TABLA DE CONTENIDO

1. OBJETIVO 2
2. ALCANCE 2
3. DEFINICIONES 2
4. CONTEXTO EXTERNO E INTERNO 10
5. RESPONSABLES 11
6. METODOLOGÍA 12
7. ESTRATEGIAS 22
8. MAPA DE RIESGOS 22
9. DIVULGACIÓN 23
10. MONITOREO Y REVISIÓN GESTIÓN INTEGRAL DE RIESGOS 23
11. RIESGOS MATERIALIZADOS 24

1. OBJETIVO

Orientar la gestión integral de los riesgos institucionales de la Unidad de Licores del Meta, a través de los lineamientos estratégicos, metodológicos y operativos, para la adecuada identificación, análisis, valoración, tratamiento, seguimiento, comunicación y reporte de eventos que puedan afectar el cumplimiento de los objetivos institucionales, la integridad pública, la seguridad de la información , con el fin de prevenir su ocurrencia o minimizar el impacto del evento y/o incidente, los cuales pueden afectar el cumplimiento de los objetivos institucionales y de los procesos.

2. ALCANCE

Los lineamientos presentados en este documento aplican y es de obligatorio cumplimiento para todos los procesos, dependencias y servidores públicos de la Unidad de Licores del Meta, en todos los niveles jerárquicos y procesos misionales, estratégicos y de apoyo. Incluye la gestión de riesgos en la planeación, ejecución presupuestal, prestación de servicios, adopción de tecnologías, fortalecimiento organizacional, así como en la implementación de proyectos y programas institucionales.

Adicionalmente comprende las actividades de identificación de los riesgos incluyendo el análisis, valoración, monitoreo, evaluación y seguimiento de los riesgos generales de la gestión, riesgos fiscales, riesgos para la integridad pública, así como los riesgos de lavado de activos (LA), financiación del terrorismo (FT) y financiación de la proliferación de armas de destrucción masiva (FP) -LA/FT/FP) y los riesgos de seguridad de la información.

3. DEFINICIONES

Conceptos clave para la gestión del riesgo:

- **Administración Del Riesgo:** Un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.
- **Amenazas:** Causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización.

- **Análisis Del Riesgo**: Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).
- **Apetito al riesgo:** Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.

- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata)

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Nota: También denominada Causa Eficiente o Causa Adecuada: Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.

- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Proceso efectuado para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Mapa De Procesos:** Es la interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios Es la representación gráfica de los procesos estratégicos, misionales, de apoyo y de evaluación y sus interacciones.
- **Mapa de Riesgos:** El mapa de riesgos es una representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.

- **Monitoreo:** El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas.

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Punto de Riesgo:** Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos

- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.

Nota: Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas

Conceptos clave para la gestión del riesgo fiscal:

- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.
b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

- **Gestión del Riesgo Fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales. Ejemplo: además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)"

- **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.

- **Patrimonio público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

- **Riesgo fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.

Conceptos clave para la gestión del riesgo seguridad de la información:

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Integridad:** Propiedad de exactitud y completitud.

- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Definiciones para la gestión del riesgo en seguridad y salud en el trabajo:

- **Riesgo en seguridad y salud en el trabajo:** Combinación de la probabilidad de que ocurra una o más exposiciones o eventos peligrosos y la severidad del daño que puede ser causada por estos.

Definiciones para la gestión del riesgo ambiental:

- **Riesgo Ambiental:** Posibilidad de que un evento cause un daño o impacto negativo en el medio ambiente, la salud humana, la biodiversidad o la economía, ya sea por causas naturales o por actividades humanas.

Definiciones para la gestión del riesgo para la integridad pública:

- **Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP:** esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos.

- **Riesgos para la integridad:** Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas.

- **Conflicto de interés:** Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011)

- **Corrupción:** Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias;y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015)

- **Colocación:** es la disposición del dinero proveniente de actividades delictivas. Durante esta fase inicial, el determinador o autor introduce sus fondos ilegales en actividades legales o aparentemente legales, bien a través del sistema financiero o de otros tipos de negocios o contratos, tanto nacionales como internacionales.

- **Contraparte:** cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización.

- **Debida diligencia (due dilligence):** proceso que deben llevar a cabo las entidades para identificar, prevenir, mitigar y explicar cómo abordan los impactos negativos reales y potenciales en sus propias actividades, su cadena de suministro y otras relaciones comerciales.

- **Debida diligencia en el conocimiento de la contraparte (debida diligencia del cliente):** proceso que le permite a la entidad conocer aspectos relevantes de sus contrapartes, sean partes vinculadas o relacionadas, para poder gestionar el riesgo que cualquier vinculación o relacionamiento genera.

- **Delito fuente:** según el artículo 323 de la Ley 599 de 2000, son delitos fuente del lavado de activos: tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, contrabando, contrabando de hidrocarburos o sus derivados, fraude aduanero o favorecimiento y facilitación del contrabando, favorecimiento de contrabando de hidrocarburos o sus derivados, en cualquiera de sus formas.

- **Financiación del Terrorismo (FP):** el artículo 345 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien "directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas". La Financiación del Terrorismo puede darse por: recaudación, transmisión, utilización.

- **Financiación de la Proliferación de Armas de Destrucción Masiva (FP):** fondos u otros activos a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del Consejo de Seguridad de las Naciones Unidas dentro del Capítulo VII de la Carta de las Naciones Unidas, en lo relativo a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento. La Financiación de la Proliferación puede darse por: recaudación, transmisión, utilización.

- **Fraude:** errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso

el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025)

- **Función de cumplimiento:** función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública.

- **Integración:** es dar apariencia legítima a riqueza ilícita mediante el reingreso en la economía con transacciones comerciales o personales que aparentan ser normales. Esta fase conlleva la colocación de los fondos lavados de vuelta en la economía para crear una percepción de legitimidad. El lavador podría optar por invertir los fondos en bienes raíces, artículos de lujo o proyectos comerciales, entre otros.

- **Lavado de activos:** el artículo 323 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien "adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades[relacionadas con un delito fuente], o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito". El Lavado de Activos puede darse por: colocación, ocultamiento e integración.

- **Ocultamiento:** es la separación de fondos ilícitos de su fuente mediante una serie de transacciones, cuyo fin es desdibujar la transacción ilícita original. Esta etapa supone la conversión de los fondos procedentes de actividades ilícitas a otra forma y crear esquemas complejos de transacciones financieras para disimular el rastro documentado, la fuente y la propiedad de los fondos.

- **Parte Interesada:** es un tipo de contraparte con la cual no se ha establecido ninguna relación o vinculo, pero que ha manifestado formalmente su interés en establecerlo.

- **Parte Vinculada:** para efectos del SIGRIP, es una contraparte dependiente de la organización con la cual se ha establecido una relación de especial de sujeción por su relación legal o reglamentaria, o laboral.

- **Parte Relacionada**: para efectos del SIGRIP, es una contraparte independiente de la organización con la cual se ha establecido una relación comercial, contractual o legal; o respecto de la cual se ejerce algún grado de control jerárquico, de tutela o de propiedad, sin detrimento de su independencia.

- **Programa de Transparencia y Ética Pública (PTEP) y/o Empresarial (PTEE):** Es un programa de cumplimiento, es decir, una metodología mediante la cual una entidad define acciones estratégicas para promover, al interior de la organización, una cultura de la legalidad e identificar, medir, controlar y monitorear los riesgos para la integridad que se presentan en el desarrollo de su misionalidad.

- **Recaudación:** consiste en la búsqueda de fuentes de financiación por las organizaciones terroristas, bien sean de origen legal, como los aportes de los Estados, individuos, entidades, organizaciones y donantes en general que apoyan su causa o son engañados, así como recursos provenientes de cualquier actividad delictiva, fondos que generalmente circulan en efectivo.

- **Soborno:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar. (A partir de ISO37001:2025) Soborno entrante: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad.

- **Soborno saliente:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la entidad.

- **Transmisión:** es la fase intermedia que busca poner el dinero recaudado a disposición de la organización terrorista, quedando simplemente la espera de su utilización final; corresponde al movimiento de los fondos a través de distintas técnicas, se trata de ocultar sus movimientos y destino final.

- **Utilización:** fase donde los fondos se utilizan básicamente para la financiación de la logística estructural de la organización o la logística operativa en materia de planeación y ejecución de actos terroristas.

4. CONTEXTO EXTERNO E INTERNO

La identificación del entorno interno y externo se realiza mediante el formato **PLE-FR-07** Formato matriz (DOFA), lo que permite comprender la situación estratégica y los factores que inciden en la configuración del riesgo en cada sistema de gestión.

5. RESPONSABLES

La Unidad de Licores del Meta adopta el esquema de líneas de defensa para designar las responsabilidades en la gestión integral de riesgos, así:

Líneas de Defensa	Responsabilidades
Línea estratégica (Alta Dirección y el Comité Institucional de Coordinación de Control Interno)	✓ Define y/o actualiza la política de la gestión integral de riesgos de la entidad, la cual la aprueba el Representante Legal.
Primera Línea de Defensa (Jefes de Dependencia, Líderes de proceso, servidores públicos)	✓ Gestionan los riesgos a través de la identificación, análisis, valoración, monitoreo y acciones de mejora. ✓ Diseñan y autoevalúan los controles, para evitar la materialización de los riesgos.
Segunda Línea de Defensa (Responsable de Planeación, quienes ejerzan labor de supervisión y Asesores de Gerencia)	✓ El responsable de Planeación o quien haga sus veces asesora a la línea estratégica en el análisis del contexto interno y externo, para la definición o actualización de la política de gestión integral de riesgos, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. Igualmente, consolida el Mapa de riesgos institucional y tramita su aprobación por el representante Legal. ✓ Aseguran que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. ✓ Revisan las acciones correctivas y el plan de acción establecido para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos. ✓ Asesoran a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento
Tercera Línea de Defensa	✓ Orienta, asesora y recomienda frente a la gestión integral del riesgo en coordinación con el responsable de Planeación o quien haga sus veces. ✓ Proporciona información sobre la efectividad del Sistema de Control

(Asesor de Control Interno)	Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

6. METODOLOGÍA

La Unidad de Licores Meta adopta como referencia principal la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 (agosto de 2025) como marco para la formulación, implementación, seguimiento y mejora de la gestión de riesgos institucionales, armonizada con el Modelo Integrado de Planeación y Gestión, el Modelo Estándar de Control Interno (MECI) y la estructura organizacional definida en el marco del Sistema Integrado de Gestión.

La aplicación de la metodología se desarrolla bajo los siguientes lineamientos:

- ✓ **Enfoque basado en procesos:** La entidad estructura su gestión del riesgo a partir del Mapa de Procesos institucional, asegurando que cada proceso identifique, valore y trate sus riesgos conforme a las responsabilidades asignadas.
- ✓ **Alineación estratégica:** La formulación de riesgos y controles se articula con la Plataforma estratégica institucional, los objetivos del Plan Estratégico y los instrumentos de planificación aplicables al contexto de la entidad.
- ✓ **Documentación y estandarización:** La segunda línea de defensa (Planeación o quien haga sus veces) es responsable de definir, actualizar y estandarizar los manuales, procedimientos, formatos y demás instrumentos necesarios para la aplicación de la metodología. Esto incluye asegurar que cada tipología de riesgo incorporada en la presente política cuente con lineamientos claros, homogéneos y alineados con los estándares institucionales y normativos vigentes, facilitando su correcta implementación y seguimiento en todas las dependencias.
- ✓ **Análisis de contexto:** La identificación del entorno interno y externo se realiza mediante el formato **F-DE-08 – La Organización y su contexto (DOFA)**, lo que permite comprender la situación estratégica y los factores que inciden en la configuración del riesgo en cada sistema de gestión.
- ✓ **Planeación integrada:** Instrumentos como la caracterización de procesos (formato PLE-CR-01)

La Unidad de Licores del Meta cuenta con el manual del sistema de administración de lavado de activos y financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva y reporte de información SARLAFT/FPADM, aprobado mediante Acuerdo 02 del 19 de septiembre de 2025.

6.1 Tipología de Riesgos

Tipo de riesgos	Descripción
Riesgos de Gestión	Son los riesgos asociados al cumplimiento de los objetivos estratégicos, misionales, de apoyo y de evaluación de los procesos de la entidad. Se identifican y actualizan por los líderes de proceso y sus equipos, basados en la metodología institucional de gestión del riesgo adoptada por la Guía para la Gestión Integral del Riesgo del DAFP.
Riesgos de Integridad (Corrupción + LA/FT/FPADM	Agrupan los eventos que, por acción u omisión, puedan vulnerar la ética pública, la transparencia, la confianza institucional o el adecuado manejo de los recursos. Incluye: (i) **Riesgos de Corrupción**, relacionados con el uso indebido del poder o de la función pública para obtener beneficios particulares; y (ii) **Riesgos de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM)**, asociados al uso de la entidad para legitimar recursos ilícitos, facilitar actividades criminales o dar apariencia de legalidad a activos ilícitos. Su gestión se desarrolla conforme al SIGRIP, el Programa de Transparencia y Ética Pública y las obligaciones del Estatuto Anticorrupción.
Riesgos de Seguridad de la Información	Son los eventos derivados de amenazas internas o externas que pueden explotar vulnerabilidades y afectar la confidencialidad, integridad o disponibilidad de los activos de información de la entidad. Se valoran combinando la probabilidad de ocurrencia y el impacto sobre el servicio, los datos o la operación institucional, conforme a los lineamientos del Modelo de seguridad y privacidad de la información MSPI y la ISO/IEC 27000.
Riesgo Fiscal	Es el riesgo asociado a la afectación de recursos públicos, bienes o intereses patrimoniales de naturaleza pública debido a un evento potencial que genere daño fiscal. Involucra fallas en la custodia, administración, ejecución, registro, control o protección de recursos a cargo de gestores fiscales o públicos. Su evaluación se realiza a partir de circunstancias inmediatas, puntos de riesgo fiscal, controles y riesgo residual.
Riesgos de Seguridad y Salud en el Trabajo	Corresponden a la combinación de la probabilidad de que ocurra un evento peligroso y la severidad del daño que pueda causar a la salud, integridad y bienestar de los servidores y contratistas, así como a los bienes o al medio ambiente. Incluyen riesgos físicos, químicos, biológicos, psicosociales, biomecánicos y de condiciones de seguridad.
Riesgos Ambientales	Se originan en la interacción humana con el ambiente y pueden generar impactos negativos sobre los ecosistemas o sobre la entidad. Comprenden dos enfoques: (1) **Riesgo para el Ambiente:** daños a recursos naturales, biodiversidad, clima, agua, flora, fauna o salud humana derivados de actividades institucionales o externas; y (2) **Riesgo para la Organización:**

	pérdidas financieras, reputacionales o legales derivadas de la inadecuada gestión ambiental o del incumplimiento normativo. Su administración busca reducir la incertidumbre y prevenir afectaciones al entorno y a la operación institucional.

6.2 Factor de Riesgos

Son eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional.

Se establecen los siguientes tipos de riesgo a controlar de acuerdo con su impacto:

- **Ejecución y administración de procesos:** Pérdidas derivadas de errores en la ejecución y administración de procesos, errores en las actividades que deban realizar los servidores de la entidad.

- **Fraude externo:** Pérdida derivada de actos delictivos por personas ajenas a la organización (no participa personal de la entidad).

- **Fraude interno:** Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos un participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para tercero.

- **Fallas Tecnológicas:** Eventos relacionados con la infraestructura tecnológica de la entidad, tales como errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

- **Relaciones laborales:** Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción. Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

- **Usuarios, productos y prácticas:** Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

- **Daños a activos fijos/ eventos externos:** Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentado, vandalismo, orden público.

- **Fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

- **Infraestructura:** Eventos relacionados con la infraestructura física de la entidad. Tales como: Derrumbes, Incendios, Inundaciones, Daños a activos fijos.
- **Evento externo:** Eventos por situaciones externas que afectan la entidad. Como: Fraude Externo, Suplantación de identidad, Asalto a la oficina, Atentados, vandalismo, orden público.

6.3 Niveles de aceptación del riesgo

La aceptación del riesgo se da cuando no se requiere la adopción de medidas que afecten la probabilidad o el impacto del riesgo, para lo cual se precisa lo siguiente:

- **Los riesgos solo serán aceptables cuando su valoración residual se ubique en la zona baja.** En estos casos, no será obligatorio establecer un plan de acción, pero los controles existentes deberán mantenerse y monitorearse periódicamente para asegurar su eficacia. Los riesgos de integridad (Corrupción o LA/FT/FPADM) no podrán ser aceptables a pesar de ser ubicados en una zona de riesgo baja, por lo cual deberán contar con un plan de acción que contribuya a la mitigación del riesgo.

- **Los riesgos cuyo nivel residual se ubique en zona moderada, alta o extrema deberán contar con un plan de acción formal,** el cual será diseñado, ejecutado y evaluado por los responsables del proceso, con el fin de reducirlos a niveles aceptables.

- **En ningún caso se aceptarán riesgos cuya valoración residual se encuentre en zona alta o extrema,** debiéndose adoptar acciones inmediatas para su tratamiento, ya sea mediante reducción o eliminación.

- **Los riesgos de Integridad (Corrupción y LA/FT/FPADM) son considerados inaceptables en todos los niveles, sin excepción**. Deben ubicarse al menos en zona de riesgo moderado y contar obligatoriamente con medidas de tratamiento y monitoreo permanente. Todos los procesos deben realizar procesos de análisis y evaluarse frente a este tipo de riesgos.

- Para la evaluación de los riesgos se debe determinar la probabilidad de ocurrencia y el nivel de impacto o consecuencia, combinando ambos factores para calcular su nivel de severidad. Este análisis deberá realizarse conforme a los lineamientos establecidos los procedimientos vigentes aplicables de acuerdo con el tipo de riesgo.

6.4 Niveles para calificar el impacto

Se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo. Para la calificación del impacto se adopta lo señalado en la Guía emitida por el Departamento Administrativo de la Función Pública para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 (agosto de 2025), para los Riesgos Generales de la Gestión, Riesgos Fiscales, Riesgos de Seguridad de la Información, Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP incluidos los riesgos de LA/FT/FP (manual del sistema de administración de lavado de activos y financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva y reporte de información SARLAFT/FPADM, aprobado mediante Acuerdo 02 del 19 de septiembre de 2025).

El impacto corresponde a la magnitud de las consecuencias económicas y/o reputacionales que puede generar la materialización de un riesgo. Su calificación debe permitir estimar el alcance del daño potencial que afectaría el cumplimiento de los objetivos institucionales.

Estos niveles deberán corresponder a los lineamientos técnicos y normativos propios de cada tipología, tales como:

-Normatividad o regulaciones sectoriales (MinTrabajo, MinAmbiente, MinTIC, UIAF, entre otros) y Lineamientos del DAFP.

La definición de estos niveles deberá garantizar criterios claros, medibles y homogéneos que permitan valorar adecuadamente la severidad del daño y orientar la toma de decisiones sobre el tratamiento del riesgo.

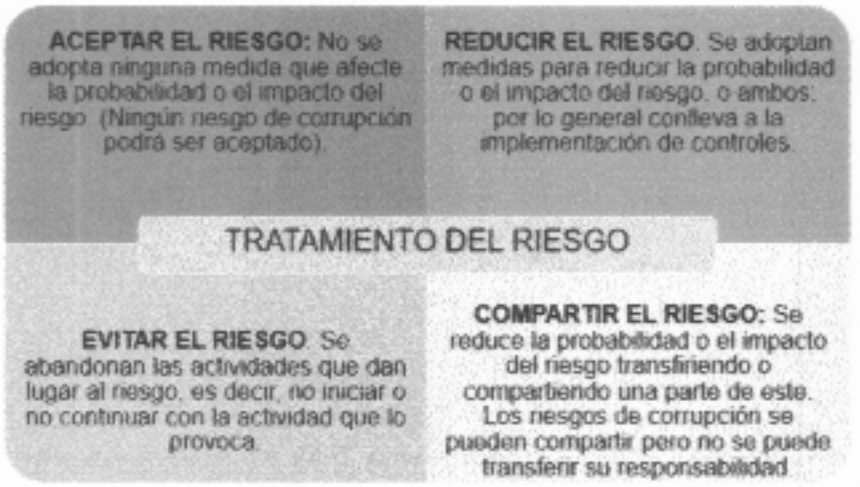
6.5 Tratamiento para combatir los riesgos

¿Qué es tratamiento del riesgo?: Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la entidad se deberá volver a analizar y

revisar dicho tratamiento. En todos los casos para los riesgos de integridad pública **nunca se pueden aceptar**. Por lo tanto, la respuesta será evitar, compartir o reducir el riesgo.

La selección de la estrategia debe sustentarse en el análisis del **riesgo residual** para procesos en operación y, en el caso de procesos nuevos, en el **riesgo inherente**.

La Unidad de Licores del Meta adopta las siguientes estrategias institucionales:

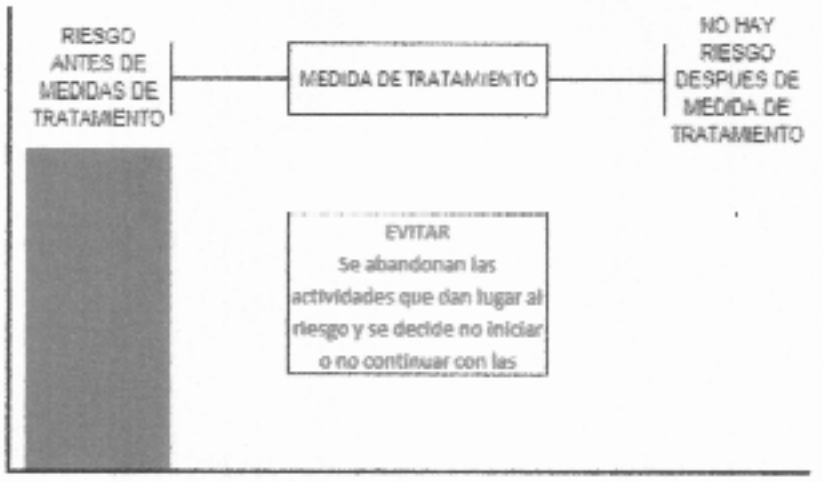


ACEPTAR EL RIESGO: Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.



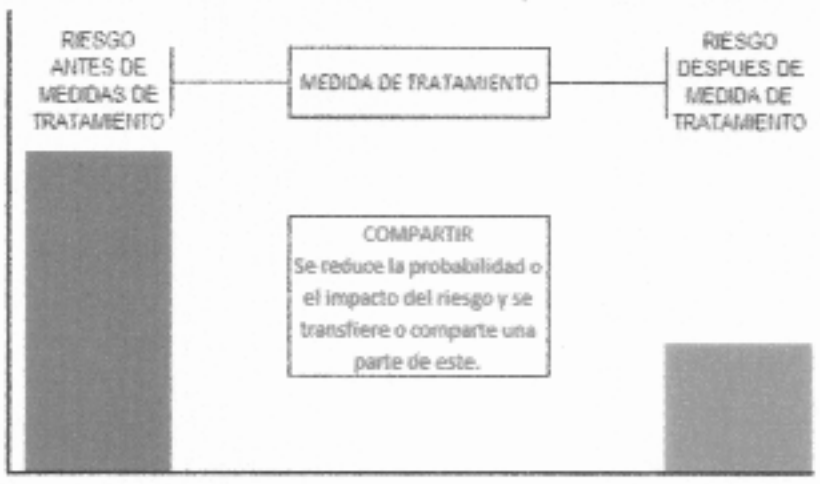
La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

EVITAR EL RIESGO: Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.



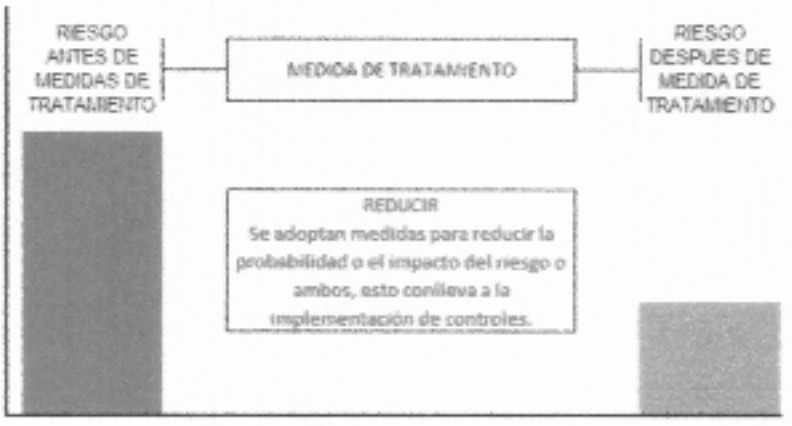
Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

COMPARTIR EL RIESGO: Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.



Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

REDUCIR EL RIESGO: El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.



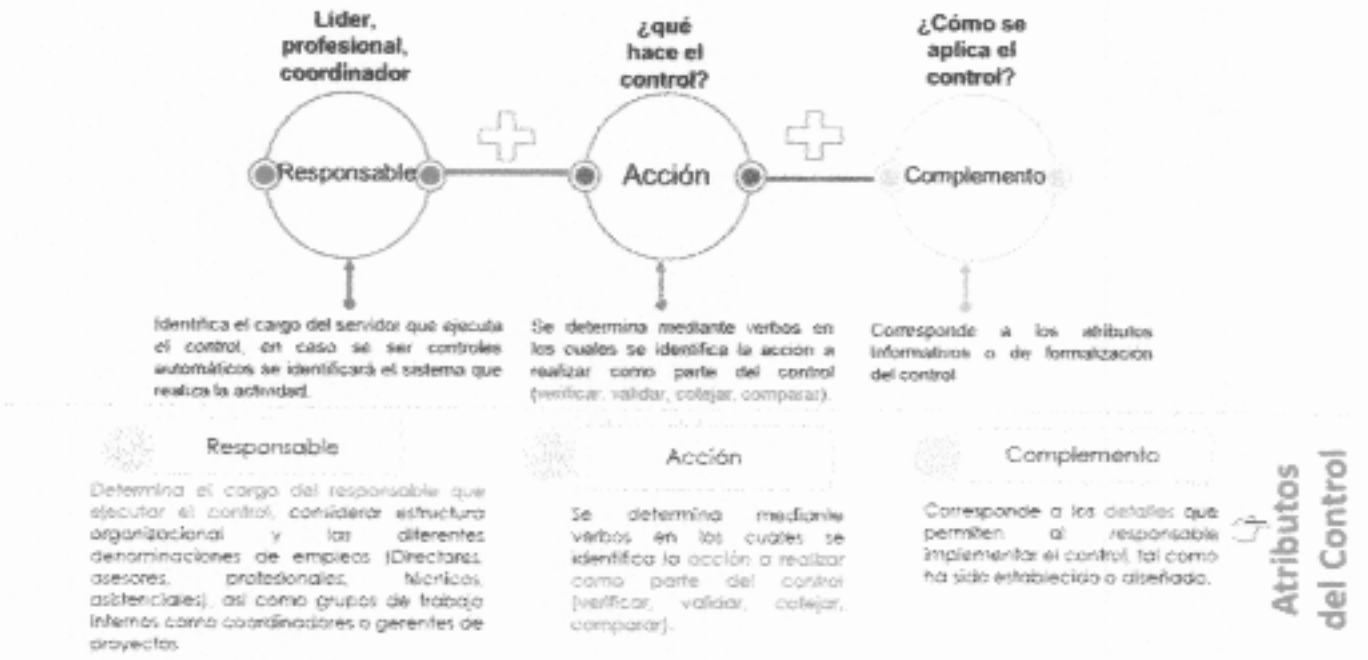
Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

6.6 Diseño de controles para la gestión de riesgos

Antes de valorar los controles es necesario conocer cómo se diseña un control. En la Unidad de Licores del Meta se establece lo siguiente:

Los controles pueden ser preventivos, detectivos o correctivos dependiendo el momento (antes, durante o después) en que se accionen respecto a la actividad que origina el riesgo (punto de riesgo). Los controles preventivos buscan asegurar que no se presente la causa raíz, los controles detectivos buscar tomar medidas ante la ocurrencia de la causa raíz para evitar que se produzca el efecto dañoso y los controles correctivos actúan ante el daño potencial, procurando detener su materialización o reparando el daño causado.

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Para un adecuado diseño de las actividades de control se adopta la siguiente estructura:



Fuente: Guía gestión integral del riesgo versión 7 agosto 2025.

Desglosando la estructura propuesta tenemos el despliegue de los atributos para el control así:

Responsable: Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (Subdirectores, asesores, profesionales, técnicos, asistenciales), así como su despliegue en grupos de trabajo internos e incluir coordinadores o gerentes de proyectos. Cuando se trate de controles automáticos se identificará el responsable de su calibración o

parametrización periódica en el sistema de información o software a través del cual opere el control.

Su definición deberá igualmente considerar que éste cuenta con un nivel de autoridad apropiado de cara a la actividad de control, así como aspectos básicos de segregación de funciones para evitar que quién sea la fuente generadora de riesgo, sea el único que aplica alguna actividad de control.

Acción: Determina para qué se realiza el control, se utilizar verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar.

Atributos Informativos o de formalización del control: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos:

- ✓ Documentación: se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
- ✓ Frecuencia: corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
- ✓ Evidencia: permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
- ✓ Ejecución: permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten. Puede darse a través de la comparación con información interna, externa o mixta.

Se tiene entonces que, para la redacción del control es necesario aplicar todos los atributos acá descritos, de manera tal que se constituyan en una herramienta de control efectiva, los cuales se agrupan a través de la estructura para la redacción del control.

Se debe dejar evidencia de la ejecución del control: Ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente:

1. Fue realizado por el responsable que se definió.
2. Se realizó de acuerdo con la periodicidad definida.
3. Se cumplió con el propósito del control.
4. Se dejó la fuente de información que sirvió de base para su ejecución.

5. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control.

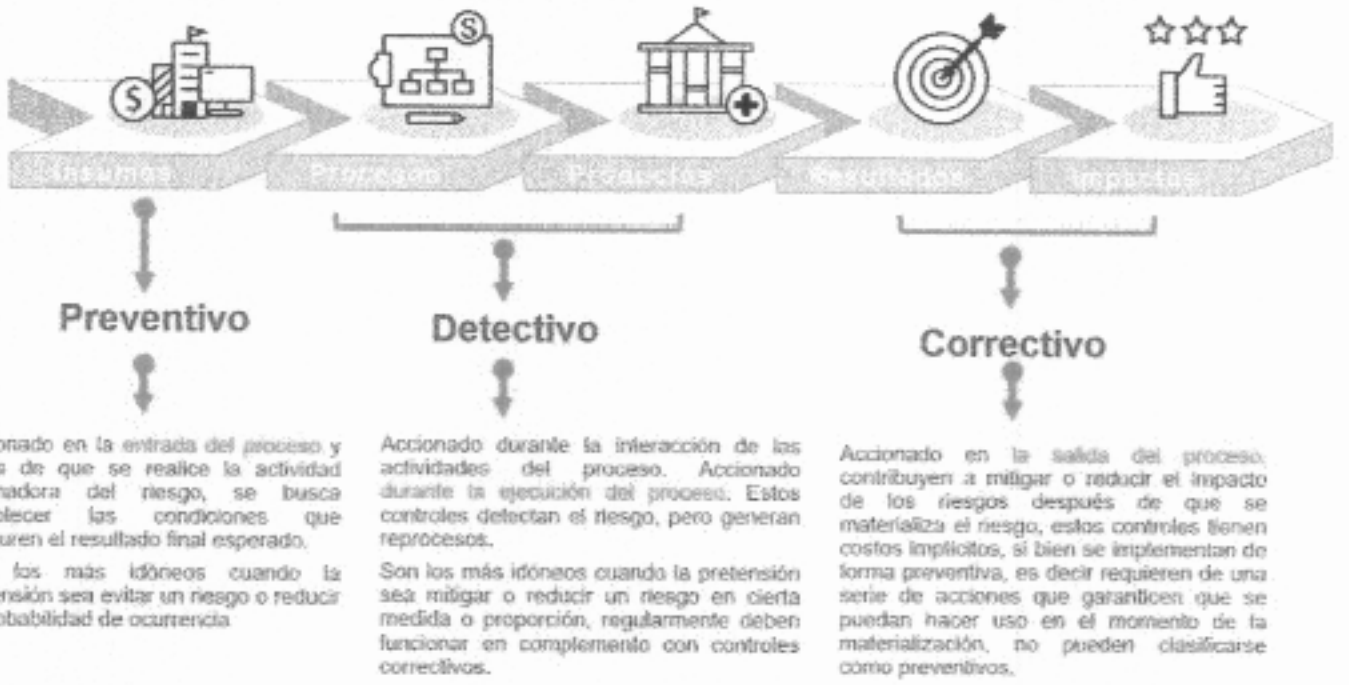
Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

Tipología de controles:

Con el fin de establecer la tipología de controles para su posterior validación, es necesario acudir al ciclo de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo, o bien una combinación de estos.

Para comprender esta estructura conceptual, a continuación, se consideran desde la cadena de valor de los procesos, con el fin de establecer en qué momento se activa el control en función de las actividades clave del proceso, base para la definición de los controles aplicables en sus 3 tipologías que se explican más adelante:

Cadena de valor del proceso y las tipologías de controles



Fuente: Guía gestión integral del riesgo versión 7 agosto 2025.

De acuerdo con el anterior esquema en el ciclo de un proceso, tenemos las siguientes tipologías de controles:

- **Control preventivo:** accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

- **Control detectivo:** accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Se debe tener en cuenta que los controles que se contemplan en esta tipología usualmente tienen que ver con pólizas de seguro, copias de seguridad (*backup*), bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez materializado, los cuales se implementan de forma preventiva, es decir requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización pero no pueden clasificarse como preventivos, ya que sería una sobrevaloración de control que podría generar análisis errados en los niveles de severidad. En consecuencia, si bien estos controles requieren en su diseño que se apliquen actividades con un enfoque preventivo, al ser activados al momento de materialización del riesgo deben ser considerados como controles correctivos no preventivos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

Control manual: ejecutados por personas.

Control automático: ejecutados por un sistema o software previamente programado o diseñado.

7. ESTRATEGIAS

Con el propósito de fortalecer la gestión integral del riesgo bajo un enfoque preventivo, de mejora continua, la Unidad de Licores del Meta adopta las siguientes estrategias institucionales, orientadas a su implementación y sostenibilidad:

- ✓ Socializar y capacitar a los procesos líderes de proceso y funcionarios en la metodología para Gestión Integral del riesgo.
- ✓ Implementar acciones para el fortalecimiento de la Gestión Integral del riesgo en todas las dependencias.
- ✓ Fomentar la cultura del autocontrol en los servidores públicos de la entidad.
- ✓ Evaluar el cumplimiento de la gestión realizada sobre los riesgos, mediante el monitoreo por parte de la segunda línea de defensa y el seguimiento y evaluación de la tercera línea de defensa.

8. MAPA DE RIESGOS

El Mapa de Riesgos es el instrumento institucional mediante el cual la Unidad de Licores del Meta identifica, analiza, valora y prioriza los riesgos que pueden afectar el logro de los objetivos estratégicos y operativos. Su función es orientar la toma de decisiones frente a la necesidad de **evitar, reducir, compartir, transferir o aceptar** los riesgos, así como definir los responsables, plazos, controles e indicadores necesarios para su gestión, monitoreo y evaluación.

Para su implementación, la entidad utilizara los documentos y/o herramientas que se adopten, modifiquen o sustituyan conforme a la evolución metodológica. Todos los instrumentos deberán estar **debidamente registrados y actualizados en el Sistema Integrado de Gestión**, garantizando su trazabilidad, estandarización y disponibilidad para las líneas de defensa.

9. DIVULGACIÓN

La Política para la Gestión Integral del Riesgo, los Mapas de Riesgos y las demás herramientas metodológicas asociadas serán divulgadas y/o socializadas de manera oportuna en todas dependencias de la Unidad de Licores del Meta, para garantizar su aplicación en la gestión de los riesgos.

La documentación se mantendrá disponible para consulta y actualización permanente en las dependencias responsables. La difusión se realizará mediante los canales institucionales oficiales como el correo institucional y mesas de trabajo o de socialización.

10. MONITOREO Y REVISIÓN GESTIÓN INTEGRAL DE RIESGOS

El monitoreo y la revisión de la Gestión Integral del Riesgo se desarrollarán a través de **tres (3) etapas**, garantizando la trazabilidad, eficacia y mejora continua de la entidad, a continuación, se describen las etapas para el monitoreo y revisión de la gestión integral del riesgo: Riesgos de Gestión, Fiscales, Riesgos de Integridad Pública y Seguridad de la Información y los Riesgos LAFT/FPADM:

1) **Autocontrol de los líderes de proceso (Primera Línea de Defensa)**: Los líderes de cada proceso realizarán monitoreo permanente a la identificación, análisis, valoración, tratamiento y reporte del riesgo, verificando la efectividad de los controles y el cumplimiento de los planes de acción establecidos. Los Líderes de proceso reportan de manera cuatrimestral al Responsable de Planeación el monitoreo con evidencias a través del formato PLE-FR-08 (Formato mapa de riesgo institucional)

2) **Aseguramiento (Segunda Línea de Defensa):** Responsable de Planeación o el Profesional de apoyo efectuará un monitoreo técnico al sistema de administración del riesgo, con una periodicidad mínima semestral, **dos (2) veces al año**, verificando la

correcta aplicación de los lineamientos, metodologías y herramientas institucionales. El responsable de Planeación o quien haga sus veces consolida cuatrimestralmente el monitoreo del mapa de riesgos institucional y presenta para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. Adicionalmente, reporta dicho monitoreo de manera cuatrimestral a la Oficina de Control Interno, con las respectivas evidencias dentro de los primeros diez (10) días enero, de mayo y de septiembre.

Respecto a los **riesgos LAFT/FPADM: La Oficial de Cumplimiento** efectuará un monitoreo técnico al sistema de administración del riesgo, con una periodicidad mínima semestral, **dos (2) veces al año**, verificando la correcta aplicación de los lineamientos, metodologías y herramientas institucionales. Además, debe realizar monitoreo continuo, para evaluar la eficacia de los controles y cumplir oportunamente con los roles y responsabilidades señaladas en el manual del sistema de administración de lavado de activos y financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva y reporte de información SARLAFT/FPADM, aprobado mediante Acuerdo 02 del 19 de septiembre de 2025. En consecuencia, en el mes de enero y julio de cada año presentará un informe con el análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. Adicionalmente, de manera conjunta con la profesional de planeación reportan monitoreo de los **riesgos LAFT/FPADM** de manera cuatrimestral a la Oficina de Control Interno, con las respectivas evidencias dentro de los primeros diez (10) días enero, de mayo y de septiembre PLE-FR-08 (Formato mapa de riesgo institucional)

3) **Evaluación independiente por la Oficina de Control Interno (Tercera Línea de Defensa):** La Oficina de Control Interno realizará la evaluación objetiva e independiente a la gestión integral del riesgo, con como mínimo dos (2) veces durante la vigencia, conforme al **Plan Anual de Auditoria.**

11. RIESGOS MATERIALIZADOS

Con el propósito de fortalecer el seguimiento realizado por la primera línea de defensa y garantizar decisiones basadas en evidencia, se establecen los siguientes criterios para determinar cuándo un riesgo se considera materializado en la Unidad de Licores del Meta:

Un riesgo se entenderá como materializado cuando ocurra un evento, acción u omisión que genere consecuencias negativas tangibles para el cumplimiento de los objetivos institucionales. La materialización deberá evidenciarse mediante uno o más de los siguientes elementos:

- Hallazgos o informes derivados de auditorías internas o externas que reflejen el incumplimiento de controles clave o debilidades estructurales en los procesos.

- Incidentes, eventos o situaciones que representen afectación económica, operativa, jurídica, ambiental o reputacional a la entidad.
- Indicadores de gestión o de riesgo que reflejen un desvío de las metas u objetivos definidos.
- Informes o evidencias que den cuenta de fallas sistémicas, irregularidades, fraudes o pérdidas, relacionadas directamente con el riesgo identificado.
- Quejas, reclamos, demandas o sanciones impuestas por entes de control o usuarios que correspondan con la exposición a riesgos previamente identificados.

Reporte inmediato: Ante la materialización de cualquier riesgo, el líder del proceso deberá reportarlo de manera inmediata a la segunda línea de defensa (Responsable de Planeación o quien haga sus veces), para su análisis, registro, definición de acciones correctivas y actualización del mapa de riesgos correspondiente. Además, se levanta la acción correctiva a través del (formato de acciones correctivas) PLE-FR-09

CONTROL DE REGISTROS Ver listado maestro de formatos.			
ANEXOS: PLE- FR- 08 Formato Mapa de riesgos institucional PLE- FR- 09 Formato de Acciones Correctivas PLE- FR- 07 Formato matriz DOFA			
CONTROL DE CAMBIOS			
Fecha de Solicitud	**Descripción detallada del cambio / Modificación**	**Fecha de Vigencia**	**Versión**
Elaborado por:	**Revisado por:**	**Aprobado por:**	
Nombre: Lida Mayerly Rondón	Nombre: Lida Mayerly Rondón	Nombre: Wilintong Ortíz Arias	
Cargo: Profesional Universitario (E)	Cargo: Profesional Universitario (E)	Cargo: Gerente (E)	
Fecha: 30/10/2026	Fecha:30/10/2026	Fecha: 30/10/2026	