultados de las evaluaciones de riesgo a nivel inherente y residual se representan en el gráfico N° 03 Mapa de calor del riesgo descrito en la fase 03 Evaluación de riesgos.

De acuerdo al nivel del riesgo residual obtenido, se precisan acciones a considerar según el cuadro N° 06 descritas en la fase 03.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 26 de 32
	<b>Gestión Integral de Riesgos</b>	

- Frecuencia de evaluación del riesgo residual para NTO ISO/IEC 17020:**  
 Se realizará de acuerdo a la tabla N° 17 "Frecuencia de evaluación del riesgo residual", se registrará mediante el DG MFO012 formulario Lista de Asistencia y/o DGMFO028 formulario Acta de Reunión en caso de reunión presencial; de ser virtual, el DGMFO012 formulario Lista de Asistencia será reemplazado por la lista generada por el MS-TEAMS.

**Tabla N° 17 "Frecuencia de evaluación del riesgo residual"**

<b>Frecuencia de evaluación del riesgo residual</b>		
<b>Nivel</b>	<b>Descripción</b>	<b>Frecuencia de revisión</b>
4	Extremo	Una vez pasado 1 mes.
3	Alto	Una vez pasado 3 meses.
2	Medio	Una vez pasado 6 meses.
1	Bajo	Una vez pasado 9 meses o 1 año.

#### 1.1.1 Fase 5.- Tratamiento al Riesgo

El tratamiento que se le brinda a un riesgo tiene como propósito mantener la criticidad del riesgo dentro de los niveles de apetito al riesgo definidos por SEDAPAL. Se desarrolla después de la evaluación del riesgo residual

- a. Etapa 1 – Definición de la estrategia de tratamiento al riesgo.
  - En esta etapa se definirá la estrategia de tratamiento a los riesgos identificados para mantenerlos dentro de los niveles establecidos en el apetito de riesgo.
  - Existen diversas alternativas para gestionar los riesgos de acuerdo a sus características, estas se aplican una vez realizada la evaluación del riesgo residual y de acuerdo al apetito de riesgo.
  - Las estrategias y respuestas al riesgo a aplicar varían en función al riesgo a gestionar y al apetito de riesgo.

Para esta etapa, se definirán las estrategias según la siguiente tabla:

**Tabla N° 18 Tabla Estrategia de Respuesta**

ESTRATEGIA DE RESPUESTA	DESCRIPCIÓN	¿CUÁNDO SELECCIONARLO?
Evitar	Dejar de realizar la actividad o la acción que genera el riesgo debido a que el nivel del riesgo es inaceptable.	Cuando el beneficio de implementar un control sea menor al costo del riesgo inherente y sus posibles consecuencias.
Reducir o Mitigar	Establecer controles para disminuir la probabilidad de ocurrencia del riesgo y el impacto.	Cuando el beneficio de implementar un control sea mayor al costo del riesgo inherente y la Empresa se encuentre en capacidad de realizar el tratamiento del riesgo.

ESTRATEGIA DE RESPUESTA	DESCRIPCIÓN	¿CUÁNDO SELECCIONARLO?
Transferir	Transferir a un tercero u otra de las partes con la capacidad financiera o especialización necesaria para administrar adecuadamente el riesgo, o enfrentar las pérdidas originadas ante la ocurrencia de la adversidad y manejar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo.  El riesgo se debería transferir o compartir a otra de las partes que pueda	Cuando el beneficio de implementar un control sea mayor al costo del riesgo inherente y un tercero tenga una mayor capacidad para realizar su tratamiento, debido a su especialización, infraestructura entre otros factores.
Aceptar (*)	Conservar el riesgo en su presente nivel realizando una adecuada administración y monitoreo.	Cuando el control (efectivo) relacionado al riesgo, no disminuya su criticidad y el riesgo deba permanecer monitoreado debido a que su alteración puede afectar la continuidad operativa del negocio. <u>Asimismo, se deberá continuar monitoreando a través de las acciones de control establecidas en los planes de tratamiento (riesgos altos y extremos)</u>
Eliminar	Eliminar la causa raíz que ocasiona el riesgo. Además, la Empresa debe diseñar actividades para afrontar las posibles consecuencias de la eliminación realizada.	Cuando es factible eliminar la causa raíz que ocasiona el riesgo, verificando previamente, que el beneficio obtenido por esta acción sea mayor al costo sus consecuencias para la Empresa.

b. Etapa 2 - Elaboración de planes de tratamiento.

Corresponde a la propuesta de medidas a implementar con el fin de abordar una estrategia de tratamiento definida sobre el riesgo identificado.

Para definir los planes de acción es necesario considerar lo siguiente:


- Cuando el control que mitiga el riesgo se encuentra mal diseñado.
- Cuando el riesgo no cuenta con controles.
- Cuando el riesgo residual se encuentra por encima de los niveles de tolerancia.
- Cuando el nivel del riesgo llega a sus niveles altos y extremos.

Es importante que se defina al responsable de realizarla, la fecha de inicio y fin y se documente formalmente la actividad a ser implementada empleando el DGMFO0039 Formulario Plan de Tratamiento de Riesgos.

c. Etapa 3 – Definición de indicadores clave de riesgos (KRIs)

Son métricas financieras u operacionales que ofrecen una base razonable para estimar la probabilidad de ocurrencia y severidad de uno o más eventos de riesgo.

- Identificación de riesgos que requieren KRI
- Riesgos residuales de severidad igual o mayor a alto y que estén relacionados a un proceso crítico.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 28 de 32
	<b>Gestión Integral de Riesgos</b>	

- Riesgos de acuerdo al criterio del dueño del proceso.

Características imprescindibles para el diseño de KRI`s:

- Ser dinámico.
- No redundante.
- Medible.
- De fácil implementación.

### 1.1.2 Fase 6.- Supervisión y Seguimiento

Esta fase implica hacer la supervisión, seguimiento o monitoreo de las acciones y/o controles acordados, de los diferentes procesos críticos, sean estos controles ya establecidos e implantados como controles propuestos o acordados implantar a futuro, de acuerdo al presupuesto de SEDAPAL, plan de crecimiento y situación financiera.

- Cada funcionario a cargo del proceso es responsable de remitir semestralmente al Equipo de Gestión Institucional (EGI) sobre el estado situacional de los riesgos de sus respectivos procesos, a través del Informe de Revisión por la Dirección del SIG.
- El EGI consolida la información del reporte de seguimiento de riesgos de procesos recibida de cada uno de los funcionarios a cargo de cada uno de los procesos, para ser remitida al Comité de Riesgos en la frecuencia que se determine, permitiendo de esta manera que se efectúen los ajustes, toma de decisiones u otra acción que dicho órgano considere necesario.

- a. Etapa 1: Cronograma de seguimiento a los Planes de Tratamiento.

Los planes de acción definidos deben consolidarse y monitorearse a través de un cronograma de implementación, de acuerdo a lo establecido en el DGMFO0039 Formulario Plan de Tratamiento de Riesgos.

- b. Etapa 2: Evaluación de la eficacia de los controles.

Una vez culminada la implementación del Plan de Tratamiento de Riesgos, se realiza de acuerdo a los criterios establecidos en la Fase 4.

Evaluación de la eficacia de los controles para la NTP ISO/IEC 17020:


Realizar el seguimiento a la eficacia de los controles como máximo cada tres meses, por el CT-EGCM, mediante el DGMFO012 Formulario Lista de Asistencia y/o DGMFO028 Formulario Acta de Reunión en caso de reunión presencial; de ser virtual, el DGMFO012 Formulario Lista de Asistencia será reemplazado por la lista generada por el MS-TEAMS.

- c. Etapa 3: Evaluación de riesgo residual y actualización de su clasificación.

Se evalúan si las estrategias de tratamiento al riesgo implementadas tuvieron algún impacto en los riesgos residuales, por lo tanto, finalizada las acciones comprendidas en el DGMFO0039 Formulario Plan de Tratamiento de Riesgos, los responsables del proceso deben reevaluar el riesgo residual. De esta manera, se vuelven a clasificar los riesgos residuales con la criticidad actualizada.

- d. Etapa 4: Actualización de los documentos de riesgos.

La identificación del riesgo, evaluación del riesgo, elaboración de controles, y el tratamiento del riesgo pueden estar sujetos a actualizaciones debido a las necesidades que se identifiquen, sean ajenas a la gestión de riesgos o parte de la mejora continua. De presentarse alguna situación que justifique la actualización de los riesgos, se realiza en DGMMR0038 Matriz de Riesgos y Controles siguiendo la ruta de aprobación correspondiente.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 29 de 32
	<b>Gestión Integral de Riesgos</b>	

Actualización de los documentos de riesgos para la NTP ISO/IEC 17020:


- a) Realizar la revisión y/o actualización de la DGMMR0038 Matriz de Riesgos y Controles, como máximo a los tres meses de su última actualización y/o revisión, o cuando se identifiquen nuevas oportunidades o situaciones de riesgo que afecten la imparcialidad y/o el sistema integrado de gestión, se tomarán mejores medidas de control.
- b) Colocar en subrayado los riesgos, oportunidades y controles recientemente identificados y agregados y/o actualizaciones en el DGMFO0039 Formulario Plan de Tratamiento de Riesgos, en tanto que, los nuevos riesgos y/u oportunidades que requieran tomar acciones se colocarán en el DGMFO0039 Formulario Plan de Tratamiento de Riesgos, en subrayado, así como la respectiva fecha en la sección "Fecha de actualización" de ambos registros.
- c) Identificar de manera continua los riesgos a la imparcialidad, de sus actividades, o de sus relaciones, o de las relaciones de su personal, y/o oportunidades mediante una reunión con el Comité de evaluación de riesgos, cada tres meses y/o cuando se requiera y se registrará mediante el DGMFO012 Formulario Lista de Asistencia y/o DGMFO028 Formulario Acta de Reunión en caso de reunión presencial; de ser virtual, el DGMFO012 Formulario Lista de Asistencia será reemplazado por la lista generada por el MS-TEAMS, siendo responsable de ello el CT-EGCM.

### **1.2 Consideraciones para evaluación de riesgos ante cambios significativos.**

Para identificar cambios significativos se consideran aquellos aspectos en el entorno interno y externo que podrían afectarle a la Empresa. A continuación, algunos criterios o situaciones que pueden implicar cambios significativos, esta lista es referencial y no excluye otros criterios o casos que pueda establecer la Empresa. Asimismo, se ha identificado que área clave está a cargo de su identificación y reporte.

***Tabla N° 19 Situaciones de cambios significativos***

<u>Cambios significativos</u>	<u>Áreas Claves</u>
Subcontrataciones significativas. Por ejemplo, los servicios vinculados a la actividad principal del negocio o de soporte esenciales para que el negocio no sea afectado en sus ingresos, solvencia o continuidad de manera importante.	Gerencia de Logística y Servicios en coordinación con otras áreas involucradas.
Alianzas, Convenios o contratos asociativos o en participación con otras entidades. Por ejemplo, tener consorcios o asociaciones con otras entidades, o cualquier otra forma de contratos asociativos cuya estructura, composición accionaria o falla en la debida diligencia del conocimiento del asociado, entre otros, afecten la imagen o reputación de la empresa o genere o sea afectado en sus ingresos, solvencia o continuidad de manera importante	Gerencia de Asuntos Legales y Regulación
Cambios de infraestructura tecnológica o sistemas informáticos. Por ejemplo, una falla sobre la infraestructura tecnológica puede implicar riesgos como pérdidas financieras, multas, acciones legales, afectación sobre la imagen de la organización, causar problemas operativos o afectar los ingresos, solvencia o continuidad de manera importante	Gerencia de Desarrollo e Investigación

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 30 de 32
	<b>Gestión Integral de Riesgos</b>	


<u>Cambios significativos</u>	<u>Áreas Claves</u>
Proyectos o inversiones. Por ejemplo, determinar un monto mínimo para proyectos e inversiones, por la cual, puede evaluarse criterios como riesgos económicos, riesgos sociales o políticos, riesgos operacionales, riesgos financieros, riesgos regulatorios, riesgos de la naturaleza y/o riesgos tecnológicos u otros que puedan afectar los ingresos, solvencia o continuidad de manera importante	Gerencia de Proyectos y Obras en coordinación con otras áreas involucradas.
Cambios en las operaciones que se originen como consecuencia de condiciones, económicas, políticas o legales. Por ejemplo, cambio de gobierno, cambio de regulación relevante, crisis económicas nacionales e internacionales que pudieran afectar las operaciones con consecuencias negativas en los ingresos, solvencia o continuidad de manera importante.	Gerencia de Desarrollo e Investigación en coordinación con otras áreas involucradas.

Los gerentes o dueños de los procesos deben informar al EGI todo cambio que consideren que se encuentra en la tabla N° 19 Situaciones de Cambios significativos u otros que puedan impactar el desarrollo de las actividades de la Empresa.

Una vez que el EGI recibe el informe de identificación de cambios significativos, éste es evaluado por el responsable titular/suplente de la GIR en la Empresa, quien coordina y/o propone a los dueños de procesos los controles y/o planes de acción, cuando correspondan.

De requerir un análisis de riesgos adicional y/o complementario, el responsable titular/suplente de la GIR debe coordinar con el dueño del proceso a fin de revisar el informe.

Los mecanismos y herramientas de reporte para la evaluación de riesgos ante cambios significativos serán comunicado por el EGI.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 31 de 32
	<b>Gestión Integral de Riesgos</b>	

## ANEXO 1

### Técnicas para la identificación de riesgos

Para la identificación de riesgos, pueden emplearse una o más técnicas que se describen a continuación según sea el nivel de análisis que se desee efectuar.

**a. Tormenta de ideas**

El Objetivo de esta técnica es obtener una lista completa de los riesgos de la empresa con el propósito de aprovechar el conocimiento colectivo y desarrollar una lista de acontecimientos relacionados.

**b. Cuestionarios y /o encuestas**

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

**c. Entrevistas**


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

**d. Análisis de fortalezas y debilidades, oportunidades y amenazas (FODA)**

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

**e. Diagramación de Ishikawa**

Esta técnica permite identificar detectar problemas y determinar sus causas de forma estructurada, por lo que también se denomina diagrama de causa y efecto.

	<b>MANUAL</b>	<b>Código</b> : DGMMMA0004 <b>Versión</b> : 09 <b>Aprobado</b> : GG <b>Fecha</b> : 2024.08.27 <b>Página</b> : 32 de 32
	<b>Gestión Integral de Riesgos</b>	

**Anexo 2**  
**Descripción de funciones y relación entre las áreas de servicio de agua potable y alcantarillado de lima – SEDAPAL S.A. como organismo de inspección**  
**NTP ISO/IEC 17020**

<b><u>Nombre del Área</u></b>	<b><u>Responsable del Área</u></b>	<b><u>Relación directa con Organismo de Inspección</u></b>	<b><u>Relación directa con otras áreas</u></b>
Directorio	Presidente del Directorio	NO	Todas las áreas
Gerencia General	Gerente General / Gerente General Adjunto	NO	Todas las áreas
Gerencia Comercial	Gerente Comercial	NO	Todas las áreas
Gerencia de Recursos Humanos	Equipo Remuneraciones, Compensaciones y Beneficios	SI	Todas las áreas
Otras Gerencias y jefaturas citadas en el Organigrama	Gerentes y jefaturas	NO	Todas las áreas
Equipo Evaluación de Calidad	Jefe de equipo	NO	Todas las áreas
Equipo Gestión Institucional	Jefe de Equipo (SIG)	SI	Todas las áreas
Equipo Gestión Comercial y Micromedición	Jefe de equipo	SI	Gerencias
Organismo de Inspección	Coordinadora de Calidad	SI	Gerencia Comercial / Equipo Gestión Comercial y Micromedición / Equipo Gestión Institucional
Organismo de Inspección	Coordinador Técnico	SI	Gerencia Comercial / Equipo Gestión Comercial y Micromedición

Nota 1: Las funciones de los puestos citados en el presente anexo se encuentran descritas en el DG-MA001 Manual de Organización y Responsabilidades General.

Nota 2: La estructura jerárquica se describe en el Organigrama de SEDAPAL y de la Gerencia Comercial.

Nota 3: La línea de comunicación entre el Directorio, Gerencia General y Gerencia Comercial para con el Organismo de Inspección no es directa, se realiza a través del Jefe de Equipo Gestión Comercial y Micromedición.