INSTITUTO MUNICIPAL PARA EL DESARROLLO SOCIAL Y ECONÓMICO DE PALMIRA - IMDESEPAL

POLITICA DE ADMINISTRACION DEL RIESGO

Versión 2

Palmira (Valle), Diciembre 04 de 2025

Tabla de contenido

1. PRESENTACIÓN 4
2. INTRODUCCIÓN 5
3. MARCO LEGAL 7
4. MARCO CONCEPTUAL 8
5. OBJETIVOS 9
   5.1 OBJETIVO GENERAL 9
   5.2 OBJETIVOS ESPECÍFICOS 9
6. ALCANCE 11
7. TÉRMINOS Y DEFINICIONES 12
8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 22
   8.1 METODOLOGIA PARA LA GESTIÓN DEL RIESGO 22
   8.2 RESPONSABILIDADES FRENTE A LOS RIESGOS 22
9. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO 25
   9.1 DESCRIPCIÓN RIESGOS DE GESTIÓN 25
   9.2 DESCRIPCIÓN RIESGOS FISCALES 26
   9.2 DESCRIPCIÓN RIESGOS DE CORRUPCIÓN 28
   9.4 RIESGOS DE SEGURIDAD DIGITAL 28
      9.4.1 IDENTIFICACIÓN DE LOS ACTIVOS O GRUPO DE ACTIVOS DE INFORMACIÓN 29
   9.5 RIESGOS DE INTEGRIDAD PÚBLICA 32
10. ETAPAS DE LA ADMINISTRACIÓN DE RIESGOS 34
11. LINEAMIENTOS PARA MAPAS DE RIESGOS 34
12. COMUNICACIÓN Y SOCIALIZACIÓN 35
13. DE IMPACTO 35
13. ROLES Y RESPONSABILIDADES 35
   Línea Estratégica: 35
   Primera Línea de Defensa: 35
   Segunda Línea de Defensa: 36

Tercera Línea de Defensa: 36
14. ZONA DE RIESGO Y TRATAMIENTO 36
15. ANÁLISIS DE RIESGOS 37
15.1 PROBABILIDAD 37
15.2 IMPACTO 37
16. TRATAMIENTO DE RIESGOS DE CORRUPCIÓN 38
17. MONITOREO DE RIESGOS 39
18. DISEÑO DE CONTROLES 39
19. EVALUACIÓN DEL CONTROL 41

1. PRESENTACIÓN

En el marco del fortalecimiento del Sistema de Control Interno y en atención a los principios de planeación, prevención y mejora continua, el Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL realizó la revisión del documento contenido en la Resolución No. 310-23-027-2017 del 12 de diciembre de 2017, “Por medio de la cual se actualiza el Mapa de Riesgos del Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL”, mediante la cual la entidad contaba con la Política de Administración del Riesgo y los mapas de riesgos que orientaban la gestión institucional.

Como resultado de dicha revisión y considerando los cambios normativos, técnicos y metodológicos en materia de administración del riesgo, la entidad identificó la necesidad de actualizar la Política de Administración del Riesgo, con el fin de armonizarla con los lineamientos vigentes impartidos por el Departamento Administrativo de la Función Pública (DAFP), así como con los estándares establecidos en el Modelo Integrado de Planeación y Gestión – MIPG y el Sistema de Control Interno.

Esta actualización responde al compromiso institucional de fortalecer la cultura de la gestión del riesgo, el autocontrol y la autorregulación, como herramientas fundamentales para la prevención de eventos que puedan afectar el cumplimiento de la misión, los objetivos estratégicos y la adecuada prestación de los servicios a cargo de la entidad. En este sentido, la Política de Administración del Riesgo se consolida como un instrumento clave de gestión, que permite identificar, analizar, evaluar y tratar los riesgos, así como reconocer oportunidades que contribuyan al logro de los resultados institucionales.

El presente documento es el resultado de un proceso participativo y articulado, en el cual intervinieron los servidores públicos de IMDESEPAL, quienes, desde sus responsabilidades y competencias, aportaron al análisis de los riesgos asociados a los procesos institucionales. Este ejercicio fue ampliamente discutido y concertado con los responsables de cada proceso, garantizando su alineación con la normatividad vigente en materia de control interno y gestión pública.

Con la adopción de la nueva Política de Administración del Riesgo, IMDESEPAL reafirma su compromiso con una gestión pública eficiente, eficaz y responsable, orientada a la prevención de eventos que puedan afectar el cumplimiento de sus funciones, la prestación de los servicios y la generación de valor público para la ciudadanía.

2. INTRODUCCIÓN

El Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL, reafirmando su compromiso con una gestión pública eficiente, transparente y orientada al cumplimiento de los fines del Estado, adopta la presente Política de Administración de Riesgos como una herramienta estratégica destinada a fortalecer la gestión institucional y garantizar el logro de sus objetivos misionales.

Esta política define los principios y lineamientos esenciales para la identificación, análisis, evaluación, tratamiento, seguimiento y comunicación de los riesgos que puedan incidir en el cumplimiento de los propósitos institucionales. Asimismo, promueve una cultura de prevención, control y mejora continua en todos los niveles de la entidad, fomentando la corresponsabilidad en la gestión del riesgo.

El desarrollo de esta política se sustenta en las orientaciones emitidas por el Departamento Administrativo de la Función Pública (DAFP), en especial en la Guía para la Administración de Riesgos y el Diseño de Controles – Versión 7 (agosto de 2025), así como en los lineamientos dispuestos por otros entes rectores en materia de control interno y gestión del riesgo.

Con base en este marco de referencia, el IMDESEPAL orienta sus esfuerzos hacia la consolidación de una gestión integral del riesgo que facilite la toma de decisiones informadas, optimice el uso de los recursos públicos, fortalezca la confianza de la ciudadanía y contribuya a la generación de valor público, en armonía con los principios del Modelo Integrado de Planeación y Gestión (MIPG) y del Sistema de Control Interno.

La política de administración de riesgos contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual, y la aplicación de acciones, así como los responsables, el cronograma y los indicadores.

El estudio y el manejo del riesgo es una función dentro de la organización para definir un conjunto de estrategias que a partir de los recursos (físicos, humanos y financieros), busca en el corto plazo mantener la estabilidad financiera de la entidad, protegiendo los activos e ingresos y, en el largo plazo, minimizar las pérdidas ocasionadas por la ocurrencia de dichos riesgos.

El manejo adecuado de los riesgos permite lograr de manera más eficiente el cumplimiento de los objetivos misionales u generales y estar preparados para enfrentar cualquier contingencia que se pueda presentar.

Al igual que todas las entidades de la administración pública no siendo ajenas al tema de los riesgos, debemos buscar como manejarlos y controlarlos partiendo de la base de nuestra razón de ser compromiso con la comunidad y sociedad en general; por esto se debe tener en cuenta que los riesgos no solo son de carácter económico y están directamente relacionados con entidades financieras o con los que se ha denominado riesgos profesionales, sino que hacen parte de cualquier gestión que se realice.

IMDESEPAL debe evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función.

Esta herramienta administrativa le permite a la entidad autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos, garantizar su gestión institucional y fortalecer el ejercicio del Control Interno.

3. MARCO LEGAL

Ley 87 de 1993, por el cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones, artículo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecta. Artículo 2 literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Ley 489 de 1998. Estatuto Básico de la Organización y funcionamiento de la administración pública.

Decreto 1537 de 2001, por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado que en el parágrafo del Artículo 4°. Señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones. y en su artículo 3°. establece el rol que deben desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su artículo 4°. la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…).

Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano y se presenta el anexo técnico del MECI 1000:2005.

Ley 1474 de 2011, que dicta normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Guía DAFP del 2022 para la administración del riesgo y el diseño de controles en entidades públicas -versión 6-nov 2022.

Norma Técnica Colombiana NTC-ISO31000

Norma Técnica Colombiana NTC-GTC 137

4. MARCO CONCEPTUAL

IMDESEPAL como entidad pública descentralizada del orden municipal, no puede ser ajena a las herramientas disponibles y a las nuevas tendencias en administración, para lo cual requiere estar en constante actualización y estar abierta al cambio y a la aplicación de diferentes instrumentos que le permitan ser cada vez más eficiente, por lo que se hace necesario tener en cuenta todos aquellos hechos o factores que puedan afectar en un momento determinado el cumplimiento de los objetivos institucionales.

Dado que todas las organizaciones independientemente de su naturaleza, tamaño y razón de ser están permanentemente expuestos a diferentes riesgos o eventos que pueden tener en riesgo su existencia, se hace necesario introducir el concepto de Administración del Riesgo. Desde la perspectiva del control, la eficiencia del control es la reducción de los riesgos, es decir: el propósito principal del control es la eliminación o reducción de estos, propendiendo porque el proceso y sus controles garanticen, de manera razonable que los riesgos están minimizados o se están reduciendo y, por lo tanto, que los objetivos de la organización van a ser alcanzados.

Para el caso de IMDESEPAL de acuerdo con sus funciones, estructura, manejo presupuestal, contacto con la ciudadanía y el carácter de compromiso social entre otros, es necesario identificar o precisar las áreas, los procesos, los procedimientos, las instancias y controles dentro de los cuales puedan actuarse e incurrirse en riesgos que atentan contra la buena gestión y la obtención de resultados para obtener un adecuado manejo del riesgo.

Igualmente, es importante tener en cuenta que los riesgos están determinados por factores de carácter externo, también denominados del entorno y factores de carácter interno.

Entre los factores externos se destacan: la normatividad la cual constantemente se está actualizando, como lo que se expresa en sentencias que declaran sin efecto normas que venían aplicándose y que en un momento determinado pueden afectar las funciones específicas de una entidad pública y por lo tanto sus objetivos.

Entre los factores internos se destacan: el manejo de los recursos, la estructura organizacional, los controles existentes, los procesos y procedimientos, la disponibilidad presupuestal, el nivel del talento humano, la motivación y los niveles salariales, entre otros.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

La Administración de Riesgos en el Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL, tiene como finalidad orientar de manera estratégica, integral y continua la gestión del riesgo dentro de la Entidad. Este proceso busca fortalecer el pensamiento basado en riesgos como principio esencial para la toma de decisiones informadas, la priorización de acciones y el logro de resultados institucionales.

La gestión del riesgo comprende las etapas de identificación, análisis, valoración, tratamiento, seguimiento y monitoreo de los riesgos, con el propósito de reducir o eliminar los posibles impactos negativos que puedan comprometer el cumplimiento de los objetivos estratégicos. De esta manera, se promueve una gestión pública más efectiva, eficiente, transparente y orientada a la mejora continua.

En coherencia con este propósito, se establecen los siguientes objetivos específicos:

5.2 OBJETIVOS ESPECÍFICOS

1. Fortalecer la estructura organizacional para la gestión del riesgo, definiendo claramente los roles, responsabilidades y niveles de actuación de acuerdo con el modelo de las líneas de defensa, garantizando la articulación entre las dependencias y la eficacia en la implementación de controles.

2. Estandarizar las metodologías y criterios técnicos aplicables a la identificación, análisis, evaluación, tratamiento, seguimiento y monitoreo de los riesgos institucionales, promoviendo la coherencia y trazabilidad de la información en todos los procesos.

3. Verificar el cumplimiento del marco normativo y de los lineamientos establecidos por los entes de control y rectoría, con el fin de que la gestión del riesgo se ejecute conforme a los principios de integridad, transparencia y mejora continua.

4. Promover una cultura organizacional basada en la prevención y el pensamiento de riesgo, fomentando la participación activa de los servidores

públicos en la identificación oportuna de riesgos y en la implementación de acciones de control efectivas.

5. Fortalecer la toma de decisiones estratégicas, mediante el uso de información confiable sobre los riesgos institucionales, que permita anticipar escenarios, priorizar recursos y mejorar la capacidad de respuesta ante eventos adversos.

6. ALCANCE

La Política de Administración del Riesgo tiene un alcance integral y es de aplicación obligatoria para todas las dependencias, procesos, servidoras y servidores públicos de la entidad, sin distinción de su nivel jerárquico ni del ámbito en el que desarrollen sus funciones. Esta política se extiende a las áreas misionales, estratégicas y de apoyo, promoviendo una cultura institucional orientada a la identificación, valoración, tratamiento, monitoreo y comunicación de los riesgos que puedan afectar el logro de los objetivos institucionales.

Su aplicación abarca todas las etapas de la gestión pública, incluyendo la planeación estratégica y operativa, la ejecución presupuestal, la prestación de servicios a la ciudadanía, la adopción e implementación de tecnologías de la información, el fortalecimiento organizacional, así como el diseño, desarrollo y ejecución de proyectos y programas institucionales. De esta manera, se busca consolidar una gestión preventiva, articulada y orientada a la mejora continua en todos los niveles de la entidad.

7. TÉRMINOS Y DEFINICIONES

- ACTIVOS DE INFORMACIÓN PRIMARIOS. Procesos y actividades del negocio, información primaria, información vital para la ejecución de la misión de la entidad, Información personal definida específicamente en las leyes nacionales sobre privacidad. Información estratégica que se requiere para alcanzar con los objetivos determinados, información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición.
- ACTIVOS DE INFORMACIÓN SECUNDARIOS O DE APOYO. Son activos de los cuales dependen los activos primarios y estos pueden presentar vulnerabilidades que son explotables por amenazas, cuya meta es deteriorar, intervenir o acceder a los activos primarios.
- ACTIVOS DE INFORMACIÓN. Se refiere al activo que contiene información que la entidad genere, obtenga, adquiera, transforme o controles. En el contexto de seguridad digital, son activos los elementos tales como: aplicaciones de la organización, servicios web, redes información digital, tecnologías de información - TI, tecnologías de operación - TO, que utiliza la organización para funcionar en el entorno digital.
- AMENAZAS. Causa o situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización (seguridad de la información). Peligro latente de que un evento físico de origen natural, o un evento causado, o inducido por la acción humana de manera accidental o deliberada, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales.
- ANÁLISIS DE CONTEXTO. Proceso de identificación y evaluación de factores internos y externos que pueden influir en el desempeño de una organización
- ANÁLISIS DE RIESGO. Proceso para comprender la naturaleza del riesgo y determinar el nivel de criticidad.
- APETITO AL RIESGO. Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

- BENEFICIARIO FINAL. Es la persona natural que, en última instancia, posee, controla o se beneficia de una transacción, ya sea de manera directa o indirecta.

- CAMBIO CLIMÁTICO. Variación a largo plazo de los patrones climáticos y las temperaturas, según la ONU. Esta variación puede deberse a causas naturales o a la acción humana.

- CAPITAL ESTRUCTURAL. Es la valoración de los activos intangibles que surgen de la aplicación del conocimiento para llevar a cabo las funciones, tareas y actividades de la entidad. Está integrado por: infraestructura organizacional (los procesos, la estructura organizacional, los sistemas informáticos que apoyan el quehacer de la organización, la cultura organizacional, entre otros) y el conocimiento susceptible de protegerse a través de la propiedad intelectual.

- CAPITAL HUMANO. Es la valoración de los activos intangibles resultantes de la aplicación del conocimiento de cada una de las personas de la entidad en el contexto organizacional. Está relacionado con el saber hacer, modelos mentales, conocimiento tácito y explícito a nivel individual o equipos.

- CAPITAL RELACIONAL. Es la valoración de los activos intangibles que se originan en las relaciones de la entidad con el entorno. Se define como el conocimiento integrado en las relaciones (relación con clientes, usuario, proveedores, entre otros) establecidas entre la organización y sus grupos de valor.

- CARACTERIZACIÓN. Proceso mediante el cual se identifican las características sociodemográficas y contextuales de las partes interesadas, tales como edad, género, nivel educativo, condición étnica o discapacidad, con el fin de diseñar estrategias inclusivas y pertinentes.

- CAUSAS. Son todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. Aquello que se considera como fundamento, principio, origen o razón de un evento, suceso o situación. Explica los motivos por los cuales se está presentando una situación que se está analizando; la mejor manera de identificarla es preguntándose cuál es el origen del problema o situación.

- COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO. Es un órgano de asesoría y decisión en los asuntos de control interno de la Alcaldía de Santiago de Cali. En su rol de responsable y facilitador, hace parte de las instancias de articulación para el funcionamiento del Sistema de Control Interno.

- CONFIDENCIALIDAD. Propiedad de la información que la hace no estar disponible al conocimiento o divulgación de personas, entidades o procesos no autorizados. Esta propiedad de la información hace que sea accesible sólo a personal autorizado previniendo su divulgación no autorizada cuando está almacenada o en tránsito.

- CONSECUENCIAS. Son 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.

- COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO. Es una instancia y mecanismo rector, articulador y ejecutor, a nivel institucional, de las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento del Modelo Integrado de Planeación y Gestión – MIPG.

- CONTEXTO DEL RIESGO. Es la clasificación que establece la estructura conceptual, define lineamientos e incorpora mejores prácticas y traza la ruta de implementación de acuerdo con la clase de riesgo. En este caso serán Contexto de Gestión, Corrupción y Seguridad de la Información, lo que determina diferentes variables en la identificación y descripción asociada al riesgo.

- CONTEXTO ESTRATÉGICO. Son las condiciones internas y externas, que pueden generar eventos que originen oportunidades o afecten negativamente el cumplimiento de la misión y objetivos de la entidad, es insumo básico para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones internas y externas de la entidad.

- CONTROL CORRECTIVO. Medida que permite mitigar el impacto frente a la materialización del riesgo.

- CONTROL DETECTIVO. Medida que permite disminuir la probabilidad de ocurrencia del riesgo y detectar que algo ocurre y devuelve el proceso a los controles preventivos.

- CONTROL PREVENTIVO. Medida que permite eliminar las causas del riesgo, para prevenir su ocurrencia o materialización, así como la disminución de la probabilidad con relación a las causas que dependen de la entidad.

- CONTROL. Medida que permite reducir o mitigar un riesgo.

- DEBIDA DILIGENCIA. Equivalente a su término en inglés *“que diligencie”*, es el proceso mediante el cual la entidad adopta medidas para el conocimiento

de sus contrapartes, incluyendo, pero sin limitarse a su identidad, antecedentes, reputación, sus relacionados, su negocio, operaciones, productos y el volumen de sus transacciones.

- EVALUACIÓN DEL RIESGO. Proceso para determinar el nivel de riesgo asociado al nivel de probabilidad de que dicho riesgo se concrete y al nivel de severidad de las consecuencias (impacto).
- EVENTO DE SEGURIDAD DE LA INFORMACIÓN. Ocurrencia identificada de un sistema, servicio de red o infraestructura que indica una posible infracción de la política de seguridad de la información, falla de controles implementados o una situación desconocida que puede ser relevante para la seguridad de la información. Un evento en la seguridad de la información no significa necesariamente una implicación en la confidencialidad, integridad o disponibilidad de la información, a veces es esperado o deseable para conocer y aprender de ello y así fortalecer la seguridad si es necesario. El evento compromete los niveles de riesgo, pero no afecta la operación de la organización y sus objetivos.
- EVENTO. Ocurrencia o cambio de un conjunto particular de circunstancias. Tipo de cambio que no presenta resultados negativos. Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo conocido, programado o esperado no suceda.
- EXPECTATIVAS. Percepciones, intereses o deseos implícitos que las partes interesadas tienen sobre el desempeño de la entidad, y que influyen en su satisfacción y confianza.
- FACTORES AMBIENTALES. Condiciones naturales y regulaciones relacionadas con la sostenibilidad y la gestión de recursos.
- FACTORES ECONÓMICOS. Condiciones y dinámicas económicas que afectan la operatividad de una entidad, como inflación, tasas de interés y acceso a financiamiento.
- FACTORES ESTRATÉGICOS. Elementos internos que determinan la dirección y planificación institucional de una organización.
- FACTORES POLÍTICOS. Decisiones y dinámicas de poder que pueden influir en la normativa, la regulación y la estrategia de la organización.
- FACTORES TECNOLÓGICOS. Avances e innovaciones que impactan la operación, eficiencia y competitividad de una organización.

- FINANCIACIÓN DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA (FP). Son 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.

- FINANCIACIÓN DEL TERRORISMO (FT). 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.

- FRAUDE EXTERNO. Pérdida derivada de actos de fraude 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 beneficios ya sean tangibles e intangibles para sí mismo o para terceros.

- FRAUDE. Consiste en una acción que resulta contraria a la verdad y a la rectitud, el fraude se comete en perjuicio de una persona u organización, también es considerado como la utilización de una conducta deshonesta o engañosa con el fin de obtener alguna injusta ventaja sobre otra persona u organización y que conlleve a un beneficio particular, desviando la gestión pública basada en el bien común.

- FUENTE DE IDENTIFICACIÓN. Fuente de información que permite identificar cambios o situaciones relacionados con los riesgos, generación de riesgos, materialización, exposición. Para esta entidad serán considerados los reportes generados por la segunda línea de defensa, tercera línea de defensa y los entes de control externos.

- FUGA DE CAPITAL INTELECTUAL. Posibilidad de que una amenaza concreta pueda causar una pérdida de información de los activos tangibles e intangibles (aquellos que no se ven) pero que se ha convertido en conocimiento útil para la organización.
- GESTIÓN DEL RIESGO. Actividades coordinadas para dirigir y controlar una Entidad con respecto al riesgo y proporcionar a la administración un aseguramiento razonable frente al logro de los objetivos.
- GRUPO DE INTERÉS. Parte interesada que influye en la gestión pública, tiene interés en sus resultados o puede convertirse en usuario de los servicios y trámites de la entidad.
- GRUPO DE VALOR. Parte interesada que recibe directamente los servicios de la entidad o participa de forma directa o indirecta en el cumplimiento de su misión institucional.
- HARDWARE. equipo de procesamiento de datos, equipos móviles. equipos fijos, periféricos para procesamiento, medios para datos (pasivo), medio electrónico, otros medios, que por su criticidad son considerados activos de información, no sólo activos fijos.
- IDENTIFICACIÓN DE RIESGOS. Proceso de encontrar, reconocer y describir riesgos. La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.
- IMPACTO. Efectos producidos de acuerdo con la materialización de un riesgo o la posibilidad de que este ocurra.
- INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN. Requiere de la conjunción de eventos de seguridad de la información de modo que se afecte negativamente la información. comprometiendo la seguridad y debilitando y afectando la capacidad para alcanzar los objetivos. Puede representar pérdida, publicación o corrupción de la información y ocasionar un retraso en las operaciones. El incidente, afecta negativamente a la organización e incluso a la información a diferencia del evento.
- INFLUENCIA. Capacidad de una parte interesada para afectar de manera significativa las decisiones, estrategias o actividades de la entidad.
- INTEGRIDAD. Propiedad de la información referente a su exactitud y completitud. Esta propiedad de la información hace que la información sea

ingresada y/o modificada sólo por personal autorizado previniendo la manipulación no autorizada.

- INTERÉS. Nivel de atención o expectativa que una parte interesada tiene respecto a la gestión institucional, dependiendo de cómo le afecten sus acciones o resultados.

- LAVADO DE ACTIVOS (LA). 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.

- MAPA DE RIESGOS INSTITUCIONAL. Contiene los riesgos de mayor criticidad para la entidad con base a los parámetros analizados frente al logro de los objetivos institucionales e integra los riesgos de acuerdo con el contexto del riesgo bajo los que se han identificado.

- MATRIZ DE ACTIVOS DE INFORMACIÓN. inventario de activos de información de la entidad en el cual se registran las características del activo y se valora su criticidad. El inventario de activos de información debe ser un documento clasificado como "Confidencial".

- MATRIZ DE ESFUERZO E IMPACTO. Herramienta que permite priorizar acciones estratégicas en función de los recursos requeridos y sus posibles efectos.

- NECESIDADES. Requisitos explícitos que deben ser cumplidos por la entidad y que pueden derivarse de normas legales, compromisos institucionales o demandas sociales y comunitarias.

- NORMOGRAMA. Documento que compila las normas regulatorias y complementarias aplicables a un proceso organizacional.

- OPORTUNIDADES. Factores del entorno que pueden favorecer el crecimiento o fortalecimiento de la organización.

- ORGANIZACIÓN. Autoridades, estructura de la organización, organización del sistema o de proyectos, subcontratistas /proveedores / fabricantes.

- PARTES INTERESADAS. Personas naturales o jurídicas, grupos u organizaciones que pueden afectar o ser afectadas por las decisiones, servicios o actividades de una entidad pública.
- PELIGRO. Fuente o situación con capacidad de producir daño en términos de lesiones, deterioro a la propiedad, al medio ambiente o una combinación de ellos.
- PERSONAL. Recurso humano que, debido a su conocimiento y experiencia en los temas críticos para el proceso, son consideradas activos de información.
- 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 un año.
- RED. Medios y soportes de transmisión activa o activa, interfaz de comunicación, equipos de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- RIESGO DE CORRUPCIÓN. Posibilidad de que, por acción u omisión, se use el poder del servidor público para desviar la gestión de lo público hacia un beneficio privado.
- 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).
- RIESGO DE SEGURIDAD Y SALUD EN EL TRABAJO. Combinación de la probabilidad de que ocurran eventos o exposiciones peligrosos relacionados con el trabajo y la severidad de la lesión y deterioro de la salud que pueden causar los eventos o exposiciones.
- RIESGO FISCAL. Es el efecto dañino sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- RIESGO INHERENTE. Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- RIESGO RESIDUAL. Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento. Es el resultado de aplicar la efectividad de los controles al riesgo inherente.
- RIESGO. Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- SEGURIDAD DE LA INFORMACIÓN. Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- SEGURIDAD INFORMÁTICA. Se refiere a la protección del sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene.
- SERVICIO TERCERIZADO. Corresponde a los servicios y productos suministrados externamente.
- SITIO. Ubicación y/o depósito específico donde esté el activo de información, ambiente externo, instalaciones, zona, servicios esenciales, comunicación, servicios públicos.
- SOFTWARE. Sistema operativo, software de servicio, mantenimiento o administración, paquete de software o software estándar, aplicaciones de negocio.
- TECNOLOGÍA EMERGENTE. La tecnología se define como emergente cuando causa un cambio radical en los negocios, la industria o la sociedad, incluyen tecnologías de información, comunicación inalámbrica de datos, comunicación hombre a máquina, impresión bajo demanda, biotecnologías y robótica avanzada, entre otras. La tecnología puede considerarse emergente en un contexto particular, aunque se haya considerado establecida en otro.
- TECNOLOGÍA INFORMÁTICA. Es aquella que posibilita el procesamiento de información a través de medios artificiales como los equipos de cómputo o sistemas informáticos.
- TOLERANCIA AL RIESGO. Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Para el riesgo de corrupción la tolerancia es inaceptable.
- UIAF. Es la sigla que identifica a la Unidad de Información y Análisis Financiero que es una Unidad Administrativa Especial de carácter técnico, adscrita al Ministerio de Hacienda y Crédito Público, cuyas funciones serán de intervención del Estado con el fin de detectar prácticas asociadas con el lavado de activos.

- VULNERABILIDAD. Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La política de administración de riesgos en el Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL, contiene los lineamientos para gestionar los riesgos identificados de gestión, corrupción, fiscales, seguridad digital, Integridad Pública y Seguridad Salud en el Trabajo, mediante la aplicación de controles que permitan el desarrollo de una gestión pública efectiva y el cumplimiento de los objetivos estratégicos, respondiendo a las necesidades y expectativas de sus partes interesadas.

8.1 METODOLOGIA PARA LA GESTIÓN DEL RIESGO

La metodología tiene como propósito identificar, analizar, valorar y gestionar los riesgos que puedan afectar el cumplimiento de los objetivos institucionales de IMDESEPAL, considerando tanto los factores internos como externos que inciden en su operación.

Para ello, se parte del contexto estratégico de la entidad, el cual incluye su misión, visión, objetivos institucionales y el entorno en el que desarrolla sus funciones. Así mismo, se analiza la caracterización de los procesos, teniendo en cuenta su objetivo, alcance y los posibles eventos que puedan impactar negativamente su desempeño.

El proceso de gestión del riesgo busca reconocer aquellos riesgos que están o no bajo el control de la organización, y establecer las acciones de mitigación, control o tratamiento que permitan prevenir, reducir o asumir adecuadamente sus efectos.

El adecuado manejo de los riesgos contribuye al desarrollo y fortalecimiento institucional, garantizando que los planes, programas y proyectos de IMDESEPAL se ejecuten de manera efectiva y en coherencia con su misión constitucional y legal. Para lograrlo, se requiere un enfoque sistemático que contemple la identificación, análisis, valoración y definición de alternativas de acción, promoviendo una gestión preventiva, articulada y orientada a la mejora continua.

8.2 RESPONSABILIDADES FRENTE A LOS RIESGOS

La responsabilidad frente a los riesgos de gestión, corrupción, fiscales, seguridad digital, Integridad Pública y Seguridad Salud en el Trabajo, se establece teniendo en cuenta el esquema de las líneas de defensa definidas en la dimensión 7 (Control Interno), del Modelo Integrado de Planeación y Gestión (MIPG). A continuación, se presenta dicha tabla:

Línea de defensa	Responsables	Responsabilidad frente a los riesgos
Línea Estratégica	Representante Legal Comité Institucional de Coordinación de Control Interno.	Aprobar la política de administración de los riesgos de gestión, corrupción, fiscales y de seguridad digital. Velar porque se garantice el cumplimiento de la misión, visión, objetivos institucionales y/o estratégicos, planes, programas y proyectos de la entidad. Definir, aprobar y supervisar el cumplimiento del marco general para la administración del riesgo y la continuidad del negocio. Retroalimentar al Comité Institucional de Gestión y Desempeño, respecto a los ajustes que se deban realizar a la administración del riesgo. Analizar los riesgos, amenazas, vulnerabilidades de mayor criticidad y escenarios de pérdida de continuidad del negocio, los cuales, pueden afectar el cumplimiento de la misión, visión, objetivos institucionales y/o estratégicos, planes, programas, proyectos, metas, compromisos y capacidades para prestar los servicios.
Primera línea de defensa	Líderes de proceso y sus equipos (En general servidores públicos en todos los niveles de la organización).	Supervisar que los equipos de trabajo estén ejecutando los controles definidos. Definir, adoptar, aplicar y hacer monitoreo a los controles definidos para mitigar los riesgos, detectando las deficiencias en los controles y proponiendo las mejoras a que haya lugar. Identificar, valorar, evaluar, controlar, mitigar y actualizar, cuando se requiera, los riesgos que pueden afectar la misión, visión, objetivos institucionales y/o estratégicos, planes, programas y proyectos de la entidad asociados a su proceso o subproceso. Reportar los avances y evidencias del monitoreo a los riesgos, dentro de los plazos establecidos.

		Revisar y ejecutar, de acuerdo con su competencia y alcance, lo relacionado con la continuidad del negocio. Informar a las áreas o dependencias que hacen parte de la segunda línea de defensa, los riesgos que se hayan materializado.
	Funcionarios y contratistas	Conocer los riesgos asociados al proceso o subproceso, en especial los relacionados con sus funciones, y aplicar los controles y/o acciones establecidas para abordarlos. Participar en la elaboración y administración de los mapas de riesgos, de acuerdo con sus competencias o labores ejecutadas. Reportar de manera oportuna, y a las instancias correspondientes, la materialización de riesgos, con el objeto de realizar un adecuado tratamiento y/o mitigación.
Segunda línea de defensa	Media y Alta Gerencia: Jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, comités de riesgos (donde existan), comité de contratación, áreas financieras, de TIC, entre otros que generen información para el Aseguramiento de la operación.	Acompañar, orientar y generar alertas a los líderes de los procesos, subprocesos, programas o proyectos y sus equipos de trabajo, en la identificación, análisis, valoración y evaluación de los riesgos, de acuerdo con su competencia y conocimiento. Supervisar que los controles y las actividades para la administración de los riesgos, ejecutadas por la primera línea de defensa, sean apropiadas, eficaces y funcionen correctamente. Asesorar a la línea estratégica en el análisis del contexto interno y externo para la definición de la política de administración de los riesgos de gestión, corrupción, fiscales y de seguridad digital y el establecimiento de los niveles de apetito, tolerancia y capacidad del riesgo. Actualizar la documentación que soporta el plan de continuidad del negocio. Evaluar que la administración de los riesgos esté acorde con la presente

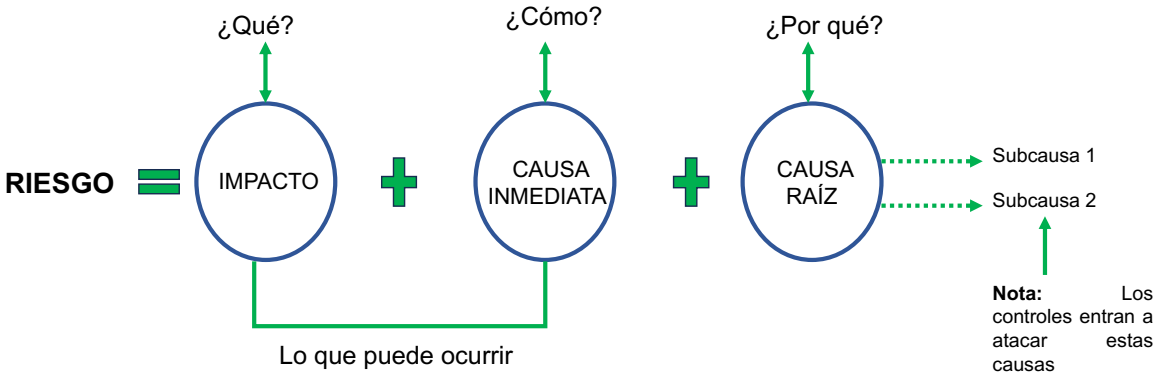
		política de administración de los riesgos de gestión, corrupción, fiscales y de seguridad digital.
Tercera línea de defensa	Oficina de Control Interno	Realizar recomendaciones a la primera línea de defensa, de manera coordinada con la segunda línea de defensa, en la administración de los riesgos y el plan de continuidad del negocio. Recomendar mejoras a la política y metodología de administración del riesgo. Realizar evaluación y seguimiento a la gestión del riesgo y al plan de continuidad del negocio y reportar los resultados a los líderes de los subprocesos, al Comité Institucional de Coordinación de Control Interno y a la Alta Dirección. Proporcionar información a la Alta Dirección y al Comité Institucional de Coordinación de Control Interno sobre la efectividad del Sistema de Control Interno, con un enfoque basado en riesgos.

9. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

El Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL, empleará metodologías establecidas por el Departamento Administrativo de la Función Pública (DAFP) y otras guías relevantes, como las de Colombia Compra Eficiente, adaptándolas a sus necesidades.

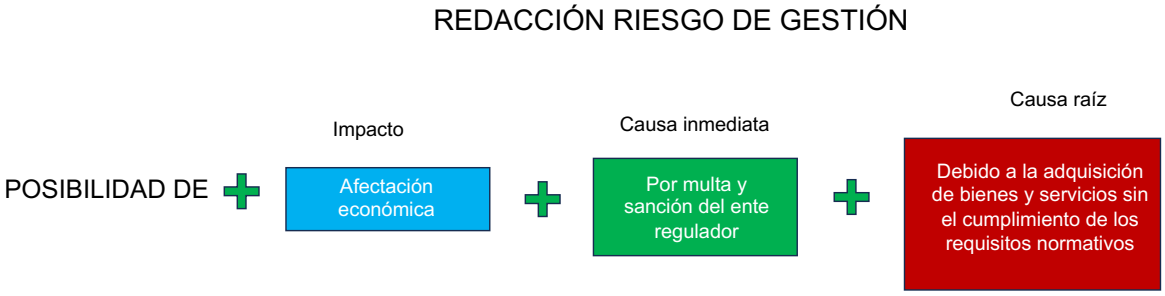
9.1 DESCRIPCIÓN RIESGOS DE GESTIÓN

Para realizar una correcta descripción de los riesgos de gestión, se establece una estructura que facilitará su redacción y claridad, la cual, inicia con la frase POSIBILIDAD DE y que contiene lo siguiente:



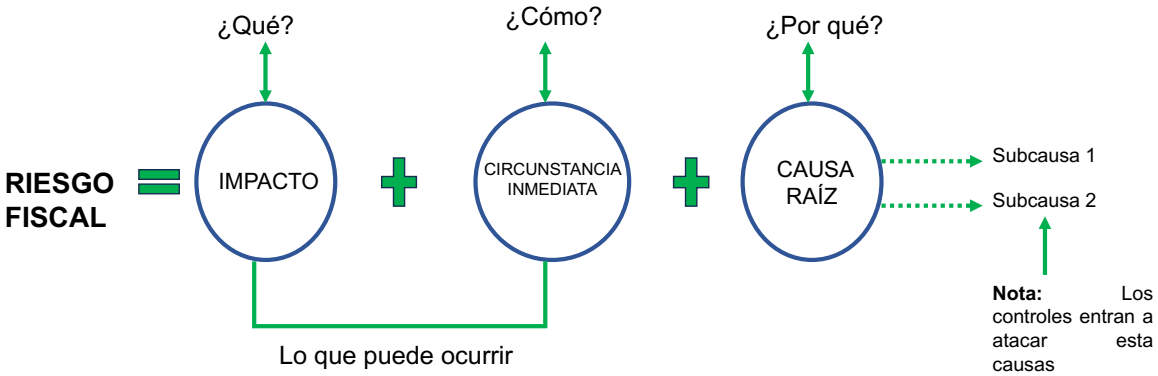
Desglosando la estructura propuesta se tiene lo siguiente:

➢ **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
➢ **Causa inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
➢ **Causa raíz:** Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.



9.2 DESCRIPCIÓN RIESGOS FISCALES

En lo que respecta a los riesgos fiscales, se establece una estructura que facilitará su redacción y claridad, la cual, inicia con la frase POSIBILIDAD DE (debido a que se refiere a un evento potencial) y que contiene lo siguiente:

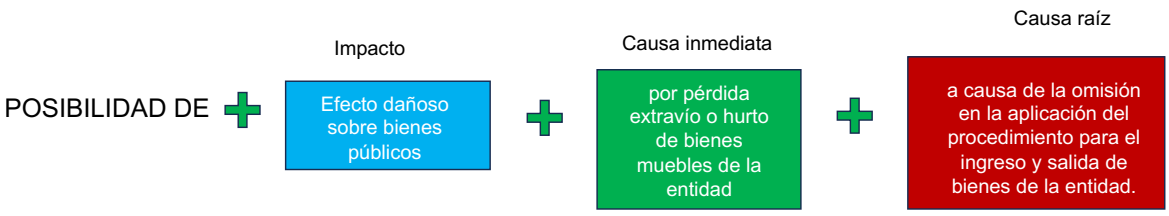


Desglosando la estructura propuesta se tiene lo siguiente:

➢ **Impacto:** Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
➢ **Circunstancia inmediata:** Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica (causa raíz) para que se presente el riesgo.
➢ **Causa raíz:** Corresponde al por qué; que es el evento (acción u omisión), que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

NOTA: Un aspecto fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública (consultar términos y definiciones disponibles en este documento).

REDACCIÓN RIESGO FISCAL



9.2 DESCRIPCIÓN RIESGOS DE CORRUPCIÓN

El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado, implicando de esta manera que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos. Por lo tanto, es necesario que en la descripción del riesgo de corrupción concurran los siguientes componentes, los cuales hacen parte de su definición.

Acción u omisión + Uso del poder + Desviación de la gestión de lo público + Beneficio privado

REDACCIÓN RIESGO DE CORRUPCIÓN

POSIBILIDAD DE + Recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros + Con el fin de celebrar un contrato.

9.4 RIESGOS DE SEGURIDAD DIGITAL

La identificación y evaluación de los riesgos de seguridad y privacidad de la información tienen como objetivo prevenir o minimizar efectos no deseados, promover la mejora continua y comprender las posibles consecuencias y probabilidades de ocurrencia. Estas actividades se fundamentan en tres criterios fundamentales que afectan a un activo o conjunto de activos en el proceso: integridad, confidencialidad y disponibilidad.

El enfoque de gestión de riesgos de seguridad de la información se centra en los activos de información, partiendo de la identificación de vulnerabilidades y amenazas presentes en ellos, seguido de un análisis exhaustivo de las posibles consecuencias. Este enfoque permite la implementación y supervisión de los

controles establecidos, con el fin de mitigar los impactos que podrían surgir en caso de materialización de dichos riesgos.

Clasificación	Descripción
Pérdida de la confidencialidad	La pérdida de la confidencialidad se refiere a la revelación no autorizada de información sensible o privada. Esto puede ocurrir de manera accidental o intencional, y puede tener consecuencias graves para las personas o entidades afectadas.
Pérdida de la integridad	Se refiere a la garantía de que los datos y sistemas informáticos no han sido modificados, corrompidos o eliminados sin autorización. Es uno de los pilares fundamentales de la seguridad informática, junto con la confidencialidad y la disponibilidad.
Pérdida de la disponibilidad	Se refiere a la garantía de que los datos y sistemas informáticos están accesibles para los usuarios autorizados cuando los necesitan. Es uno de los pilares fundamentales de la seguridad informática, junto con la confidencialidad y la integridad.

9.4.1 IDENTIFICACIÓN DE LOS ACTIVOS O GRUPO DE ACTIVOS DE INFORMACIÓN

Es fundamental asegurar la identificación de directrices para la detección y prevención del uso indebido de información privilegiada y otras situaciones que puedan representar riesgos para la entidad, conforme a lo establecido en la documentación pertinente. Esta documentación, conocida como "Formato de Matriz de Inventario de Activos de Información", define los niveles de confidencialidad, integridad y disponibilidad necesarios para la gestión de la información de los procesos.

A partir del inventario actualizado de activos de información de cada proceso, según lo registrado en el "Formato de Matriz de Inventario de Activos de Información", se procede con el análisis para identificar los riesgos de seguridad y privacidad de la información, considerando la valoración de amenazas, vulnerabilidades y su posible impacto en los activos de información.

Tipo de Activo	Definición	Ejemplos
Información	Corresponden a este tipo de activos de información, los datos e información almacenada o procesada física o electrónicamente que tiene significado o relevancia para la entidad, en cualquier formato que se genera, almacena, gestiona, transmite.	Personales: Bases y archivo de datos, hojas de vida. Financieros: Balances financieros, etc. Legales: Acuerdos de confidencialidad, etc. Investigación y desarrollo: Licencias, estudios, etc. Estratégicos: Planes, indicadores, seguimientos, etc. Otros: Documentación de sistemas de información, copias de seguridad, etc.
Software	Activo informático lógico como programas, herramientas ofimáticas y demás utilizadas para la ejecución de las actividades de la Entidad.	Sistemas operativos. Herramientas Ofimáticas. Motor de bases de datos. Antivirus. Software Estadístico. Software de Georreferenciación. Motores de bases de datos. Software de diseño y programación. Compiladores.
Hardware	Estos activos corresponden al tipo utilizado para llevar a cabo la captura, procesamiento, almacenamiento, difusión y divulgación de la información. Engloban todos los componentes físicos que posibilitan el funcionamiento de un entorno informático.	Discos duros o extraíbles. Servidores físicos o virtuales. Computadores. Dispositivos móviles.
Servicios	Recursos esenciales necesarios para el funcionamiento efectivo de los procesos. Estos pueden incluir instalaciones para el almacenamiento y la protección de sistemas de información y comunicaciones, así como archivos documentales. Se refiere al espacio designado para preservar y proteger los datos o información crucial para la entidad.	Edificaciones. Centros de cómputo. Archivo Central.

Bases de datos personales	Conjunto de datos y registros que describen a individuos o entidades legales.	Base de datos de historias laborales. Base de datos de identificación personal. Base de datos de procedimientos administrativos. Base de datos de salud. Bases de datos de contactos con otras entidades. Bases de datos a inscripción de cursos ofertados por la Entidad.
Infraestructura crítica cibernética	Es la infraestructura respaldada por tecnologías de la información y operativas, cuyo funcionamiento es fundamental para proporcionar servicios esenciales tanto a los ciudadanos como al Estado.	Página Web. Aplicativos de trámites y servicios. Otros.

Teniendo en cuenta que un riesgo de seguridad de la información se entiende como la posibilidad de que una amenaza explote una vulnerabilidad, afectando la confidencialidad, integridad o disponibilidad de un activo de información y generando consecuencias negativas para la organización. Para su formulación, el riesgo debe describirse considerando los siguientes elementos:

Iniciar con la palabra: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
¿Qué puede suceder? - Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

¿Cómo puede suceder? - Causa inmediata: Identificar si esta sucede por pérdida de confidencialidad, pérdida de integridad o pérdida de disponibilidad de la información.

¿Por qué puede suceder? - Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, definir aquí la amenaza y la vulnerabilidad del activo de información.

EJEMPLO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

¿Qué puede suceder?	¿Cómo puede suceder?	¿Por qué puede suceder?	Descripción
Posibilidad de afectación económica y reputacional	Pérdida de disponibilidad de la información	debido al hurto o daño de medios o documentos por ausencia de protección física de la edificación, puertas y ventanas	Posibilidad de afectación económica y reputacional por Pérdida de disponibilidad de la información debido al hurto o daño de medios o documentos por Ausencia de protección física de la edificación, puertas y ventanas

9.5 RIESGOS DE INTEGRIDAD PÚBLICA

En los riesgos de integridad pública, la causa inmediata deberá ser alguna de las siguientes: (1) Fraude interno; (2) Soborno; (3) Actuar en el marco de un conflicto de intereses no declarado; o (4) Corrupción.

El fraude, soborno y conflicto de intereses son formas específicas en que puede manifestarse la corrupción. Para los demás actos de desviación de poder, que no derivan en un fraude y no están precedidos por un soborno o un conflicto de intereses, se usará, de forma general, la causa de corrupción.

En los riesgos de integridad pública, la causa inmediata deberá ser alguna de las siguientes: (1) Fraude interno; (2) Soborno; (3) Actuar en el marco de un conflicto de intereses no declarado; o (4) Corrupción.

El fraude, soborno y conflicto de intereses son formas específicas en que puede manifestarse la corrupción. Para los demás actos de desviación de poder, que no derivan en un fraude y no están precedidos por un soborno o un conflicto de intereses, se usará, de forma general, la causa de corrupción.

Tipos de riesgo para la integridad pública asociados a Corrupción

Impacto	Causa Inmediata		Causa Raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, Informes inexactos o descripciones incorrectas	Descripción de la actividad en el flujo del proceso

		realizadas con culpa o dolo para beneficio personal o de terceros.	
	Soborno Entrante	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.	
	Soborno Saliente	Ofrecer, prometer o dar 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.	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere 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.	
	Presunto acto de Corrupción	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere 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.	

10. ETAPAS DE LA ADMINISTRACIÓN DE RIESGOS

1. Identificación: Reconocer los riesgos inherentes a los procesos institucionales.
2. Análisis: Evaluar probabilidad de impacto de cada riesgo.
3. Valoración: Clasificar riesgos según su nivel inherente y residual.
4. Tratamiento: Establecer medidas de control y mitigación.
5. Monitoreo y Seguimiento: Evaluar la eficacia de los controles aplicados.

11. LINEAMIENTOS PARA MAPAS DE RIESGOS

1. Los riesgos deben estar asociados a los objetivos estratégicos y procesos de la entidad.
2. Los mapas de riesgos serán aprobados por los líderes de procesos y revisados por el Director Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL.
3. Los riesgos de integridad pública y seguridad digital serán tratados con prioridad especial.
4. Los riesgos residuales en zonas de riesgo bajo podrán ser aceptados, siempre que no involucren corrupción o soborno.
5. Los mapas serán actualizados anualmente, antes del 31 de enero de cada vigencia salvo que circunstancias excepcionales requieran ajustes.

12. COMUNICACIÓN Y SOCIALIZACIÓN

La política de riesgos será divulgada a través de:

- Página web institucional.
- Correos electrónicos.
- Sesiones de formación, inducción y reinducción.

Esto garantiza que todos los servidores públicos y contratistas estén informados sobre los lineamientos y controles establecidos.

13. DE IMPACTO

Para los riesgos de Integridad pública, gestión y de seguridad de la información la Identificación de áreas de impacto será la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

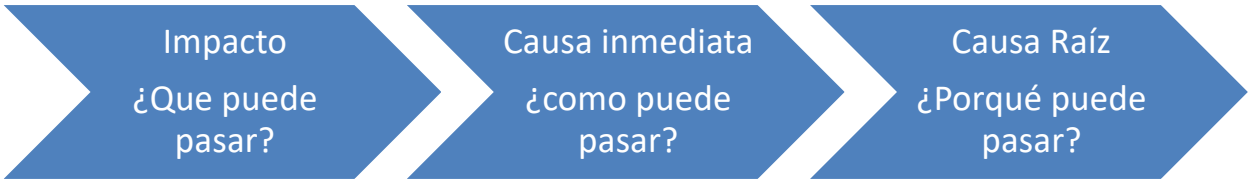
Para los riesgos fiscales la Identificación de áreas de impacto será la “Efecto dañoso sobre los recursos, bienes o bienes de interés patrimonial” y la consecuencia será solo económica.

13. ROLES Y RESPONSABILIDADES

Línea Estratégica:
Bajo el liderazgo del Director y el Comité Institucional de Coordinación de Control Interno Define marco general para la gestión del riesgo y el control y supervisa su cumplimiento, establece la Política para la administración del riesgo.

Primera Línea de Defensa:
Desarrolla e implementa procesos de control y gestión de riesgos (identificación, análisis, valoración, monitoreo y acciones de mejora) Servidores Públicos: Implementar controles operativos.

Durante la etapa de identificación de riesgos y su descripción se deberá mantener la siguiente estructura.



Segunda Línea de Defensa:

Asegura que los controles implementados y procesos de gestión están diseñados y operan efectivamente a través de seguimiento a la implementación de lineamientos establecidos.

Tercera Línea de Defensa:

Oficina de Control Interno: Evaluar la efectividad de los controles y realizar auditorías independientes.

14. ZONA DE RIESGO Y TRATAMIENTO

Los riesgos identificados serán tratados según su clasificación:

Zona de Riesgo	Nivel de Aceptación	Tratamiento
Muy Baja o Baja	Aceptable	Se administra mediante actividades propias del proceso y se monitorea bimensualmente.
Moderada	Parcialmente Aceptable	Se implementan acciones de control preventivas para reducir la probabilidad de ocurrencia del riesgo. Monitoreo bimensual.
Alta y Extrema	No Aceptable	Se adoptan medidas estrictas para reducir o compartir el impacto y la probabilidad del riesgo. Se implementan controles inmediatos.

15. ANÁLISIS DE RIESGOS

15.1 PROBABILIDAD

La probabilidad de ocurrencia de un riesgo se evaluará considerando la tabla propuesta por el departamento Administrativo de la Función Pública en la guía para la administración de riesgos y diseño de controles versión 6.

Tabla 4 Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Departamento administrativo de Función Pública

15.2 IMPACTO

De igual manera, el impacto se mide según las consecuencias para el Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL en los siguientes niveles y se utilizará la tabla propuesta por el departamento Administrativo de Función Pública.

Tabla 5 Criterios para definir el nivel de impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Departamento Administrativo de Función Pública

Mapa de Calor

Para identificar zonas de riesgo, se utiliza un mapa de calor que combina probabilidad e impacto.

- Zonas Verdes: Riesgo aceptable.
- Zonas Amarillas: Riesgo moderado que requiere monitoreo continuo.
- Zonas Rojas: Riesgo extremo que requiere tratamiento inmediato.

16. TRATAMIENTO DE RIESGOS DE CORRUPCIÓN

Los riesgos de corrupción no son aceptables en ninguna circunstancia. Se adoptan los siguientes tratamientos:

1. Evitar: Suspender actividades que generen riesgos extremos.
2. Reducir: Implementar controles estrictos para mitigar riesgos identificados.
3. Compartir: Delegar ciertos aspectos del riesgo a terceros que puedan gestionarlo de manera más efectiva.

Los líderes de proceso deben documentar, socializar y monitorear continuamente estos riesgos, reportándolos a la Oficina de Control Interno.

17. MONITOREO DE RIESGOS

El monitoreo permite evaluar la efectividad de los controles implementados y detectar posibles fallos o áreas de mejora. Este proceso se desarrolla en tres niveles:

1. Línea Estratégica:
    - Realiza monitoreos semestrales a través del Comité de Coordinación de Control Interno para garantizar el cumplimiento de la política de riesgos.
2. Primera Línea de Defensa:
    - Los líderes de procesos monitorean mensualmente las acciones de control y enviaran un informe a la Segunda Línea de Defensa (Líder Política de Evaluación y Seguimiento) de manera trimestral, es decir, con corte al 30 de marzo, 30 de junio, 30 de septiembre y 31 de diciembre, dentro de los cinco (5) primeros días hábiles del mes siguiente de cada trimestre.
3. Segunda Línea de Defensa:

Supervisa de manera trimestral la efectividad de los controles aplicados por la primera línea y asegura que se implementen las acciones correctivas necesarias.

4. Tercera Línea de Defensa:

La Oficina de Control Interno realizará auditorías periódicas para validar la eficacia de los controles y emite recomendaciones preventivas.

18. DISEÑO DE CONTROLES

Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración.

La estructura es la siguiente: Para el diseño de controles.

Responsable: Persona responsable de la ejecución del control (tener en cuenta que se debe colocar como responsable a un funcionario de planta y se debe citar el cargo)

Acción: Acción de control, se determina mediante verbos que indican la acción que deben realizar como parte del control, así como su periodicidad.

Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control. (dejar claro aquí, el propósito del control, así como qué hacer en caso de desviaciones y cuál es el registro generado.

Lo anterior, estableciendo su tipología (preventivo, detectivo y/o correctivo) de acuerdo con la conveniencia y efectividad con base a la zona de riesgo inherente que se halló inicialmente.

Se requiere que al iniciar la identificación y formulación de controles o bien sea la revisión periódica de los que se han ejecutado se logre evidenciar las siguientes situaciones en la construcción de los mismos:

1. Describir el responsable de la actividad de control
2. Definir la periodicidad de la actividad de control que hará el responsable
3. Detallar la actividad de control que se realizará
4. Definir la forma en la que va a desarrollar la actividad de control
5. Identificar la desviación que puede sucederle a la actividad de control y determinar cómo sería abordada.
6. Describir la evidencia que queda como resultado del punto 3 y 5

Tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y , por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, presentamos en la siguiente tabla:

Tabla Tipología de controles

Características		Descripción		Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%

	Implementación	Automático	Se ejecutan por un sistema y/o aplicativo de manera automática s	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%

Fuente: Departamento Administrativo de la Función Pública

19. EVALUACIÓN DEL CONTROL

En el último paso metodológico, se determina la evaluación de los controles de acuerdo con la tipología de riesgo, por lo que para los riesgos los controles serán evaluados con base a su diseño desde la tipología (Tabla Tipología de controles).

Ejemplo: El riesgo No 1 tiene dos controles uno detectivos y uno correctivo, su probabilidad inherente es de 60% y un impacto inherente (80%)

Control 1: Detectivos (15%) + Automático (25%) = 40%

Control 2: Correctivo (10%) + Manual (15%) = 25%

Riesgo	Probabilidad inherente	Impacto Inherente	Control 1	Control 2
1	60%	80%	40%	25%

Evaluación control 1:

Probabilidad Inherente = 60

Incidencia en la Probabilidad Residual= 60*40%=24

Probabilidad Residual 1= 60 – 24 = 36

Evaluación control 2:

Impacto Inherente = 80

Incidencia en el Impacto Residual = 80*25%=20

Impacto Residual 1 = 80 – 20 = 60

Zona de Riesgo Residual 1 :

Probabilidad Residual= 36

Impacto Residual = 60

Acciones Ante la Materialización de Riesgos

Cuando un riesgo se materializa, el Instituto Municipal para el Desarrollo Social y Económico de Palmira – IMDESEPAL debe:

1. Informar al Representante de la Alta Dirección
2. Realizar denuncias, si aplica, ante las autoridades competentes.
3. Implementar acciones correctivas inmediatas.
4. Analizar las causas y establecer medidas de mejora.
5. Actualizar el mapa de riesgos y los planes de tratamiento.

Esta Política empezará entrará en vigor a partir de su aprobación por el Comité Institucional de Coordinación de Control Interno.

	Nombres y apellidos	Firma	Fecha
Elaborado por:	Mónica Tovar Rosas		04/12/2025
Revisado por:	Mary Luz Flórez Florez		04/12/2025
Aprobado por:	Jaime Steven Celorio González		04/12/2025
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para firma			