Manual de

Gestión de Riesgos

INTRODUCCIÓN

INTER RAPIDÍSIMO S.A., reconoce que la incertidumbre es un elemento inherente al desarrollo de sus actividades y a la toma de decisiones en todos los niveles. En un entorno dinámico y competitivo como el sector logístico, la adecuada gestión de riesgos es fundamental para proteger la continuidad del negocio, fortalecer la resiliencia organizacional, apoyar el cumplimiento de los objetivos estratégicos y salvaguardar la generación de valor.

El presente manual establece los lineamientos metodológicos definidos en la **Política de Gestión Integral de Riesgos GPL-PRO-L-02**, así como los criterios y herramientas para la identificación, análisis, evaluación, tratamiento, monitoreo, comunicación y reporte de los riesgos que puedan afectar a la organización. Su aplicación fortalece un enfoque preventivo, sistemático e integrado, alineado con el Sistema Integrado de Gestión Empresarial (SIGE) y con el modelo de gobierno corporativo.

La metodología aquí definida se fundamenta en marcos de referencia y mejores prácticas reconocidas, entre los que se destacan ISO 31000 y COSO ERM, con el fin de orientar una gestión de riesgos consistente, trazable y alineada con el contexto estratégico, operativo, normativo y tecnológico, así como con los niveles de apetito y tolerancia al riesgo definidos.

A través de este manual, la organización promueve una cultura de riesgo basada en la anticipación, la responsabilidad, la rendición de cuentas y la mejora continua, como soporte para la toma de decisiones y el fortalecimiento de su desempeño sostenible.

1. Objetivos

Objetivo general

Establecer los lineamientos y criterios para la gestión integral de riesgos en **INTER RAPIDÍSIMO S.A.,** orientados a la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos y oportunidades que puedan afectar el logro de los objetivos organizacionales, fortaleciendo la toma de decisiones y contribuyendo a la creación, protección y sostenibilidad del valor para la organización y sus grupos de interés.

Objetivos específicos

- Identificar, analizar y evaluar los riesgos asociados a los procesos, proyectos, activos y actividades, con el fin de priorizar su tratamiento y mantener el riesgo residual dentro de los niveles definidos de apetito y tolerancia.
- Diseñar, implementar y fortalecer controles y planes de tratamiento que permitan reducir la probabilidad o impacto de los riesgos, contribuyendo a la continuidad del negocio y a la eficacia operacional.

- Proveer información confiable y oportuna sobre el perfil de riesgo organizacional como insumo para la toma de decisiones, la planeación estratégica y la asignación eficiente de recursos.
- Proteger los activos críticos, incluyendo información, tecnología, infraestructura y demás recursos estratégicos que soportan la operación, garantizando su confidencialidad, integridad, disponibilidad y uso adecuado.
- Fortalecer el cumplimiento de las obligaciones regulatorias, contractuales y éticas, contribuyendo a la prevención de riesgos LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses y otras conductas que puedan afectar a la organización.
- Promover la identificación oportuna de riesgos emergentes y cambios del contexto interno y externo, fortaleciendo la capacidad de anticipación y adaptación.
- Fomentar una cultura organizacional orientada a la gestión del riesgo, basada en la responsabilidad, la transparencia, la rendición de cuentas y la mejora continua.

2. Alcance

El presente manual establece el marco metodológico para la gestión integral de riesgos en **INTER RAPIDÍSIMO S.A.,** y será aplicable a todas las contrapartes, los procesos, actividades y activos en todas las sedes, operaciones y ubicaciones donde la organización desarrolle sus actividades.

La gestión de riesgos se articula con el Sistema Integrado de Gestión Empresarial (SIGE), así como con los diferentes sistemas de gestión, marcos normativos y modelos de control adoptados por la organización, incluyendo la gestión de riesgos asociados a LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses entre los que se destacan:

- ISO 9001 – Sistema de Gestión de la Calidad.
- ISO 39001 – Sistema de Gestión de la Seguridad Vial.
- ISO 45001 – Sistema de Gestión de Seguridad y Salud en el Trabajo.
- ISO 14001 – Sistema de Gestión Ambiental.
- ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27005 – Gestión de Riesgos de Seguridad de la Información.
- ISO 28001 – Seguridad en la Cadena de Suministro.
- ISO 22301 – Continuidad del Negocio.
- COSO ERM – Gestión de Riesgos Empresariales.
- SARLAFT, PTEE y buenas prácticas de SAGRILAFT.
- OEA – Operador Económico Autorizado.
- Estándares GRI y demás lineamientos de sostenibilidad aplicables.

La aplicación de esta metodología se materializa principalmente a través de la **Matriz de Riesgos GPL-PRO-R-03** y demás herramientas definidas por la organización, mediante las cuales se identifican, valoran, monitorean, reportan y gestionan los riesgos asociados a los procesos, proyectos y actividades de la organización.

Definiciones y Abreviaturas

- Apetito de Riesgo: Cantidad y tipo de riesgo que la organización está dispuesta a asumir en la búsqueda y logro de sus objetivos estratégicos y en la creación de valor.
- Capacidad de Riesgo: Nivel máximo de riesgo que la organización puede soportar sin comprometer su viabilidad financiera, operativa, reputacional o estratégica.
- Categoría del Riesgo: Clasificación general del riesgo según su naturaleza o fuente (ej. legal, operativo, reputacional, financiero).
- Causas: Factores, eventos o condiciones (internas y externas) que, individualmente o en combinación, pueden dar lugar a la materialización de un riesgo.
- Confidencialidad (CID): Propiedad de la información que garantiza que esta no sea divulgada ni puesta a disposición de individuos, entidades o procesos no autorizados.
- Control: Medida o acción implementada para modificar el riesgo, ya sea reduciendo su probabilidad de ocurrencia o mitigando su impacto.
- COSO ERM: Marco de referencia para la gestión del riesgo empresarial, diseñado para identificar eventos potenciales y gestionar el riesgo dentro del apetito definido.
- Disponibilidad (CID): Propiedad de la información y los sistemas asociados de ser accesibles y utilizables cuando son requeridos por una entidad o proceso autorizado.
- Eficacia del Control: Grado en que un control implementado logra reducir la probabilidad de ocurrencia de un riesgo o mitigar su impacto.
- Evento de Riesgo: Situación o suceso potencial que puede afectar el logro de los objetivos de la organización.
- Factores de Riesgo: Condición o atributo que aumenta la probabilidad de que un riesgo se materialice o que incrementa la severidad de su impacto.
- Fuente de Riesgo: Elemento que, por sí solo o en combinación, tiene el potencial intrínseco de dar origen a un riesgo.
- Gestión del Riesgo: Conjunto de actividades coordinadas para identificar, evaluar, controlar, tratar y monitorear los riesgos, con el fin de proporcionar una seguridad razonable sobre el logro de los objetivos.
- Impacto: Consecuencia o resultado de la materialización de un riesgo sobre los objetivos de la organización, que puede ser de naturaleza financiera, operativa, reputacional, entre otras.
- Incertidumbre: Estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o su probabilidad.

- Integridad (CID): Propiedad de la información que garantiza su exactitud, completitud y protección frente a modificaciones no autorizadas.
- KPIs: Key Performance Indicators -Indicadores Clave de Desempeño-.
- LA/FT: Lavado de Activos y Financiación del Terrorismo.
- Mapa de Riesgos: Representación gráfica de los riesgos, posicionados en una matriz según su probabilidad de ocurrencia y la severidad de su impacto.
- Materialización del Riego: Ocurrencia efectiva de un evento de riesgo identificado que genera impactos negativos o positivos sobre los objetivos de la organización.
- OEA: Operador Económico Autorizado.
- Oportunidad: Posibilidad de que la incertidumbre tenga un efecto positivo sobre los objetivos de la organización, generando valor, eficiencia o crecimiento.
- Probabilidad: Medida de la posibilidad de que un evento de riesgo ocurra en un período determinado.
- PTEE: Programa de Transparencia y Ética Empresarial.
- Riesgo: Efecto de la incertidumbre sobre los objetivos de la organización, que puede manifestarse en impactos positivos o negativos.
- Riesgo Aceptable: Nivel de riesgo que la organización decide asumir de acuerdo con su apetito y tolerancia al riesgo.
- Riesgo Emergente: Riesgo nuevo o en evolución que surge a partir de cambios en el entorno interno o externo de la organización, cuya probabilidad, impacto o naturaleza aún no está completamente definida, pero que puede afectar el cumplimiento de los objetivos en el corto, mediano o largo plazo
- Riesgo Inherente: Nivel de riesgo existente antes de considerar la eficacia de los controles implementados.
- Riesgo Residual: Nivel de riesgo que permanece después de aplicar los controles y medidas de tratamiento del riesgo.
- Riesgo de Seguridad de la Información: Posibilidad de que una amenaza explote una vulnerabilidad de un activo de información, causando un impacto adverso en la organización.
- SAGRILAFT: Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos y Financiación del Terrorismo.
- SARLAFT: Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.
- Tolerancia del Riesgo: Grado de variación aceptable respecto al apetito de riesgo definido para un objetivo específico.

  Tratamiento de Riesgos: Proceso para seleccionar e implementar opciones destinadas a modificar el riesgo, tales como evitarlo, reducirlo, transferirlo o aceptarlo.

3. Marco de Referencia y Principios de Gestión

La gestión integral de riesgos de la organización se fundamenta en marcos de referencia, estándares internacionales y buenas prácticas reconocidas, con el propósito de asegurar un enfoque estructurado, consistente e integrado con los sistemas de gestión, el modelo de control interno y la estrategia organizacional.

La metodología definida en el presente manual articula la gestión de riesgos con los siguientes estándares, marcos normativos y modelos de referencia:

Gestión empresarial y riesgos

- ISO 31000: Directrices para la gestión del riesgo.
- COSO ERM: Marco de Gestión de Riesgos Empresariales.
- ISO 22301: Sistema de Gestión de Continuidad del Negocio.

Calidad, operación y sostenibilidad

- ISO 9001: Sistema de Gestión de la Calidad.
- ISO 39001: Sistema de Gestión de la Seguridad Vial.
- ISO 45001: Sistema de Gestión de Seguridad y Salud en el Trabajo.
- ISO 14001: Sistema de Gestión Ambiental.
- ISO 28001: Seguridad en la Cadena de Suministro.

Seguridad de la información y cumplimiento

- ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27005: Gestión de Riesgos de Seguridad de la Información.
- SARLAFT, PTEE y las buenas prácticas del SAGRILAFT.
- OEA: Operador Económico Autorizado.
- Lineamientos de Gobierno Corporativo y sostenibilidad aplicables.

Estos marcos permiten fortalecer la gestión integral de riesgos, asegurando su alineación con los objetivos estratégicos, el apetito y tolerancia al riesgo definidos, la continuidad del negocio, el cumplimiento normativo, la generación de valor y el modelo de gobierno corporativo de la organización.

En relación con los sistemas de cumplimiento, la gestión de los riesgos asociados al Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) se desarrolla en el marco de los sistemas SARLAFT, PTEE y buenas prácticas del SAGRILAFT, adoptados por la organización, los cuales cuentan con manuales, procedimientos y lineamientos específicos.

El presente manual establece el marco metodológico general para la gestión de estos riesgos, el cual se articula y complementa con los documentos de cumplimiento, en donde se detallan las disposiciones particulares, controles y mecanismos específicos requeridos por la normatividad aplicable.

Principios de la gestión del riesgo

La gestión integral de riesgo se rige por principios orientados a garantizar su eficacia, consistencia, integración y alineación con las mejores prácticas de gestión empresarial, promoviendo la toma de decisiones informada y la protección del valor organizacional.

- Creación, protección y sostenibilidad del valor: La gestión de riesgos contribuye al logro de los objetivos estratégicos, fortalece la resiliencia organizacional y apoya la generación de valor para la organización y sus partes interesadas.
- Integración: La gestión del riesgo se incorpora en los procesos organizacionales, el direccionamiento estratégico, el gobierno corporativo y la toma de decisiones en todos los niveles.
- Enfoque estructurado y sistemático: La gestión de riesgos se desarrolla mediante una metodología definida, documentada y consistente, que facilita resultados comparables, confiables y trazables.
- Personalización y contexto: La metodología se adapta al contexto interno y externo de la organización, a la naturaleza de sus operaciones y al nivel de exposición al riesgo.
- Participación e inclusión: Promueve la participación de líderes de proceso, empleados y grupos de interés relevantes, asegurando la consideración de diferentes perspectivas en la identificación, análisis y tratamiento de los riesgos.
- Uso de la mejor información disponible: Las decisiones relacionadas con la gestión de riesgos se fundamentan en información confiable, actualizada, verificable y oportuna.
- Factores humanos y culturales: Reconoce la influencia de la cultura organizacional, el comportamiento humano, las competencias y el liderazgo en la prevención y tratamiento de los riesgos.
- Dinamismo y adaptación al cambio: El sistema evoluciona conforme a cambios del entorno, del contexto organizacional, de los riesgos emergentes y de las necesidades estratégicas.
- Mejora continua: La gestión de riesgos se somete a procesos permanentes de evaluación, aprendizaje y fortalecimiento, incrementando progresivamente la madurez del sistema.

4. Definición del Contexto de la Organización

La comprensión del contexto organizacional constituye un elemento fundamental para la gestión integral de riesgos, en la medida en que los factores internos y externos pueden influir directamente en el logro de los objetivos estratégicos, la toma de decisiones y la sostenibilidad del negocio.

La identificación, análisis y actualización periódica del contexto se realizará de conformidad con lo establecido en el **Procedimiento de Planeación Directiva GPL-PLD-P-01** y en el **Instructivo Análisis del Contexto GPL-GPL-I-03,** así como mediante el análisis de partes interesadas por medio del **Instructivo Identificación y Análisis de Partes Interesadas GPL-GPL-I-04**.

Este análisis permitirá identificar tendencias, cambios regulatorios, factores económicos, tecnológicos, sociales, ambientales, competitivos y demás variables relevantes que puedan generar riesgos emergentes u oportunidades para la organización, incluyendo aquellos asociados a LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses, facilitando su identificación, análisis y gestión bajo el enfoque basado en riesgos.

Gestión de Oportunidades

Las oportunidades identificadas durante el análisis del contexto organizacional, así como aquellas que surjan en espacios estratégicos o instancias de decisión de la Alta Dirección, serán gestionadas mediante lo establecido en el **Procedimiento de Proyectos IDI-PYT-P-01**, asegurando su adecuada planeación, ejecución, seguimiento y control.

Por su parte, las oportunidades identificadas por los líderes de proceso u otras instancias organizacionales podrán ser evaluadas mediante la herramienta de gestión documental, considerando su nivel de urgencia de implementación en Alto, Medio y Bajo sobre los objetivos estratégicos, operacionales o de sostenibilidad.

5. Apetito, Tolerancia y Capacidad de Riesgo

INTER RAPIDÍSIMO S.A., define su apetito, tolerancia y capacidad de riesgo como parte integral del marco de referencia para la gestión de riesgos, con el propósito de orientar la toma de decisiones y establecer los niveles de exposición que la organización está dispuesta a asumir en el desarrollo de sus actividades.

Estos lineamientos permiten asegurar que la gestión del riesgo se mantenga alineada con los objetivos estratégicos, la continuidad del negocio, la sostenibilidad financiera y la generación de valor para la organización y sus grupos de interés.

La definición y actualización del **apetito y tolerancia del riesgo** será aprobada por la Junta Directiva, quien revisará periódicamente su pertinencia o cuando se presenten cambios relevantes en la estrategia corporativa, el contexto organizacional, el entorno regulatorio o eventos significativos que puedan modificar el perfil de riesgo de la organización.

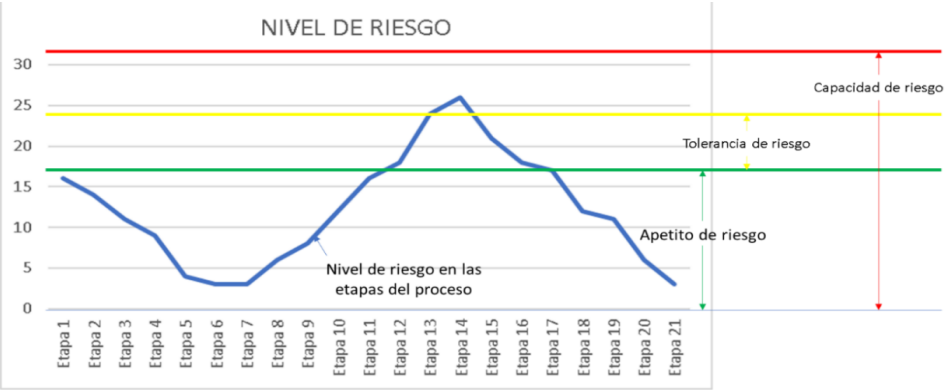
Para la adecuada gestión del riesgo, la organización considera los siguientes conceptos:

- **Apetito de riesgo:** Nivel y tipo de riesgo que la organización está dispuesta a asumir para alcanzar sus objetivos estratégicos y generar valor.
- **Tolerancia al riesgo:** Nivel de variación aceptable respecto al apetito de riesgo definido para un objetivo específico, permitiendo una operación dinámica sin comprometer la estrategia organizacional.

- **Capacidad de riesgo:** Límite máximo de riesgo que la organización puede soportar sin afectar su viabilidad financiera, operativa, legal, reputacional o estratégica.
- **Nivel de riesgo:** Resultado de la valoración obtenida mediante la metodología definida por la organización, considerando la probabilidad de ocurrencia y el impacto potencial del evento.

Estos conceptos constituyen la base para la definición de los criterios de aceptación del riesgo y permiten evaluar el nivel de riesgo residual, orientando decisiones relacionadas con el tratamiento, mitigación, transferencia, evitación o aceptación de los riesgos identificados.

Gráficamente, los anteriores conceptos se relacionan así:



Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

Criterios de Aceptación del Riesgo

Los criterios de aceptación del riesgo se establecen considerando el apetito y la tolerancia al riesgo definidos por la organización, así como los resultados de la valoración del riesgo residual obtenida mediante la metodología y matriz de riesgos vigentes.

Solo se aceptan riesgos residuales que se ubiquen en el nivel “Insignificante” en la matriz de calor (Nivel 1). Este es el nivel de Apetito de Riesgo formal de la organización.

Para el caso de los riesgos LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses, la tolerancia y nivel de aceptación del riesgo es cero (0).

Estos criterios permiten determinar cuándo un riesgo puede ser aceptado, monitoreado, tratado o escalado, con el fin de mantener los niveles de exposición dentro de los parámetros definidos por la organización. La aceptación de riesgos se determina con base en el **nivel de riesgo residual**, entendido como la exposición remanente una vez considerados los controles existentes.

De acuerdo con esta clasificación, los riesgos se gestionarán de la siguiente manera:

- **Nivel Insignificante (Dentro del Apetito de Riesgo):** Se consideran aceptables para la organización, y requerirán acciones de mejora, sin perjuicio del monitoreo rutinario y la validación de cambios en el contexto que puedan modificar su nivel de exposición.
- **Nivel Bajo (Dentro de la Tolerancia de Riesgo):** Se consideran administrables mediante controles estándar. Requieren seguimiento periódico y definir las acciones de mejora para asegurar su estabilidad y detectar variaciones relevantes.
- **Nivel Medio (Dentro de la Tolerancia al Riesgo):** Requieren seguimiento periódico, control continuo y evaluación preventiva, con el fin de evitar su incremento. Según su naturaleza y tendencia, se establecerán acciones de mejora o fortalecimiento de controles.
- **Nivel Alto (Fuera del Apetito y de la Tolerancia al Riesgo):** Requieren la implementación prioritaria de acciones de mejora orientadas a reducir su probabilidad o impacto, así como seguimiento reforzado y escalamiento a las instancias definidas por la organización cuando corresponda.
- **Nivel Significativo (Fuera de la Tolerancia de Riesgo):** Se consideran inaceptables para la organización y requieren intervención inmediata, definición de planes de mejoramiento, evaluación estratégica y escalamiento al Comité de Ética, Riesgos y Cumplimiento, Presidente Ejecutivo o Junta Directiva, según su impacto potencial.

El objetivo de estas acciones es reducir el riesgo residual hasta niveles que se encuentren dentro del apetito o tolerancia definidos por la organización.

Alineación entre Objetivos Estratégicos y Riesgos

La organización asegura la integración del enfoque basado en riesgos en la planeación estratégica, mediante la identificación y análisis de los riesgos que pueden afectar el cumplimiento de los objetivos organizacionales.

Para ello, los objetivos estratégicos deberán estar asociados a los riesgos relevantes que puedan impactar su logro, permitiendo su monitoreo a través de indicadores y facilitando la toma de decisiones informada. Esta alineación permite priorizar la gestión del riesgo, orientar la asignación de recursos y fortalecer el seguimiento al desempeño organizacional.

Los lineamientos específicos para esta articulación se desarrollarán a través de las herramientas de direccionamiento estratégico definidas por la organización, tales como el Balanced Scorecard, tableros de control, planes tácticos y demás mecanismos aplicables.

Herramientas de Control y Monitoreo

Con el fin de mantener los riesgos residuales dentro de los niveles definidos en el apetito y la tolerancia al riesgo, así como fortalecer la capacidad de respuesta de la organización frente a eventos adversos, **INTER RAPIDÍSIMO S.A.,** emplea diversas herramientas de control, seguimiento y monitoreo integradas al Sistema de Gestión de Riesgos.

Entre las principales herramientas se encuentran:

- **Matriz de Gestión de Riesgos y Oportunidades:** Herramienta que permite identificar, analizar, evaluar, priorizar y monitorear los riesgos asociados a los procesos, proyectos y actividades. Su representación mediante matrices de calor facilita la toma de decisiones frente a la aceptación, tratamiento o escalamiento de los riesgos identificados.
- **Indicadores Clave de Desempeño (KPIs) e Indicadores Clave de Riesgo (KRIs):** Métricas definidas para monitorear el desempeño organizacional, el comportamiento de los riesgos y la efectividad de los controles implementados, facilitando la identificación oportuna de desviaciones y la toma de decisiones para su gestión.
- **Reportes del Perfil de Riesgo:** Mecanismos periódicos de consolidación y análisis del estado de los riesgos identificados, tendencias, indicadores asociados y efectividad de controles, proporcionando información relevante para el Comité de Revisión por la Dirección y Auditoría, Presidente Ejecutivo, Junta Directiva y demás instancias de gobierno.
- **Planes de Mejoramiento y Tratamiento:** Herramientas orientadas a gestionar acciones correctivas, preventivas y de fortalecimiento de controles, enfocadas en reducir la exposición al riesgo y mejorar el desempeño organizacional.

6. Modelo de Gestión de Riesgos

La gestión integral de riesgos en **INTER RAPIDÍSIMO S.A.,** se desarrolla mediante una metodología estructurada, sistemática y continua, orientada a identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos que puedan afectar el logro de los objetivos organizacionales.

La metodología incorpora la valoración del riesgo inherente y del riesgo residual, considerando la efectividad de los controles existentes, la evolución del contexto y la necesidad de implementar acciones de tratamiento cuando corresponda. Así mismo, será aplicable de manera integral a los riesgos asociados a LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses, en el marco de SARLAFT, PTEE y buenas prácticas de SAGRILAFT, adoptados por la organización.

Las oportunidades identificadas serán gestionadas mediante los mecanismos definidos por la organización, conforme a lo establecido en el presente manual y en los procedimientos asociados.

Etapa 1: Identificación del Riesgo

La identificación del riesgo es una etapa proactiva y permanente cuyo propósito es reconocer eventos, circunstancias o situaciones que puedan afectar negativamente el cumplimiento de los objetivos organizacionales.

Durante esta etapa se identifican riesgos actuales, potenciales y emergentes asociados a los procesos, actividades, proyectos, activos, terceros y al entorno en el que opera la organización.

- Enfoque: La identificación deberá considerar riesgos inherentes a cada proceso, riesgos emergentes derivados de cambios del entorno, riesgos asociados a nuevas tecnologías, transformación digital, ciberseguridad, cambios regulatorios, mercado y continuidad del negocio.

- Responsables: La identificación de riesgos es responsabilidad de los líderes de proceso, con acompañamiento metodológico del equipo de procesos (SIGE) y del proceso de Cumplimiento según la naturaleza del riesgo.

- Criterios de Activación: La identificación o actualización de riesgos deberá realizarse, entre otros casos, cuando se presenten:

  - lanzamiento de nuevos productos o servicios;
  - ingreso a nuevos mercados;
  - adopción de nuevas tecnologías o sistemas de información;
  - cambios significativos en procesos o estructura organizacional;
  - incidentes relevantes o materialización de riesgos;
  - cambios regulatorios;
  - desarrollo de proyectos estratégicos o iniciativas de transformación.

Los proyectos estratégicos, iniciativas de transformación, implementaciones tecnológicas y demás proyectos relevantes, deberán incorporar la gestión de riesgos desde su formulación y durante el ciclo de vida del proyecto, teniendo en cuenta la **Matriz de Escalamiento GPL-PRO-F-08**, con el propósito de asegurar la gestión oportuna del riesgo, la toma de decisiones y la implementación de acciones de tratamiento.

Activos de Información

De conformidad con lo establecido en el **Instructivo de Inventario y Clasificación de Activos de Información GSI-GSI-I-01,** los líderes de proceso y responsables de cada área serán los responsables de identificar, clasificar, valorar y mantener actualizados los activos de información bajo su administración o uso, considerando su criticidad para la operación y el cumplimiento de los objetivos organizacionales.

El proceso de Seguridad de la Información actuará como responsable metodológico y técnico, brindando lineamientos, acompañamiento y seguimiento al proceso de gestión de activos de información, con el fin de asegurar la aplicación homogénea de los criterios definidos por la organización.

Así mismo, en conjunto con los responsables de los activos, se identificarán y evaluarán las amenazas y vulnerabilidades asociadas a la Confidencialidad, Integridad y

Disponibilidad (CID) de dichos activos, con el propósito de determinar los riesgos que puedan afectar la seguridad de la información y definir los controles correspondientes.

La información resultante se documentará en la **Matriz de Riesgos por Activos de Información GSI-GSI-R-87.** La clasificación y valoración de activos deberá revisarse periódicamente o cuando se presenten cambios relevantes en procesos, tecnología, regulación o criticidad del negocio.

De igual forma, aquellos riesgos asociados a los activos de información que puedan impactar los objetivos organizacionales deberán ser gestionados conforme a la metodología definida en el presente manual y registrados en la **Matriz de Riesgos GPL-PRO-R-03.**

Descripción y Estructura del Riesgo

Cada riesgo deberá redactarse de forma clara, concreta y sin ambigüedades, permitiendo comprender el evento que podría afectar el cumplimiento de los objetivos organizacionales, así como su contexto y posible impacto.

Evento de Riesgo

Situación, circunstancia o incidente potencial que puede materializarse y generar efectos adversos sobre el cumplimiento de los objetivos de la organización.

Causas del Riesgo

Factores internos o externos que, de manera individual o combinada, pueden originar la ocurrencia o materialización de un riesgo. La adecuada identificación de causas permite establecer controles preventivos y definir acciones orientadas a reducir la probabilidad de ocurrencia.

Consecuencias del Riesgo

Efectos o impactos que podrían generarse en caso de materialización del riesgo, afectando variables como operación, cumplimiento, finanzas, reputación, seguridad, servicio o continuidad del negocio.

Consideraciones Generales

- Durante la identificación de riesgos se deberán tener en cuenta los siguientes criterios:
- La ausencia de control no constituye un riesgo, sino una condición que puede incrementar la probabilidad o el impacto del evento identificado.
- Cada riesgo identificado deberá asociarse, en la medida de lo posible, a un Macroproceso, Proceso, Subproceso, proyecto o activo relevante, con el fin de facilitar su gestión, trazabilidad y seguimiento.

La redacción del riesgo deberá diferenciar claramente entre causa, evento y consecuencia.

Categoría del Riesgo

Con el fin de facilitar la clasificación y gestión de los riesgos identificados, la organización establece diferentes categorías de riesgo, las cuales permiten categorizar el tipo de exposición al que se encuentra expuesta la compañía, de acuerdo con el origen, características y posibles efectos derivados de su materialización.

La definición de la categoría del riesgo será realizada por el líder del proceso o experto responsable, considerando el contexto del riesgo identificado y su posible afectación sobre la organización.

- **Normativo:** Exposición de la organización frente a posibles incumplimientos, desviaciones o inobservancia de disposiciones regulatorias, lineamientos normativos y requerimientos emitidos por entes de vigilancia y control.

- **Legal:** Exposición de la organización frente a consecuencias jurídicas, contractuales o coercitivas derivadas del incumplimiento de obligaciones legales, regulatorias o contractuales.

- **Económico:** Exposición de la organización frente a pérdidas económicas, afectaciones financieras o disminución patrimonial derivadas de la materialización de un riesgo.

- **Liquidez:** Exposición de la organización frente a limitaciones en la disponibilidad de recursos financieros o flujo de caja que afecten el cumplimiento oportuno de sus obligaciones operativas y financieras.

- **Reputacional:** Exposición de la organización frente al deterioro de la imagen, credibilidad, confianza y buen nombre corporativo ante sus grupos de interés.

- **Operacional:** Exposición de la organización frente a interrupciones, fallas, retrasos o afectaciones en la ejecución de sus procesos y prestación de servicios.

- **Contagio:** Exposición de la organización frente a afectaciones generadas por actuaciones, relaciones o situaciones asociadas a terceros o contrapartes vinculadas.

- **SARLAFT:** Exposición de la organización frente a la posibilidad de ser utilizada directa o indirectamente para actividades relacionadas con el Lavado de Activos, la Financiación del Terrorismo y/o el Financiamiento de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM), derivadas de relaciones, operaciones, productos, servicios, canales o contrapartes vinculadas.

- **PTEE:** Exposición de la organización frente a posibles actos de corrupción, soborno transnacional, fraude o conductas contrarias a la ética y transparencia empresarial, que puedan generar afectaciones legales, económicas, reputacionales y de cumplimiento.

- **Tecnológico:** Exposición de la organización frente a fallas, obsolescencia, indisponibilidad o deficiencias en la infraestructura tecnológica, sistemas de información, aplicaciones o herramientas tecnológicas que soportan la operación del negocio.

- **Seguridad de la Información:** Exposición de la organización frente a la pérdida de confidencialidad, integridad y disponibilidad de la información, así como accesos no autorizados, incidentes de ciberseguridad o vulnerabilidades que afecten los activos de información de la compañía.

Etapa 2: Valoración del Riesgo

La valoración del riesgo tiene como propósito analizar y comprender la naturaleza de los riesgos identificados, sus causas, consecuencias y la probabilidad de ocurrencia, con el fin de facilitar la toma de decisiones sobre su tratamiento, priorización y control, incluyendo aquellos asociados a LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses .

La evaluación del riesgo se realiza mediante la determinación de la probabilidad de ocurrencia y el impacto en caso de materializarse el evento, bajo un enfoque basado en riesgos y conforme a las metodologías definidas por la organización.

Este proceso se desarrolla con base en la mejor información disponible y constituye una responsabilidad compartida entre los líderes de proceso, el equipo de procesos (SIGE) y el proceso de Cumplimiento, conforme a sus roles dentro del sistema de gestión de riesgos.

La valoración inicia con el análisis del riesgo inherente, entendido como el nivel de exposición existente antes de considerar la eficacia de los controles implementados, y constituye la base para la determinación del riesgo residual.

Paso 1: Análisis del Riesgo Inherente

El riesgo inherente corresponde al nivel inicial de exposición al riesgo y se determina mediante la combinación entre la probabilidad de ocurrencia y el impacto potencial del evento, conforme a la metodología y escalas definidas por la organización. Se calcula multiplicando la probabilidad de ocurrencia por el impacto potencial.

A. Probabilidad de Ocurrencia

Representa la posibilidad de que un evento de riesgo se materialice dentro de un periodo determinado. Su estimación deberá realizarse con base en información objetiva, histórico de eventos, condiciones actuales del proceso, tendencias del entorno y juicio experto.

Para su determinación podrán emplearse la siguiente valoración:

Escala de Probabilidad: La probabilidad corresponde a la posibilidad de que el riesgo ocurra, considerando antecedentes, indicadores del proceso, frecuencia, entorno operativo, controles existentes y comportamiento histórico.

Para calificar la probabilidad, se tomará como base el nivel de exposición al riesgo inherente al proceso o actividad correspondiente, aplicando los siguientes criterios:

Nivel	Valoración	Porcentaje
5	Casi Seguro	81% - 100%
4	Probable	61% - 80%
3	Posible	41% - 60%
2	Improbable	21%- 40%
1	Rara vez	0% - 20%

B. Impacto

El análisis de impacto permite determinar la naturaleza, alcance y magnitud de las consecuencias que podrían generarse en caso de materialización de un riesgo. Un mismo evento puede afectar simultáneamente distintos objetivos organizacionales, procesos, recursos y grupos de interés.

Para su valoración se analizarán, entre otros aspectos:

- Los factores internos y externos que puedan influir en la materialización del riesgo o en la severidad de sus efectos.
- Las consecuencias inmediatas como aquellas que puedan presentarse de forma posterior o acumulativa (consecuencias secundarias).

La evaluación del impacto se realizará de acuerdo con los siguientes criterios:

Nivel	Valoración	Porcentaje
5	Catastrófico	81% - 100%
4	Mayor	61% - 80%
3	Moderado	41% - 60%
2	Menor	21%- 40%
1	Leve	0% - 20%

C. Riesgo Inherente

Corresponde al nivel inicial de exposición de la organización frente a un evento de riesgo, antes de considerar la eficacia de los controles existentes.

Su valoración resulta de la combinación entre el nivel de probabilidad de ocurrencia y el nivel de impacto potencial, conforme a las escalas definidas en la presente metodología. El puntaje obtenido determinará su clasificación de severidad y servirá como base para el análisis posterior del riesgo residual.

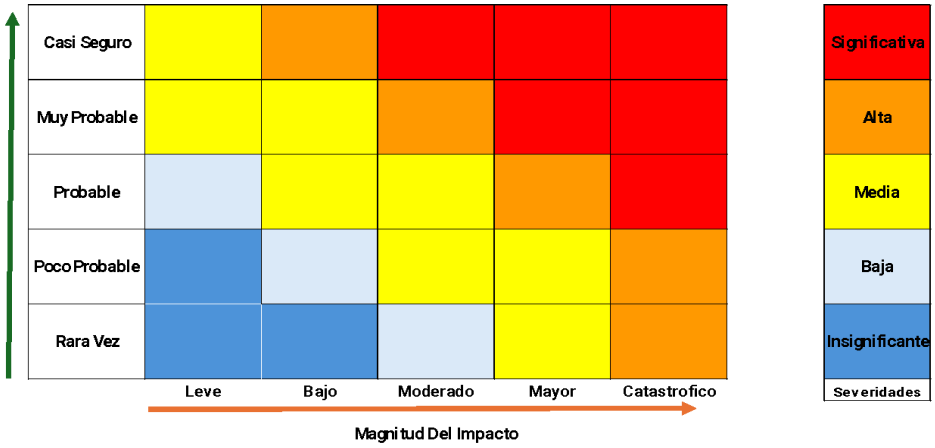
Severidad del Riesgo

La severidad del riesgo corresponde al nivel de exposición de la organización frente a un evento de riesgo, determinado por la combinación entre la probabilidad de ocurrencia y el impacto potencial, conforme a la metodología definida por la organización.
Los niveles de severidad establecidos son los siguientes:

	Severidad Significativa: Riesgos con capacidad de impedir el logro de objetivos estratégicos clave, generar impactos críticos en la operación, afectar la continuidad del negocio o producir consecuencias severas para la organización.
	Severidad Alta: Riesgos con potencial de generar disrupciones importantes en la operación, afectar significativamente los resultados o comprometer de manera relevante el cumplimiento de los objetivos.
	Severidad Media: Riesgos que pueden generar desviaciones moderadas en el cumplimiento de los objetivos, pero que pueden ser gestionados mediante controles adicionales, acciones correctivas o seguimiento reforzado.
	Severidad Baja: Riesgos con impacto limitado y baja probabilidad de ocurrencia, administrables mediante controles estándar y seguimiento periódico.
	Severidad insignificante: Riesgos cuyo impacto es bajo y se consideran aceptables dentro de los niveles definidos por la organización.

Valoración	Porcentaje
Significativo	60% - 100%
Alto	40% -48%
Medio	17% - 36%
Bajo	11% - 16%
Insignificante	0%- 10%

La severidad del riesgo se representa gráficamente en el **Mapa de Calor,** la cual permite visualizar el nivel de exposición del riesgo y determinar si este se encuentra dentro del apetito, dentro de la tolerancia o fuera de los límites aceptables definidos por la organización.



Etapa 3: Control del Riesgo

Una vez valorado el riesgo inherente, la siguiente etapa consiste en analizar y evaluar los controles existentes implementados por la organización para gestionar los riesgos identificados, incluyendo aquellos asociados a LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses

El propósito de esta fase es determinar la **eficacia real de los controles** y calcular el **riesgo residual**, entendido como el nivel de exposición remanente después de la aplicación de dichos controles.

A. Evaluación del Diseño y Eficacia de los Controles

Esta etapa evalúa la solidez de los controles implementados, considerando tanto su diseño como su operación efectiva. La adecuada identificación, documentación y valoración de los controles constituye un elemento fundamental para obtener una medición confiable del riesgo residual.

Los controles definidos por la organización deberán ser integrales y estar alineados con la naturaleza de los riesgos identificados, garantizando su adecuada cobertura sobre las causas, eventos y consecuencias asociadas.

Así mismo, deberán diseñarse e implementarse de manera que aseguren su funcionamiento oportuno, efectivo y eficiente, contribuyendo a la reducción de la probabilidad de ocurrencia o a la mitigación del impacto en caso de materialización del riesgo.

Diseño del Control

Para efectos de la presente metodología, el diseño del control evalúa si el mecanismo implementado es adecuado para gestionar la causa, evento o consecuencia del riesgo identificado. En dicha evaluación se considerarán, entre otros aspectos:

- Claridad del objetivo del control.

- Responsable definido.
- Frecuencia de ejecución.
- Evidencia disponible.
- Cobertura frente al riesgo.
- Oportunidad de aplicación.

Tipos de Control y Afectación del Riesgo

Los controles se clasifican según su propósito y el momento en que actúan sobre el riesgo, impactando su probabilidad de ocurrencia o la magnitud de sus consecuencias:

Tipo de Control	Propósito	Afectación de Probabilidad	Afectación de Impacto
Preventivo	Reduce la probabilidad de ocurrencia del evento mediante la disminución de vulnerabilidades o causas	Disminuye	No Disminuye
Detectivo	Permite detectar el evento una vez ocurrido, facilitando la activación de acciones oportunas que reducen sus consecuencias.	No Disminuye	Disminuye
Correctivo	Permite corregir o mitigar las consecuencias del evento una vez materializado, reduciendo su impacto.	No Disminuye	Disminuye

Valoración de la Eficacia del Control

La eficacia de cada control se determinará mediante criterios objetivos asociados a su diseño, nivel de formalización y ejecución operativa, conforme a los parámetros definidos por la organización.

Esta evaluación permitirá establecer el grado real de contribución del control en la reducción de la probabilidad de ocurrencia o del impacto del riesgo identificado.

Para la valoración de la eficacia se considerarán, como mínimo, los siguientes criterios:

Criterio	Peso Máximo	Variables de Valoración
Automatización	5	Manual (1), Semiautomático (3), Automático (5).
Documentación	5	No Documentado (1), Documentado (5) en el SIGE.

Criterio	Peso Máximo	Variables de Valoración
Periodicidad	5	Bianual (0), Anual (0.5), Semestral (1), Trimestral (2), Bimestral (2.5), Mensual (3), Quincenal (3.5), Semanal (4), Diaria (5), A demanda (4.5).

Cuando existan múltiples controles asociados a una misma variable (probabilidad o impacto), la eficacia aplicable se calculará mediante el promedio de los valores asignados a los controles que afectan dicha variable.

De esta manera, la organización podrá determinar de forma específica:

- La reducción aplicable a la probabilidad, con base en los controles de tipo preventivo.
- La reducción aplicable al impacto, con base en los controles de tipo detectivo y correctivo.

La existencia documental del control no garantiza su eficacia; será necesario validar su ejecución periódica y la disponibilidad de evidencias objetivas. En caso de no demostrarse su aplicación efectiva, la organización podrá ajustar su calificación o considerarlo no efectivo para efectos de la valoración del riesgo residual.

B. Determinación del Riesgo Residual

El riesgo residual corresponde al nivel de riesgo que permanece después de considerar la eficacia de los controles implementados y representa la exposición real de la organización frente al riesgo.

Su determinación tiene como propósito garantizar que los niveles de riesgo residual se mantengan dentro de los criterios de aceptación definidos por la organización, en coherencia con el apetito y la tolerancia al riesgo establecidos, permitiendo orientar la toma de decisiones sobre su tratamiento, monitoreo o aceptación.

Decisión Estratégica: El riesgo residual obtenido se comparará con los niveles definidos en el **apetito y la tolerancia al riesgo**.

- Si el riesgo se encuentra **dentro del apetito**, podrá ser aceptado.
- Si se encuentra **dentro de la tolerancia**, deberá ser monitoreado y gestionado.
- Si se encuentra **fuera de la tolerancia**, deberá ser tratado mediante acciones de mitigación, transferencia, evitación o fortalecimiento de los controles.

Cuando el riesgo residual se mantenga en niveles no aceptables o presente tendencia creciente, deberá ser escalado a las instancias de gobierno definidas por la organización para la toma de decisiones correspondientes.

Etapa 4: Tratamiento del Riesgo

El tratamiento del riesgo es la etapa mediante la cual la organización define, aprueba e implementa las acciones necesarias para modificar el nivel de riesgo residual, con el propósito de llevarlo a niveles aceptables, en coherencia con el apetito y la tolerancia al riesgo aprobados por la Junta Directiva.

Este proceso permite fortalecer los controles existentes, reducir la exposición al riesgo, aprovechar capacidades organizacionales y contribuir a la continuidad, sostenibilidad y cumplimiento de los objetivos estratégicos. Para ello, la organización desarrollará, entre otras, las siguientes actividades:

- Identificación de la Causa Raíz: Analizar y determinar las causas que originan o favorecen la materialización del riesgo, con el fin de intervenirlas de manera efectiva y sostenible.
- Análisis de Desviaciones: Identificar situaciones, condiciones, fallas o variaciones del proceso normal que puedan contribuir a la ocurrencia del riesgo.
- Propuesta de Tratamiento: Definir la estrategia más adecuada para gestionar el riesgo, considerando su nivel de exposición, impacto y el análisis costo-beneficio de las acciones con base en:

Opción de Tratamiento	Descripción	Ejemplo
Evitar el riesgo	Modificar o eliminar actividades para que el riesgo no pueda ocurrir.	Cancelar el lanzamiento de un nuevo servicio si implica incumplir requisitos regulatorios o superar la capacidad de endeudamiento.
Mitigar el riesgo	Implementar controles o acciones que disminuyan la probabilidad de ocurrencia o el impacto del riesgo.	Mejorar los procesos de verificación de clientes y proveedores para reducir el riesgo de lavado de activos o fraude.
Transferir el riesgo	Pasar el riesgo a un tercero (total o parcialmente), generalmente mediante seguros, contratos o garantías.	Contratar seguros de responsabilidad civil, seguros de transporte de mercancía, o incluir cláusulas de indemnización en contratos.
Aceptar el riesgo	Asumir el riesgo cuando su nivel es bajo o el costo de mitigación es mayor	Aceptar retrasos ocasionales en entregas de última milla en zonas rurales, porque el costo de mitigarlo sería mayor que la pérdida.

La organización podrá gestionar los planes de tratamiento asociados a riesgos de mayor exposición como iniciativas estratégicas o proyectos, integrándolos con los mecanismos de planeación y gestión de proyectos, con el fin de asegurar su priorización, asignación de recursos, seguimiento y trazabilidad.

Planificación y Ejecución Operativa:

Las acciones definidas para el tratamiento del riesgo deberán formalizarse mediante planes de mejoramiento, según lo establecido en el **Procedimiento de Planes de Mejoramiento GPL-PRO-P-07**, los cuales constituyen el mecanismo para asegurar la ejecución, seguimiento y trazabilidad de las medidas aprobadas por la organización.

Dichos planes deben contener la siguiente información:

- Planes de Mejoramiento: Actividades específicas orientadas a eliminar, reducir, transferir o controlar el riesgo identificado.
- Entregables: Documentos, registros, soportes o resultados verificables derivados de la implementación de las acciones definidas.
- Responsable de implementación: Persona o rol encargado de ejecutar las acciones.
- Responsable de autorización: Líder de proceso o instancia competente que aprueba el plan de tratamiento y valida su pertinencia
- Activos de información asociados (ISO 27001): Se detallan los activos de información relacionados con el riesgo, cuando se aplique.
- Cronograma: Fecha de inicio y fecha de finalización del plan de mejoramiento.
- Estado de implementación: No iniciado, en ejecución, retrasado o finalizado.
- Indicador de seguimiento (cuando aplique): Métrica definida para evaluar el avance o efectividad de la acción implementada.

La ejecución de los planes de tratamiento deberá monitorearse a través de la herramienta de gestión documental definida por la organización, verificando fechas de cumplimiento, calidad de entregables, avance de actividades y efectividad de las acciones implementadas.

Cuando se evidencien retrasos, incumplimientos o resultados no efectivos, deberán definirse acciones complementarias, ajustes al plan o escalamiento a las instancias correspondientes.

Niveles de Aceptación del Riesgo

Los niveles de aceptación del riesgo definen el tratamiento requerido, la intensidad del monitoreo y el nivel de escalamiento aplicable a los riesgos residuales, de acuerdo con su ubicación en la matriz de calor y en coherencia con el apetito y la tolerancia al riesgo establecidos por la organización.

Tipo de Riesgo	Zona de Riesgo	Opciones de Tratamiento	Color (Semáforo)
Insignificante	Zona de Aceptación	**Aceptar.** No requiere acciones adicionales, sin perjuicio del	Azul

Tipo de Riesgo	Zona de Riesgo	Opciones de Tratamiento	Color (Semáforo)
		monitoreo rutinario y validación de cambios de contexto.	
Bajo	Zona de Aceptación Controlada	**Mantener controles existentes y seguimiento periódico**. Podrán implementarse mejoras preventivas cuando aplique.	Azul
Medio	Zona de Tolerancia y Advertencia	**Monitorear y gestionar.** Reforzar controles, establecer acciones preventivas o planes de mejora según tendencia del riesgo.	Amarillo
Alto	Zona Inaceptable (Fuera del apetito y tolerancia)	**Evitar o Transferir.** Eliminar la actividad que lo origina o trasladar el impacto. Escalar al Comité de Ética, Riesgos y Cumplimiento para su aprobación.	Naranja
Significativo	Zona Inaceptable Extrema (Fuera del apetito y tolerancia)	**Evitar o Mitigar al máximo.** Si el riesgo es inherente a una actividad crítica, escalar al Comité de Revisión por la Dirección y Auditoría o Junta Directiva para su Aceptación Excepcional o para la definición de acciones estratégicas	Rojo

Nota: Los riesgos asociados a LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses corrupción, fraude, soborno y LA/FT/FPADM se consideran de especial atención y deberán gestionarse conforme a los lineamientos de cumplimiento definidos por la organización, independientemente de su calificación residual.

Persistencia de Riesgos en Niveles No Aceptables

Cuando, una vez implementadas las medidas de tratamiento definidas, un riesgo continúe ubicado en niveles no aceptables o por fuera de la tolerancia establecida por la organización, deberán activarse mecanismos formales de análisis, decisión y escalamiento ante las instancias competentes.

El reporte inicial deberá ser comunicado por el Líder de Proceso al proceso de Cumplimiento, mediante correo electrónico, adjuntando el análisis técnico y los soportes correspondientes.

En estos casos se seguirá el siguiente esquema de actuación:

- **Sustentación técnica:** El Líder de Proceso deberá presentar al proceso de Cumplimiento la justificación de la persistencia del riesgo, incluyendo causas identificadas, controles implementados, resultados obtenidos, impactos potenciales y limitaciones para su mitigación.
- **Revisión y decisión del Comité de Ética, Riesgos y Cumplimiento:** El proceso de Cumplimiento presentará ante el Comité, órgano que evaluará la situación y podrá definir medidas adicionales, fortalecer controles existentes, aprobar nuevos planes de tratamiento, establecer controles compensatorios o solicitar análisis complementarios.
- **Escalamiento superior:** Cuando el riesgo continúe en niveles no aceptables, comprometa objetivos estratégicos o supere la capacidad de respuesta definida por la organización, será escalado al Presidente de la organización para la definición de acciones estratégicas, incluyendo aceptación excepcional, transferencia, suspensión de actividades, redefinición operativa, reasignación de recursos y activación de planes de continuidad. En caso de continuar en niveles aceptables se deberá reportar a la Junta Directiva.
- **Registro y trazabilidad:** Toda decisión adoptada respecto a la aceptación excepcional, continuidad del riesgo, nuevos tratamientos o escalamiento deberá quedar formalmente documentada en el formato **Acta de Aceptación Excepcional del Riesgo GPL-PRO-R-22**, garantizando trazabilidad, responsables, vigencia de la decisión y compromisos derivados.
- **Actualización metodológica:** Con base en la decisión aprobada por el Comité de Ética, Riesgos y Cumplimiento, Presidente Ejecutivo y/ o Junta Directiva, deberá ser notificada el área de Procesos (SIGE) quién realizará la actualización correspondiente en la **Matriz de Riesgos GPL-PRO-R-03** y efectuará el seguimiento respectivo.

Convocatoria Extraordinaria Comité de Ética, Riesgos y Cumplimiento

Cuando un riesgo permanezca en niveles no aceptables, presente una condición de alta criticidad o pueda generar impactos relevantes sobre la operación, la continuidad del negocio, el cumplimiento normativo, la seguridad de la información (CID) y en situaciones relacionadas con LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses se deberá solicitar la realización de un comité extraordinario, con el fin de analizar la situación y definir las acciones correspondientes.

Etapa 5: Monitoreo, Seguimiento y Mejora del Riesgo

El monitoreo, seguimiento y mejora del riesgo constituyen un proceso continuo y sistemático orientado a evaluar la eficacia de los controles implementados, verificar el cumplimiento de los niveles de riesgo definidos y fortalecer permanentemente el sistema de gestión de riesgos, incluyendo aquellos asociados a LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses.

Este proceso contempla el seguimiento periódico y comparativo del riesgo inherente y del riesgo residual, con el fin de evaluar la efectividad de los controles, identificar desviaciones y asegurar que los niveles de exposición se mantengan dentro del apetito y la tolerancia al riesgo definidos por la organización.

A través del proceso de Cumplimiento, la organización realiza seguimiento al comportamiento de los riesgos, analizando sus causas, tendencias y controles, con el fin de fortalecer la toma de decisiones, gestionar riesgos emergentes y asegurar la alineación con el contexto estratégico, normativo, tecnológico y operativo de la organización.

Responsabilidad del Monitoreo: El monitoreo es responsabilidad permanente de los líderes de los procesos, quienes junto con sus equipos deberán asegurar la revisión periódica de los riesgos bajo su gestión y enfocarse en los siguientes aspectos:

- Validación y Eficacia: Verificar de manera continua la eficacia de los controles, tanto en su diseño como en su operación, asegurando que los riesgos permanezcan dentro de niveles aceptables.
- Aprendizaje Organizacional: Analizar eventos, incidentes, cambios y tendencias, incluyendo riesgos materializados, con el fin de generar lecciones aprendidas que fortalezcan la gestión futura.
- Anticipación y Adaptación: Detectar cambios en el contexto interno y externo para identificar riesgos emergentes o modificaciones en el perfil de riesgo de la organización.
- Monitoreo Integral del Riesgo: Incluir en el seguimiento no solo los riesgos de alta exposición, sino también aquellos clasificados como bajos o menores, con el fin de identificar tendencias, patrones y señales tempranas que puedan evolucionar en el tiempo.
- Gestión de la Mejora: Definir e implementar nuevos controles y realizar seguimiento a la ejecución de los planes de tratamiento, verificando su avance y efectividad.

A. Objetivos del Seguimiento del Riesgo

El seguimiento y monitoreo de la gestión de riesgos permite:

- Exposición: Realizar seguimiento prioritario a los riesgos residuales ubicados por encima de los niveles de tolerancia definidos, especialmente aquellos clasificados como Alto o Significativo.
- Gestión de Planes de Mejoramiento: Verificar el estado de avance y evaluar la efectividad de los planes implementados, definiendo acciones adicionales cuando se requiera.
- Aprendizaje y Conectividad: Analizar riesgos previamente gestionados y validar si las acciones implementadas contribuyen a mitigar riesgos similares, relacionados o recurrentes.
- Toma de decisiones: Proveer información oportuna y confiable para apoyar decisiones operativas, tácticas y estratégicas.

B. Trazabilidad y Documentación

El seguimiento de los planes de mejoramiento estará a cargo del proceso de Cumplimiento, por medio de la herramienta de gestión de documental, que incluye:

- Verificación: Cada plan de mejoramiento debe tener su responsable de verificación y la fecha de seguimiento.
- Estado: Control del avance de los planes (No iniciado, en ejecución, retrasado o finalizado).
- Evidencia: Evaluación de la efectividad de las acciones implementadas, con base en la calidad y oportunidad de las evidencias.
- Eficacia: Validación del resultado obtenido con la implementación de las acciones definidas.
- Reapertura: En caso de que un plan de mejoramiento no sea efectivo, deberá reabrirse, definiendo nuevas acciones, responsables y plazos para su implementación, con base en lo definido en el **Procedimiento de Planes de Mejoramiento GPL-PRO-P-07.**

Reporte y Escalamiento de Riesgos

Este apartado define los mecanismos de reporte y escalamiento de los riesgos, en función de su nivel de exposición y en coherencia con los límites de apetito y tolerancia al riesgo definidos por la organización.

El reporte y escalado de riesgos se realizará a través de **informes estructurados de gestión del riesgo**, los cuales consolidan la información relevante sobre el perfil de riesgo, el estado de los controles, la evolución de los riesgos, acciones de tratamiento y demás aspectos necesarios para la toma de decisiones por parte de las instancias de gobierno.

Estos informes podrán ser de carácter **periódico o extraordinario**, dependiendo del nivel de exposición y criticidad del riesgo.

Mecanismos de Reporte y Escalado General

Condición de Riesgo	Frecuencia de Reporte	Destinatario de la Escalada
Reporte ejecutivo que incluye el análisis consolidado del perfil de riesgo, tendencias, riesgos emergentes, evaluación de la efectividad del sistema de gestión de riesgos y recomendaciones estratégicas.	Mensual	Comité de Ética, Riesgos y Cumplimiento
Informe que integre la evolución del sistema de gestión de riesgos, el comportamiento del perfil de riesgo y las principales conclusiones para la toma de decisiones estratégicas.	Cada "Q (Quarter)"	Comité de Revisión por la Dirección y Auditoría

Nota: Los reportes de gestión de riesgos deben incluir el seguimiento a indicadores, análisis de tendencias, riesgos emergentes, materializaciones significativas, estado de planes de tratamiento y, cuando aplique, aspectos relacionados con la cultura de gestión del riesgo.

C. Acciones a Seguir ante Materialización o Cambio de Nivel de Riesgo

Cuando se identifique un riesgo fuera de los niveles de aceptación definidos o se presente su materialización, deberán activarse oportunamente los siguientes mecanismos de reporte, gestión, análisis y escalamiento correspondientes.

Reporte inicial: El Líder de Proceso deberá reportar mediante correo electrónico el evento o cambio en el nivel de riesgo, en un plazo máximo de **dos (2) días hábiles**, al proceso de Cumplimiento, adjuntando la información disponible al momento del reporte**.**

El reporte deberá incluir como mínimo

- Descripción del evento o cambio en el nivel de riesgo.
- Análisis preliminar de causas.
- Impacto generado o potencial.
- Controles afectados.
- Acciones inmediatas implementadas.
- Propuesta de plan de tratamiento.

Este registro se realizará a través del formato de **Registro y Gestión de Eventos de Riesgo GPL-PRO-R-23**, garantizando la trazabilidad de la información.

Revisión del Plan: El proceso de Cumplimiento realizará la revisión del reporte y del plan de tratamiento propuesto, verificando su coherencia con la metodología definida en el presente manual, nivel de exposición, su alineación con los objetivos organizacionales, suficiencia de las acciones planteadas y necesidad de escalamiento adicional.

Escalamiento y aprobación: Una vez surtida la validación técnica por parte del Proceso Cumplimiento, el caso será presentado al Comité de Ética, Riesgos y Cumplimiento para su análisis, validación y aprobación del plan de tratamiento, cuando aplique según la criticidad del riesgo.

Cuando la situación represente alta criticidad, afectación significativa a la operación, continuidad del negocio, cumplimiento regulatorio o seguridad de la información, se podrá solicitar la convocatoria extraordinaria del Comité de Ética, Riesgos y Cumplimiento.

Formalización y Registro: Posterior a la aprobación del Comité de Ética, Riesgos y Cumplimiento, el Líder de Proceso deberá formalizar el plan de tratamiento mediante el formato de **Registro y Gestión de Eventos de Riesgo GPL-PRO-R-23**, el cual deberá estar firmado por las partes correspondientes.

Así mismo, el plan de mejoramiento será registrado por el proceso de Cumplimiento en la herramienta de gestión documental, de conformidad con los lineamientos establecidos en el **Procedimiento de Planes de Mejoramiento GPL-PRO-P-07**, garantizando la trazabilidad, seguimiento y control de las acciones definidas.

Actualización matriz de riesgos: Con base en la decisión adoptada y las acciones aprobadas, el Líder de Proceso, en conjunto con el Gestor de Proceso, actualizarán la **Matriz de Riesgos GPL-PRO-R-03** reflejando los cambios derivados de la materialización del riesgo, la nueva valoración del nivel de exposición y los tratamientos definidos.

Verificación y Control

Las áreas de Auditoría Interna, Cumplimiento y Seguridad de la Información según su ámbito de competencia, podrán verificar periódicamente la gestión de riesgos mediante auditorías, revisiones, monitoreos o evaluaciones independientes que incluyan:

- El cumplimiento de los controles definidos.
- Eficacia de los controles implementados.
- La correcta implementación de los cambios realizados.
- Oportunidad en el tratamiento de hallazgos y eventos materializados.

Cuando se identifican incumplimientos, debilidades de control u oportunidades de mejora, se deberán generar planes de mejoramiento conforme al **Procedimiento de Planes de Mejoramiento GPL-PRO-P-07**, los cuales deberán ser ejecutados y reportados por los Líderes de Proceso hasta su cierre efectivo.

D. Actualización y Revisión Periódica del Riesgo

Con el propósito de mantener actualizado el perfil de riesgo de la organización, asegurar la vigencia de los controles implementados y dar cumplimiento a los requisitos normativos aplicables, deberán realizarse procesos periódicos de validación, revisión y actualización de la información asociada a la gestión de riesgos.
La actualización del riesgo podrá originarse por revisiones programadas o por cambios relevantes en el contexto interno o externo de la organización.

Certificación Trimestral GPL-PRO-R-08: En el marco de los ejercicios periódicos de certificación, revisión o seguimiento definidos por la organización, cada proceso deberá:

- Validar si los riesgos identificados continúan vigentes o requieren modificación.
- Revisar si las causas, consecuencias, controles y valoraciones registradas permanecen actualizadas.
- Identificar nuevos riesgos, riesgos emergentes u oportunidades de mejora derivadas de cambios operacionales, tecnológicos, regulatorios o estratégicos.

Actualización: Cuando se requieran ajustes en riesgos, controles o valoraciones, el Gestor de Proceso asignado apoyará al Líder de Proceso en la estructuración de la solicitud de cambio y en la documentación correspondiente, conforme a los mecanismos definidos por la organización.

Notificación: Cualquier modificación o actualización, se deberá notificar al proceso de Cumplimiento.

Aprobación e Implementación: El Comité de Ética, Riesgos y Cumplimiento o la instancia competente analizará las novedades presentadas y aprobará los cambios que correspondan.

Con la aprobación respectiva:

- Los Líderes de Proceso deberán implementar las acciones requeridas y actualizar, cuando aplique, manuales, políticas, procedimientos y controles asociados.
- El área de Procesos, en conjunto con el Líder de Proceso, actualizará la **Matriz de Riesgos GPL-PRO-R-03**, garantizando consistencia metodológica y trazabilidad de los cambios realizados.
- Se divulgará los procesos involucrados y gestionarán las capacitaciones requeridas.

Seguimiento posterior: Una vez implementados los cambios, la organización realizará seguimiento a su efectividad, verificando que las modificaciones incorporadas reduzcan la exposición al riesgo y mantenga alineado el perfil de riesgo con los objetivos organizacionales.

E. Gestión de Nuevos Riesgos

Con el fin de garantizar la gestión oportuna de riesgos emergentes o no identificados previamente, la organización establece el siguiente lineamiento para la identificación, registro y escalamiento de nuevos riesgos:

Cuando un Líder de Proceso, colaborador o instancia organizacional identifique un nuevo riesgo que pueda afectar el cumplimiento de los objetivos, deberá:

- Informar oportunamente al proceso de Cumplimiento, adjuntando la descripción del riesgo, sus posibles causas, consecuencias y contexto de identificación.
- Realizar un análisis preliminar del riesgo, incluyendo una valoración inicial de probabilidad e impacto, con el acompañamiento del equipo de Procesos cuando aplique.
- Gestionar el registro del riesgo en la **Matriz de Riesgos GPL-PRO-R-03**, asegurando su trazabilidad y consistencia metodológica.

Una vez registrado:

- El riesgo deberá ser presentado al Comité de Ética, Riesgos y Cumplimiento para su análisis, validación y aprobación.
- El Comité definirá la necesidad de tratamiento, priorización, escalamiento o integración del riesgo dentro del perfil de riesgo organizacional.

Posterior a su aprobación:

- El Líder de Proceso será responsable de implementar las acciones requeridas para su gestión.

- El proceso de Cumplimiento realizará seguimiento a su evolución y asegurará su integración en los reportes del perfil de riesgo organizacional.

Este mecanismo permite asegurar una gestión dinámica, anticipativa y alineada con los cambios del entorno, fortaleciendo la capacidad de respuesta de la organización frente a riesgos emergentes.

F. Gestión de Indicadores de Riesgo y Desempeño

La organización cuenta con un sistema de indicadores orientado a medir y monitorear periódicamente el comportamiento de los riesgos, la eficacia de los controles y el avance de los planes de tratamiento, como parte integral del Sistema de Gestión de Riesgos.

Estos indicadores permiten identificar desviaciones, tendencias y alertas tempranas, facilitando la toma de decisiones y la mejora continua, con el fin de mantener los niveles de riesgo dentro del apetito y la tolerancia definidos por la organización.

Los indicadores deberán contar con definición, fórmula, frecuencia de medición, responsables, metas y criterios de análisis, conforme a los lineamientos corporativos establecidos.

Su administración y control se realizará mediante la **Ficha Técnica de Indicadores GPL-PRO-R-06.**

Los resultados serán revisados periódicamente y, cuando evidencien desviaciones relevantes o tendencias negativas, deberán generar las acciones de análisis, tratamiento o escalamiento correspondientes.

7. Gobernanza del Riesgo

La gestión integral de riesgos en **INTER RAPIDÍSIMO S.A.,** se fundamenta en el modelo de las **Tres Líneas**, orientado a asegurar una adecuada segregación de funciones, rendición de cuentas y supervisión efectiva del riesgo en todos los niveles de la organización.

Esta estructura define claramente los roles y responsabilidades desde la ejecución operativa hasta las máximas instancias de dirección, garantizando una gestión del riesgo proactiva, coordinada y alineada con el apetito de riesgo, la estrategia y los objetivos organizacionales.

La organización cuenta con la **Matriz de Roles y Responsabilidades GPL-PRO-F-01,** documento que establece las funciones, niveles de responsabilidad y mecanismos de rendición de cuentas de los actores involucrados en el Sistema de Gestión de Riesgos.

A. Primera Línea: Propiedad y Gestión del Riesgo

La primera línea de defensa está conformada por los procesos de la compañía, las personas que ejecutan y los líderes responsables, quienes tienen la función directa de identificar, evaluar, gestionar y monitorear los riesgos asociados a sus actividades, deben implementar

los controles establecidos, realizar seguimiento a los riesgos identificados y promover la adopción de buenas prácticas en la gestión de riesgos dentro de sus respectivos ámbitos de actuación. Asimismo, son responsables de reportar oportunamente cualquier evento de riesgo, debilidad de control o situación que pueda afectar el adecuado desarrollo de las operaciones.

Los procesos, personas que ejecutan y líderes responsables

- Propiedad y Monitoreo: Identificar, reportar y mantener actualizada la **Matriz de Riesgos GPL-PRO-R-03** de su proceso.
- Valoración y Tratamiento: Realizar la valoración y análisis de los riesgos. Definir, planear, implementar y ejecutar los planes de mejoramiento para la mitigación.
- Control y Reporte: Monitorear la eficacia de los controles, detectar materializaciones y reportar eventos de riesgo a las instancias correspondientes, incluyendo el análisis de causa raíz.
- Cultura: Promover una cultura de gestión de riesgos y oportunidades al interior de sus equipos.

Responsables de la Matriz de Gestión de Riesgos

- Riesgos Operacionales, de liquidez, de continuidad: Procesos (SIGE).
- Riesgos de LA/FT/FPADM, soborno y corrupción: Cumplimiento.
- Riesgos de Proyectos**:** PMO o dependencia o grupo designado por la organización.
- Riesgos de Seguridad de la Información: Seguridad de la Información.

Equipo de Procesos (SIGE)

- Soporte Metodológico: Apoyar a los líderes en la identificación, valoración y actualización de riesgos.
- Validar criterios metodológicos y consistencia de valoraciones.
- Documentación y Divulgación: Certificar trimestralmente que los riesgos y controles están actualizados. Gestionar las modificaciones en la **Matriz de Riesgos GPL-PRO-R-03**.
- Divulgar los documentos actualizados y facilitar la documentación de lecciones aprendidas.
- Coordinación: Coordinar con el área de capacitación para la sensibilización en gestión de riesgos.

Proceso Cumplimiento

- Definir y mantener actualizado los criterios y lineamientos para la gestión de riesgos, garantizando coherencia con el marco normativo.
- Asegurar la integración de la gestión de riesgos dentro del SIGE.
- Consolidar y reportar al Comité de Ética, Riesgos y Cumplimiento y al Comité de la Revisión por la Dirección y Auditoría la evolución del perfil del riesgo, incluyendo los riesgos críticos y aspectos relevantes.

- Realizar una verificación a nuevas normativas o cambios en el entorno, que puedan traducirse en nuevos riesgos o impacten la actualización de los controles de los riesgos existentes.
- Vigilar continuamente cómo se mueven los riesgos en el mapa de calor corporativo. Deben poner especial atención en aquellos riesgos que caen en los cuadrantes de nivel Alto y Significativo, garantizando que no superen el "apetito de riesgo" definido por la Junta Directiva.
- Realizar revisiones periódicas o pruebas de recorrido para confirmar que los controles asociados a temas críticos estén bien diseñados y se ejecuten correctamente.
- Monitorear que los planes de acción propuestos por los líderes de proceso se cumplan en los tiempos estipulados

B. Segunda Línea: Supervisión y Monitoreo del Riesgo

La segunda línea de defensa está integrada por las funciones especializadas encargadas de implementar, supervisar y monitorear la gestión integral del riesgo, estas funciones establecen lineamientos, metodologías y políticas orientadas a la gestión de riesgos, realizan seguimiento al cumplimiento de los controles definidos y promueven una cultura organizacional basada en la prevención y el control. .

Oficial de Seguridad de la Información

- Supervisión de políticas y controles de seguridad: Asegurar que las políticas y procedimientos de seguridad de la información estén implementados y cumplan con normativas y estándares.
- Monitoreo continuo de riesgos tecnológicos: Realizar seguimiento permanente a vulnerabilidades, incidentes y amenazas que puedan afectar la información.
- Gestión de incidentes: Coordinar la respuesta ante incidentes de seguridad y reportar los eventos relevantes al Comité de Revisión por la Dirección y Auditoría .
- Capacitación y sensibilización: Diseñar y ejecutar programas de capacitación en seguridad de la información y ciberseguridad.
- Evaluación y mejora continua: Apoyar en la revisión y actualización de controles, incorporando lecciones aprendidas y mejores prácticas en seguridad de la información.

Oficial de Cumplimiento

- Vigilancia del sistema de prevención de LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses SARLAFT, PTEE y buenas prácticas del SAGRILAFT
- Velar por la implementación y cumplimiento del SARLAFT, PTEE y buenas prácticas del SAGRILAFT .
- Seguimiento: Monitorear los factores de riesgo en la operación y reportar operaciones sospechosas a las autoridades competentes.
- Cultura: Capacitar y sensibilizar al personal sobre riesgos y las medidas de prevención.

C. Tercera Línea: Aseguramiento Independiente

Proporciona un aseguramiento independiente y objetivo, junto con un asesoramiento sobre la adecuación y eficacia del gobierno y la gestión del riesgo (incluyendo el Control Interno), esto se logra mediante la aplicación competente de procesos sistemáticos y disciplinados, informando de sus observaciones a la Junta Directiva y a la Alta Dirección para apoyar el logro de los objetivos organizacionales, promover la transparencia y facilitar la mejora continua.

Auditoría Interna

- Evalúa la eficacia del sistema de gestión de riesgos.
- Verifica el cumplimiento de controles, políticas y normativas aplicables.
- Reportar resultados al Comité de Revisión por la Dirección y Auditoría y Junta Directiva.

D. Gobernanza Superior y Comités (Máxima Supervisión)

Máximas instancias responsables de supervisión, dirección estratégica y toma de decisiones frente al riesgo.

Junta Directiva

- Aprobación Estratégica: Aprobar el sistema de gestión de riesgos, incluyendo los niveles de tolerancia y apetito de los riesgos.
- Supervisión y Recursos: Monitorear el cumplimiento normativo, la eficacia de los controles internos y el desempeño del sistema. Asegurar la asignación de recursos necesarios.
- Dirección: Aprobar informes de gestión de riesgos. Definir estrategias para fortalecer la cultura organizacional de ética y transparencia.

Representante Legal

- Liderazgo Ejecutivo: Lidera y garantiza la implementación efectiva del sistema de gestión de riesgos en toda la organización.

Comité de Ética, Riesgos y Cumplimiento

- Revisión y Decisión Operativa: Aprobar la **Matriz de Riesgos GPL-PRO-R-03** con sus respectivas modificaciones. Evaluar, aprobar y validar los planes de mejoramiento a los riesgos materializados. Evaluar propuestas de modificación, actualización o eliminación de riesgos, nuevas valoraciones y solicitudes de aceptación fuera del nivel de tolerancia.
- Supervisión y Escalado: Supervisar la efectividad de los controles internos y dar seguimiento al cumplimiento de los planes de acción. Analizar y evaluar los riesgos de alta prioridad. Escalar a la Junta Directiva los riesgos que no puedan ser mitigados a niveles aceptables.
- Reporte: Informar periódicamente a la Alta Dirección y Junta Directiva sobre el estado de los riesgos.

Nota: Las decisiones deberán quedar documentadas en el **Acta de Reunión GPL-GPL-R-05**.

Comité de Revisión por la Dirección y Auditoría

- Orientación: Proponer acciones de mejora a riesgos que requieran decisiones estratégicas y orientar a los equipos en la toma de decisiones. Evaluar el comportamiento del perfil de riesgo organizacional.
- Cultura: Promover activamente la cultura de gestión del riesgo y la autorregulación.
- Informes: Evaluar las matrices de gestión de riesgos y el registro de eventos. Presentar informes del comportamiento del sistema y las acciones implementadas a la Junta Directiva.

Nota: Las decisiones deberán quedar documentadas en el **Acta de Reunión GPL-GPL-R-05**.

E. Órganos de Control Externos:

Revisoría Fiscal

- Cumplimiento y Estabilidad: Verifica el cumplimiento de las disposiciones legales y regulatorias aplicables. Revisa los estados financieros y evalúa el impacto de los riesgos en la estabilidad financiera.
- Informes: Emite informes y recomendaciones a la Junta Directiva, asegurando la transparencia y confiabilidad de la información.

8. Capacitación y Competencias

La organización establecerá programas de formación, sensibilización y fortalecimiento de competencias orientados a asegurar el conocimiento, apropiación y aplicación efectiva de los lineamientos, metodologías y responsabilidades asociadas a la gestión integral de riesgos, incluyendo lo relacionado a LA/FT/FPADM, corrupción, soborno, fraude y conflictos de intereses

El desarrollo de competencias constituye un elemento clave para consolidar una cultura preventiva, fortalecer la toma de decisiones informada y contribuir al mejoramiento continuo del Sistema de Gestión de Riesgos.

Formulación del Plan Anual de Capacitación (PAC)

El Plan Anual de Capacitación garantizará que las acciones formativas respondan a necesidades reales de la organización y estén alineadas con su contexto estratégico, operativo y normativo.

Para su estructuración se considerarán, entre otros aspectos:

- Identificación de Necesidades: Anualmente, se identifican las necesidades de capacitación o entrenamiento en los diferentes procesos de la organización, en conjunto con el área de Gestión del Conocimiento. La identificación se basa en los resultados de las evaluaciones de programas anteriores, hallazgos de auditorías, análisis de las causas de las deficiencias operativas o de gestión señaladas, cambios en el contexto o normativos o eventos materializados y lecciones aprendidas.
- Gestión de Recursos: El Plan determina los recursos necesarios para su ejecución, asegurando su viabilidad y cobertura.
- Priorización y cobertura: Definición de públicos objetivo, niveles de criticidad y alcance requerido.

Alcance de la Capacitación

Los programas deberán cubrir los aspectos clave de la gestión de riesgos, promoviendo la apropiación metodológica, la autogestión y la cultura de mejora continua.

- Personal Nuevo: Se capacita al momento de su vinculación, asegurando su conocimiento sobre los sistemas de gestión de riesgos, SARLAFT, PTEE y las buenas prácticas del SAGRILAFT sus responsabilidades.
- Personal Existente: Se realizan capacitaciones periódicas (mínimo anual), orientadas a reforzar conocimientos, actualizar lineamientos y fortalecer la cultura de riesgo.

Evaluación de la Efectividad de la Capacitación

La organización evaluará la efectividad de las capacitaciones realizadas, con el fin de asegurar su impacto en la gestión del riesgo. Para ello podrá considerar evaluaciones de conocimiento, seguimiento a la aplicación de la metodología, disminución de errores operativos o eventos de riesgo entre otros.

Los resultados obtenidos servirán como insumo para la mejora continua del Plan Anual de Capacitación.

9. Comunicación y Consulta

La comunicación y consulta es un proceso continuo, transversal y bidireccional presente en todas las etapas de la gestión del riesgo, orientado a fortalecer la comprensión, participación y rendición de cuentas a los grupos de interés y contrapartes internas y externas.
Este proceso permite fortalecer la toma de decisiones informada, la apropiación del sistema de gestión de riesgos y la consolidación de una cultura organizacional basada en la prevención y la gestión responsable.

- Política y Liderazgo: El Comité de Ética, Riesgos y Cumplimiento promoverá la actualización de la **Política de Gestión Integral de Riesgos GPL-PRO-L-02** y su adecuada socialización en todos los niveles, asegurando claridad en roles y responsabilidades.

- Divulgación y Retroalimentación: La información relacionada con la gestión de riesgos, incluyendo la **Matriz de Riesgos GPL-PRO-R-03**, será comunicada y puesta a disposición de los procesos a través de los mecanismos formales definidos en el SIGE, garantizando su consulta, actualización y trazabilidad.
- Rol de la Primera Línea: Los líderes de proceso son responsables de comunicar a sus equipos los riesgos, controles y acciones de mejoramiento, promoviendo el entendimiento, la participación y la cultura de gestión del riesgo.
- Apoyo Metodológico: El equipo de procesos, en conjunto con los entes de control, promoverá el fortalecimiento de la cultura de riesgo a través de espacios de asesoría, mesas de trabajo y acompañamiento técnico.
- Comunicación Externa: Los riesgos residuales de nivel Alto o Significativo que involucren a grupos de interés o contrapartes crítica s serán comunicados conforme a los lineamientos organizacionales y regulatorios aplicables.

10. Divulgación de la Información

La divulgación de información en materia de riesgos tiene como propósito asegurar transparencia, disponibilidad, oportunidad y trazabilidad, facilitando la toma de decisiones en los diferentes niveles de gobierno corporativo.

Este proceso se materializa mediante reportes ejecutivos y operativos que consolidan información relevante sobre el perfil de riesgo, evolución de exposiciones, eficacia de controles y estado de planes de tratamiento.

Revisión de la Junta Directiva

La Junta Directiva revisa de manera periódica el cumplimiento de los límites de riesgo establecidos, cumplimiento del apetito y la tolerancia, riesgos críticos y tendencias relevantes e impactos potenciales sobre la solvencia, la operación y la continuidad del negocio.

Reporte y Aseguramiento por Órganos de Control

Los órganos de control presentarán informes al Comité de Revisión por la Dirección y Auditoría, incluyendo como mínimo:

- El monitoreo y la evolución de los riesgos relevantes identificados.
- Una evaluación integral de la eficacia de los controles implementados.
- El estado de los planes de mejoramiento y su nivel de cumplimiento.
- Recomendaciones para el fortalecimiento de sistemas de gestión de riesgos.

11. Actualización de Políticas y Metodología

El Sistema de Gestión de Riesgos opera bajo el principio de mejora continua. Por tanto, sus políticas, metodologías y herramientas deberán revisarse periódicamente para asegurar su pertinencia, eficacia y alineación con el contexto organizacional.

Revisión Estratégica de Políticas y Metodología

Las políticas y lineamientos asociados a riesgos deberán revisarse como mínimo cada año, o antes cuando existan cambios relevantes estratégicos, normativos y operacionales.

- Adaptación Normativa: Cualquier modificación requerida por ajustes normativos o regulatorios, fuera del ciclo de revisión, debe ser comunicada previamente al Comité de Ética, Riesgos y Cumplimiento para su análisis y consideración oportuna.
- Aprobación y Divulgación: Una vez que la política y el manual sean actualizadas, es mandatorio establecer un plan de comunicación para su divulgación y apropiación efectiva en todos los niveles de la organización.

Mantenimiento y Dinamismo de la Matriz de Gestión de Riesgos

La **Matriz de Riesgos y Oportunidades GPL-PRO-R-03** deberá mantenerse actualizada de manera permanente y ser objeto de una revisión integral **como mínimo cada año**, o cuando se presenten cambios relevantes en el contexto.

Desencadenantes de Revisión: La actualización de la matriz se realiza obligatoriamente ante cambios significativos en los objetivos, modificaciones en el alcance del proceso, cambios del contexto interno y externo, materialización de riesgos significativos o cuando se presenten cambios normativos.

12. Incumplimiento del Manual

El incumplimiento de las disposiciones establecidas en el presente manual podrá dar lugar a las acciones administrativas, disciplinarias o contractuales a que haya lugar, conforme al **Reglamento Interno de Trabajo GPL-GPL-T-17** y demás disposiciones aplicables.