POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

EMPRESA DE DESARROLLO URBANO DEL NORTE DE ANTIOQUIA EDUNA -EICE
2026

SANTA ROSA DE OSOS - ANTIOQUIA

TABLA DE CONTENIDO

Contenido

POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO 1
1. INTRODUCCIÓN 6
2. PROPÓSITO DEL DOCUMENTO 7
3. GLOSARIO 7
3.1 Conceptos clave generales para la gestión del Riesgo 7
3.2 Conceptos clave para la gestión preventiva del riesgo fiscal 8
3.3. Conceptos clave para la gestión de Riesgos de Seguridad de la Información 9
3.4 Conceptos clave para la gestión de Riesgos a la Integridad Pública 9
3.5 Conceptos clave para la gestión de Riesgos en Sector Salud 12
4. POLÍTICA GENERAL 13
5. OBJETIVO PRINCIPAL 14
6. OBJETIVOS ESPECÍFICOS 14
7. ALCANCE 15
8. ÁMBITO DE APLICACIÓN 15
9. INSTITUCIONALIDAD 15
10. REFERENTES NORMATIVOS 17
11. METODOLOGIA PARA LA ADMINISTRACION DEL RIESGO: 19
12. IDENTIFICACIÓN DEL RIESGO 22
13. ANÁLISIS Y DEFINICIÓN DE OBJETIVOS. 23
14. DESCRIPCIÓN DEL RIESGO. 23
15. IDENTIFICACIÓN DEL RIESGO. 24
16. VALORACIÓN DEL RIESGO. 24
16.1 PROBABILIDAD. 24
16.2 IMPACTO 25
16.3 ESTIMACIÓN DEL NIVEL DE SEVERIDAD INICIAL 26
17. DEFINICIÓN Y DIRECTRICES GENERALES DE CONTROL. 27
17.1. Aplicación del Criterio Experto: 27
17.2. Responsabilidad de Operación: 27
18. ESTRUCTURA OBLIGATORIA PARA LA DESCRIPCIÓN DEL CONTROL. 27

18.1. Responsable de Ejecutar el Control:....27
18.2. Acción:....27
18.3. Complemento:....27
19. TIPOLOGÍAS DE CONTROLES INSTITUCIONALES. 27
19.1. Control Preventivo: 28
19.2. Control Detectivo 28
19.3. Control Correctivo:....28
20. ATRIBUTOS DE DISEÑO Y PESOS DE EFICIENCIA. 28
Tabla No. 8: Criterios de Ponderación para el Diseño del Control 28
21. CRITERIOS DE FORMALIZACIÓN DEL CONTROL. 29
21.1. Documentación: 29
21.2. Frecuencia y Oportunidad: 29
21.3. Evidencia (Trazabilidad de la Ejecución):....29
21.4. Ejecución (Fuentes de Información): 29
22. RIESGO RESIDUAL Y ESTRATEGIAS DE TRATAMIENTO....30
22.1 CONCEPTUACIÓN DEL RIESGO RESIDUAL 30
22.2 PRINCIPIO DE MITIGACIÓN ACUMULATIVA DE LOS CONTROLES. 30
- 22.2.1. Aplicación Sucesiva: 30
- 22.2.2. Impacto en la Severidad:....30
22.3. CASO ILUSTRATIVO DE REDUCCIÓN Y RECLASIFICACIÓN RESIDUAL.....31
22.3.1. Comportamiento de las Variables Residuales:....31
22.3.2. Ubicación en la Matriz de Riesgo Residual: 31
22.4. Interpretación Gerencial:....31
22.5 ADOPCIÓN DE ESTRATEGIAS DE TRATAMIENTO....31
22.6 DESARROLLO DE LA ESTRATEGIA DE REDUCCIÓN....31
- 22.6.1. Transferencia del Riesgo:....32
- 22.6.2. Mitigación del Riesgo: 32
22.7 CRITERIOS PARA LA ACEPTACIÓN O EVITACIÓN DEL RIESGO. 32
- 22.7.1. Aceptar el Riesgo: 32
- 22.7.2. Evitar el Riesgo....32
23. GESTIÓN INTEGRAL DEL RIESGO FISCAL 32
23.1 FINALIDAD Y LUCHA CONTRA EL DETRIMENTO PATRIMONIAL....32

23.2 ELEMENTOS CONSTITUTIVOS DE LA GESTIÓN FISCAL INSTITUCIONAL. 32
23.3 EVOLUCIÓN DEL ENFOQUE CONSTITUCIONAL PREVENTIVO 33
23.4 ARQUITECTURA DEL CONTROL FISCAL MULTINIVEL. 33
23.5 DEL CONTROL FISCAL INTERNO (CFI). 34
23.5.1. Naturaleza Jurídica: 34
23.5.2. Responsabilidad de las Líneas de Defensa: 34
23.5.3. Evaluación Externa: 34
23.6 SALVAGUARDA JURÍDICA AL GESTOR PÚBLICO 34
24. DEFINICIÓN DE RIESGO FISCAL. 35
24.1 ELEMENTOS INTEGRANTES DEL RIESGO FISCAL 35
- 24.1.1. Efecto Dañoso: 36
- 24.1.2. Evento Potencial (Causa Raíz 36
24.2 DISTINCIÓN JURÍDICA ENTRE RIESGO FISCAL Y DAÑO PATRIMONIAL. 36
25. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA (SIGRIP) 38
25.1 OBJETO Y ÁMBITO DE APLICACIÓN DEL SIGRIP. 38
25.2 ENFOQUE TRANSVERSAL Y PREVENTIVO DEL SISTEMA 38
25.3 FACTORES DE VULNERABILIDAD Y MATERIALIZACIÓN 38
25.4 ARTICULACIÓN SINCROLÓGICA CON OTROS ESQUEMAS DE RIESGO 38
25.5 ETAPAS DE LA GESTIÓN DEL RIESGO DE INTEGRIDAD 39
25.6 CLASIFICACIÓN OPERATIVA DE LOS CONTROLES DE INTEGRIDAD 39
25.7 ASIGNACIÓN COLECTIVA DE ROLES Y RESPONSABILIDADES 40
25.8 FORTALECIMIENTO DE LA CULTURA DE INTEGRIDAD. 40
25.9 MATRIZ DE REFERENCIA PARA EL ANÁLISIS DE RIESGOS DE INTEGRIDAD Y CORRUPCIÓN. 40
25.10 MATRIZ DE REFERENCIA PARA RIESGOS DE LAFT/FP 42
Tabla No. 13: Esquema de Análisis para Riesgos LA/FT/FP 42
26. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL 42
26.1 OBJETO Y MARCO CONTEXTUAL DE LA SEGURIDAD DIGITAL 42
26.2 METODOLOGÍA PARA EL INVENTARIO DE ACTIVOS DE INFORMACIÓN. 42
26.3 RIESGOS INHERENTES DE SEGURIDAD DIGITAL. 43
26.4 VINCULACIÓN ENTRE LA SEGURIDAD DIGITAL Y LOS RIESGOS DE INTEGRIDAD. 43
26.5 COMPONENTE TÉCNICO DE AMENAZAS 43

Tabla No. 14: Catálogo de Amenazas de Seguridad Digital....43
26.6 COMPONENTE TÉCNICO DE VULNERABILIDADES....45
Tabla No. 15: Catálogo de Vulnerabilidades en la Entidad....45
27. INDICADORES CLAVE DE RIESGO (KRI)....46
27.1 CONCEPTUALIZACIÓN Y NATURALEZA PREVENTIVA DE LOS KRI.....46
27.2. ARTICULACIÓN ESTRATÉGICA ENTRE KPI Y KRI....46
Tabla No. 16: Alcance Comparativo de Aplicación entre KPI y KRI....47
28. ATRIBUTOS, BENEFICIOS Y LIMITACIONES DE LOS KRI....47
28.1 CARACTERÍSTICAS ESENCIALES DE LOS KRI.....47
28.2 BENEFICIOS INSTITUCIONALES DE LA IMPLEMENTACIÓN....47
28.3 LIMITACIONES INHERENTES AL USO DE KRI.....48
28.4 REQUISITOS TÉCNICOS PARA LA CONSTRUCCIÓN DE INDICADORES.....48
28.5 ETAPAS SECUENCIALES PARA LA FORMULACIÓN DE UN KRI....48
28.6 DIRECTRICES PARA LA GESTIÓN EFICIENTE Y GOBERNANZA DE LOS KRI.....49
28.7 CATÁLOGO TÉCNICO DE REFERENCIA DE KRI POR PROCESOS.....49
Tabla No. 17: Indicadores Clave de Riesgo Tipo por Macro proceso....49
29. VIGENCIA Y DEROGATORIA.....50

1. INTRODUCCIÓN

La Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE, como entidad Descentralizada del Orden Municipal ejerce sus funciones constitucionales y legales orientadas a garantizar nuestra misión Institucional. En el marco del Modelo Integrado de Planeación y Gestión MIPG y del Modelo Estándar de Control Interno MECI, la gestión del riesgo constituye un componente estratégico que permite a la entidad anticipar, identificar, valorar y tratar los eventos que puedan afectar el cumplimiento de su misión y el logro de los objetivos institucionales.

La presente Política para Gestión Integral del Riesgo se construye fundamentada en los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 del Departamento Administrativo de la Función Pública (agosto 2025), que actualiza y articula las tipologías de riesgo de gestión, fiscal, de seguridad de la información, de integridad pública (SIGRIP) y, para el sector pertinente, de salud.

El enfoque adoptado por la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA - EICE es de naturaleza preventiva, con especial énfasis en los riesgos de corrupción, contractuales, de detrimento patrimonial, de incumplimiento normativo, reputacionales y de integridad pública, reconociendo que la protección del patrimonio público y la confianza ciudadana constituyen pilares irrenunciables a la Misión Institucional.

Pone a disposición de las entidades la metodología para la Gestión Integral del Riesgo, la cual se actualiza con la incorporación de los lineamientos para la identificación y tratamiento de los riesgos a la integridad pública (SIGRIP), de acuerdo con el componente programático denominado Estrategia Institucional para la Lucha Contra la Corrupción, temática 1 Administración del Riesgo desplegado en el Anexo Técnico de los Programas de Transparencia y Ética Pública, en cumplimiento de lo establecido en la Ley 2195 de 2022 y el Decreto 1122 de 2024.

2. PROPÓSITO DEL DOCUMENTO

Establecer el marco general de actuación de todos los empleados y contratistas de la entidad para la adecuada gestión de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misión y el logro de objetivos institucionales, disminuyendo las potenciales consecuencias negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad, lo anterior en atención a la Política de Gestión Integral del Riesgo del Departamento Administrativo de la Función Pública DAFP Versión 7 de agosto del 2025.

3. GLOSARIO

MIPG: Modelo Integrado de Planeación y Gestión
MECI: Modelo Estándar de Control Interno
CICCI: Comité Institucional de Coordinación de Control Interno
CIGD: Comité Institucional de Gestión y Desempeño

3.1 Conceptos clave generales para la gestión del Riesgo

RIESGO: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
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.
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.
IMPACTO: Conjunto de consecuencias que origina la materialización de un riesgo, es decir, la afectación que éste causaría en la organización, y pueden ser económicas, legales, reputacionales, entre otras.
CAUSA INMEDIATA: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
CAUSA RAÍZ: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
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.
CONTROL: Medida que permite reducir o mitigar un riesgo.

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.
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.
EVENTO: Incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

3.2 Conceptos clave para la gestión preventiva del riesgo fiscal

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. (Ver conceptos de recursos públicos, bien público e intereses patrimoniales de naturaleza pública**).**
RECURSO PÚBLICO: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública**.**
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:
BIEN DE USO PÚBLICO: Aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: las calles, plazas, puentes, vías, parques etc.
BIENES FISCALES: Aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (consejo de estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.
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 expectativos.
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).
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". A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros.
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

3.3. Conceptos clave para la gestión de Riesgos de Seguridad de la Información

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).
CONFIDENCIALIDAD: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
INTEGRIDAD: Propiedad de exactitud y completitud.
DISPONIBILIDAD: Propiedad de ser accesible y utilizable a demanda por una entidad.
VULNERABILIDAD: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
ACTIVOS DE INFORMACION: 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

3.4 Conceptos clave para la gestión de Riesgos a 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 del Riesgo.
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
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.

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)

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 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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

3.5 Conceptos clave para la gestión de Riesgos en Sector Salud

RIESGO EN SALUD: Es el efecto negativo que tiene un evento no deseado o cualquiera de los determinantes de la salud, sobre la salud de una persona o grupos de personas, y que usualmente implica un mayor uso de tecnologías en salud para su atención, o para mitigar sus consecuencias.

SUBSISTEMA DE ADMINISTRACIÓN DEL RIESGO DE CORRUPCIÓN, OPACIDAD Y FRAUDE – SICOF: Conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por el máximo órgano social u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

✓ Mejorar la eficiencia y eficacia en las operaciones de las entidades sometidas a inspección y vigilancia evitando situaciones de Corrupción, Opacidad y Fraude. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.

✓ Prevenir y mitigar la ocurrencia de actos de Corrupción, Opacidad y Fraudes, originados tanto al interior como al exterior de las organizaciones.
✓ Realizar una gestión adecuada de los Riesgos

SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS DE CUMPLIMIENTO (SIARC): Conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por el máximo órgano social u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

✓ Mejorar la eficiencia y eficacia en las operaciones de las entidades sometidas a inspección y vigilancia evitando situaciones de riesgos asociados al LA/FT/FP, Corrupción, Fraude y de soborno transnacional. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.

✓ Prevenir y mitigar la ocurrencia de riesgos asociados al LA/FT/FP, los actos de Corrupción, Fraudes y de soborno transnacional originados tanto al interior como al exterior de las organizaciones.

✓ Realizar una gestión adecuada de los Riesgos.

SISTEMA GENERAL DE SEGURIDAD SOCIAL EN SALUD (SGSSS): Sistema integrado por el Estado, a través del Ministerio de Salud y Protección Social, quien actúa como organismo de coordinación, dirección y control; las Entidades Promotoras de Salud (EPS), responsables de la afiliación y el recaudo de las cotizaciones y de garantizar la prestación del Plan Obligatorio de Salud a los afiliados; y las instituciones prestadores de salud (IPS), que son los hospitales, clínicas y laboratorios, entre otros, encargadas de prestar la atención a los usuarios. También hacen parte del SGSSS las Entidades Territoriales y la Superintendencia Nacional de Salud. El SGSSS tiene como objetivo regular el servicio público esencial de salud y crear condiciones de acceso para toda la población residente del país, en todos los niveles de atención.

SISTEMA DE CONTROL INTERNO: Sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

4. POLÍTICA GENERAL

La Empresa de Desarrollo del Norte de Antioquia EDUNA - EICE, coherente con los componentes y elementos que define el MECI y con las políticas del Sistema de Desarrollo Administrativo, se compromete a ejercer el control efectivo de los eventos de riesgo que puedan afectar negativamente el desarrollo de sus procesos, a través del diagnóstico, identificación, análisis, valoración y administración del riesgo, contribuyendo de esta forma al logro de la Misión y los objetivos de la Entidad.

Aplica para todos los niveles, áreas, procesos y procedimientos de la entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- La gestión preventiva del riesgo Fiscal.
- Los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.
- Gestión de riesgos a la Integridad Pública.
- Gestión de Riesgos en el sector Salud.

5. OBJETIVO PRINCIPAL

Establecer los Lineamientos estratégicos y operativos que orienten la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos en Empresa de Desarrollo del Norte de Antioquia EDUNA - EICE, que puedan afectar el logro de los objetivos institucionales, en concordancia con el Modelo Integrado de Planeación y Gestión MIPG y las mejores prácticas de gestión de riesgos basadas en el marco COSO ERM.

Esta política tiene como propósito fortalecer la gobernanza, la toma de decisiones informadas y la generación de valor público, asegurando la integridad, transparencia y eficiencia en la administración de recursos.

Igualmente, busca promover una cultura organizacional orientada a la anticipación y gestión proactiva de riesgos, contribuyendo al cumplimiento de la misión institucional, la mejora continua y la confianza al interior de la entidad.

6. OBJETIVOS ESPECÍFICOS

Cuando la administración del riesgo se implementa y se mantiene, le permite además a la entidad:

- Aumentar la probabilidad de alcanzar los objetivos y proporcionar a la administración un aseguramiento razonable con respecto al logro de los mismos.
- Ser consciente de la necesidad de identificar y tratar los riesgos en todos los niveles de la entidad.
- Involucrar y comprometer a todos los servidores y contratistas de la entidad en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- Cumplir con los requisitos legales y reglamentarios pertinentes.
- Proteger los recursos de la entidad
- Establecer una base confiable para la toma de decisiones y la planificación.

- Asignar y usar eficazmente los recursos para el tratamiento del riesgo.
- Mejorar la eficacia y la eficiencia operativa.
- Mejorar el aprendizaje y la flexibilidad organizacional.

7. ALCANCE

La presente política aplica a todas las dependencias, procesos y procedimientos, servidores públicos y contratistas de la entidad, en todos los niveles jerárquicos y áreas misionales, estratégicas, de apoyo y evaluativos. 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.

8. ÁMBITO DE APLICACIÓN

La Política para la Gestión Integral del Riesgo es aplicable a todos los procesos, procedimientos, proyectos, productos y servicios de la institución y a las acciones ejecutadas por los servidores públicos durante el ejercicio de sus funciones.

9. INSTITUCIONALIDAD

El Modelo Integrado de Planeación y Gestión - MIPG define para su operación articulada en todas las entidades del orden nacional y territorial, la creación del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87de 1993 y el Decreto 648 de 2017.
Por todo lo anterior la Operatividad Institucional para la Administración Integral del riesgo de EDUNA – EICE queda de la siguiente manera:

Tabla 1. OPERATIVIDAD INSTITUCIONAL PARA LA ADMINISTRACIÓN DEL RIESGO.

INTERNO	**LINEA ESTRATEGICA**	Representante Legal	Decide e Implementa estrategias para la gestión del riesgo y la mejora continua
		Comité Institucional de Gestión y Desempeño CIGD	Analiza la gestión del riesgo y define las mejoras
		Comité Institucional de Coordinación Control Interno CICCI	Analiza eventos y riesgos críticos.
	3ª Línea	Control Interno, Auditoría Interna y/o quien haga sus veces	Responsable de la evaluación independiente, asesora y recomienda.

2ª Línea	Dirección Operativa de Riesgos, Otras dependencias de 2ª Línea Identificadas.	Define metodologías, capacita y hace seguimiento con enfoque preventivo.
3ª Línea	Líderes de Procesos	Responsables de gestionar los riesgos y hacer seguimiento a la 1ª Línea; aplican controles de gerencia operativa.

EXTERNO	Entes Rectores	Gestión y Desempeño Institucional	Propone políticas en materia de gestión y desempeño Institucional.
		Asesor en materia de Control Interno	Propone el fortalecimiento de Control Interno y Auditorías Internas en la entidad.
		Auditoría Interna	Acompañamiento en la Dimensión seguimiento, evaluación y control integral y Política de Control Interno.
		Función Pública DAFP	Lidera la política de Control Interno y brinda asistencia técnica y asesoría en materia de riesgos.

Tabla 2. RESPONSABILIDADES Y COMPROMISOS FRENTE AL RIESGO.

LINEA ESTRATEGICA		
Define el marco general para la gestión Integral del riesgo y el control y supervisa su cumplimiento, está a cargo del Representante Legal y el Comité Institucional de Coordinación de Control Interno CICCI		
PRIMERA LÍNEA DE DEFENSA	SEGUNDA LINEA DE DEFENSA	TERCERA LINEA DE DEFENSA
Desarrolla e implementa procesos de gestión y control de riesgos a través de su identificación, análisis valoración, monitoreo y acciones de mejora. Se encarga del mantenimiento efectivo de Controles Internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. La Gestión	Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen correctamente.	Proporciona información sobre la efectividad del Sistema de Control Interno SCI, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa

operacional identifica, evalúa, controla y mitiga los riesgos.		
RESPONSABLES		
Conformada por los Líderes responsables de procesos, programas o proyectos, Gerente y/o asesor quienes aplican los controles internos en el desarrollo de sus actividades cotidianas, identifican riesgos. analizan causas. definen acciones de mejora y establecen fechas de cumplimiento frente a los hallazgos encontrados. Esta línea constituye el primer nivel operativo y de respuesta frente a la gestión de riesgos y planes de mejoramiento.	A cargo de Servidores Públicos con responsabilidades de monitoreo y Evaluación de controles y riesgos: Representante Legal, Supervisores e Interventores y coordinadores de otros sistemas como instancia asesora y transversal. Rol principal: Monitorear la gestión de riesgo y control, ejecutada por la primera línea de defensa.	A cargo de la oficina de control interno, Auditoría Interna y/o quien haga sus veces. Rol principal: Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad de la OCI. El alcance de este aseguramiento, a través de la Auditoría interna cubre todos los componentes de la OCI.

Para la formulación y operación de la política de Gestión Integral del Riesgo de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA - EICE, es fundamental tener claridad de la misión institucional, sus objetivos, una visión sistémica de la gestión y el modelo de operación por procesos, de manera que no se perciba esta herramienta gerencial como algo aislado del mismo accionar administrativo. Por ende, el diseño se establece a partir de la identificación de los factores internos o externos a la entidad que pueden generar riesgos que afecten el cumplimiento de sus objetivos.

10. REFERENTES NORMATIVOS

El Riesgo y su administración están fundamentados en el siguiente Marco Normativo:

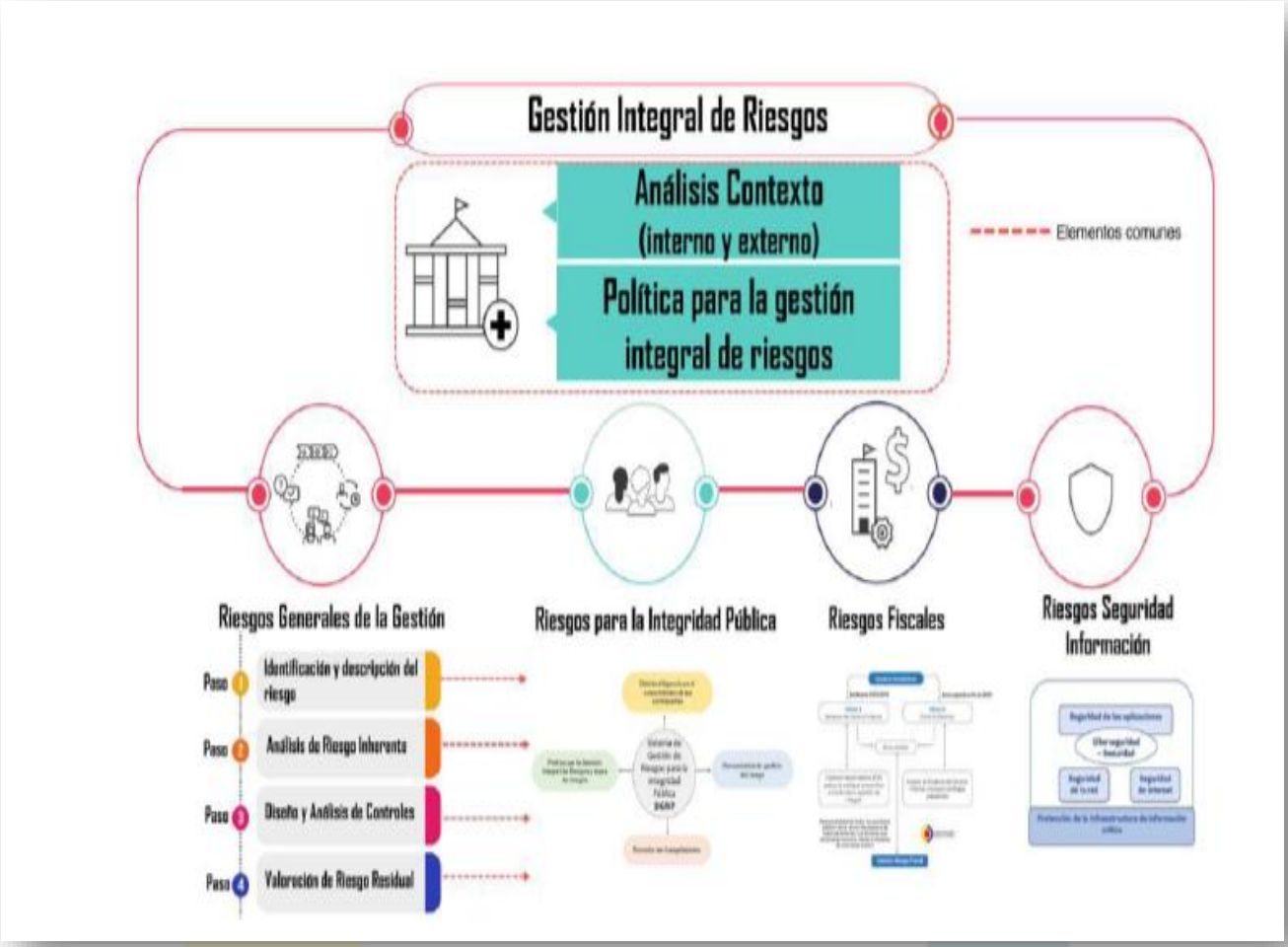
Norma	**Contenido**	
	Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (modificada parcialmente por la Ley 1474 de 2011)

		Artículo 2 OBJETIVOS DEL CONTROL INTERNO: literal a). proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. *Literal f). definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.*
	Ley 489 de 1998	Estatuto Básico de Organización y Funcionamiento de la Administración Pública. *Capítulo VI. Sistema Nacional de Control Interno*
	Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
	Decreto N° 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Titulo 21 Sistema de Control Interno. Capítulo 3 Sistema Institucional y Nacional de Control Interno. Capítulo 5 Elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del estado.
	Ley 1474 de 2011	Estatuto Anticorrupción: Art. 73. Plan anticorrupción y de atención al ciudadano. Que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti tramites y los mecanismos para mejorar la atención al ciudadano
	Decreto N° 2641 de 2012	Por el cual se reglamentan los artículos 73° y 76° de la ley 1474 de 2011.
	Decreto N° 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
	Ley 2013 de 2019	Por medio de cual se busca garantizar el cumplimiento de los principios de Transparencia y publicidad, mediante la publicación de la Declaraciones de bienes, renta y el registro de los conflictos de Interés.
	Decreto N° 648 de 2017 Articulo 7	Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública
	Decreto N° 989 de 2020	"Por el cual adiciona el capítulo 8 al título 21 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, en lo relacionado con las competencias y requisitos específicos para el empleo de jefe de oficina, asesor, coordinador o auditor de control interno o quien haga sus veces en las entidades de la Rama Ejecutiva del orden nacional y territorial"
	Ley 1952 de 2019	Por medio de la cual se expide el código general disciplinario se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario.

	Decreto Ley 403 de 2020	Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.
	Ley 2195 de 2022	Por medio de la cual de adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.
	Ley 610 de 2000	Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías
	Decreto 338 de 2022	"Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"
	Directiva Presidencial 09 de 1999	Lineamientos para la implementación de la política de Lucha contra la corrupción.
	Decreto 1122 de 2024.	Por el cual se reglamenta el Articulo73° de la Ley 1474 de 2011, modificado por el Artículo 31° de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública
	NTC ISO 31000	GESTIÓN DEL RIESGO PRINCIPIOS Y DIRECTRICES
	Guías del Modelo de seguridad y privacidad de la Información (MSPI) de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones	
	Manual Operativo Modelo Integrado de Planeación y Gestión – MIPG. Versión 7 de agosto 28 de 2026 Departamento Administrativo de la Función Pública DAFP.	
	Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 de 2025 - Departamento Administrativo de la Función Pública DAFP.	

11. METODOLOGIA PARA LA ADMINISTRACION DEL RIESGO:

Se aplican las Directrices de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 – 2025, sugerida por el Departamento Administrativo de la Función Pública DAFP.



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 - 2025, Función Pública – DAFP

Tabla 3. FACTORES DE RIESGO.

FACTOR	**DEFINICIÓN**	**DESCRIPCIÓN**
Ejecución y administración	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	Falta de aplicación de los procedimientos
		Falta segregación de funciones
		Errores de grabación, autorización
		Falta de supervisión o interventoría

	organizacional que afecta la capacidad organizacional	
Transacción u Operación (aplica para LA/FT/FP)	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la entidad (naturales o jurídicas)
		Productos (bienes o servicios) que oferta/requiere
		Canales utilizados para la operación Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Fraude Interno
		Soborno
		Gestión inadecuada de conflicto de Intereses
		Corrupción
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad. Daño	Daño a equipos
		Caída de sistemas de información y aplicaciones
		Caída de redes
		Errores de hardware y software
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
Evento Externo	Eventos por situaciones externas que afectan la entidad	Fraude Externo
		Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 - 2025, Función Pública – DAFP

Tabla 4. CLASIFICACIÓN DEL RIESGO.

TIPO	DEFINICION
Gestión Fiscal	Se entiende como aquel que afecta el cumplimiento de los objetivos institucionales debido a deficiencias en la forma en que se planifican, ejecutan, controlan o mejoran los procesos, procedimientos, proyectos y demás actividades de la entidad
	Se define como la posibilidad de que la entidad enfrente afectaciones en su sostenibilidad financiera debido a

	decisiones, acciones u omisiones que comprometan la correcta administración de los recursos públicos.
Seguridad de la información	Se entienden como la posibilidad de que eventos internos o externos afecten la confidencialidad, integridad y disponibilidad de la información institucional, ya sea por fallos tecnológicos, debilidades en los controles, errores humanos o incidentes intencionados que comprometan el tratamiento seguro de los datos y activos informáticos de la entidad
Integridad pública – corrupción	Son la posibilidad de que decisiones, acciones u omisiones de servidores públicos o terceros afecten la transparencia, imparcialidad, legalidad y correcta utilización de los recursos públicos, generando ventajas indebidas, abuso de poder, conflicto de intereses o prácticas que debiliten la confianza ciudadana y el cumplimiento de los objetivos institucionales
Integridad pública - LA_FT_FP	Se entienden como la posibilidad de que la entidad, sus servidores públicos o sus procesos sean utilizados, de manera intencional o inadvertida, para facilitar, encubrir o permitir operaciones relacionadas con el lavado de activos, la financiación del terrorismo o la financiación de la proliferación, afectando la integridad institucional, la confianza ciudadana y el cumplimiento de los principios de legalidad y transparencia.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 - 2025, Función Pública – DAFP

12. IDENTIFICACIÓN DEL RIESGO.

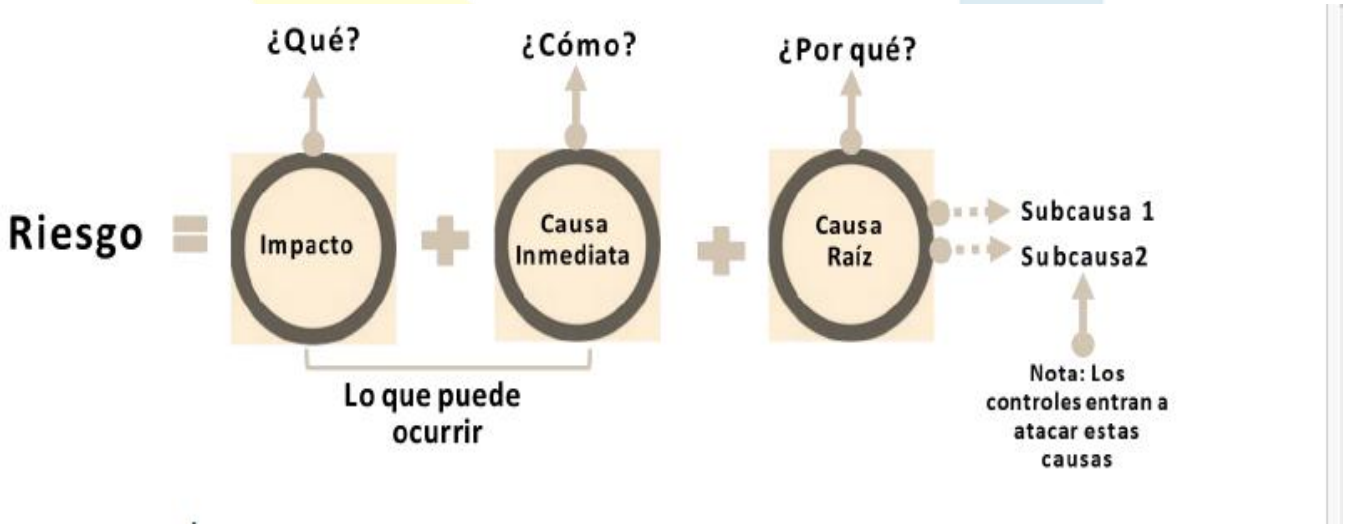
En esta etapa se deben establecer las fuentes o factores del riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para su análisis se pueden utilizar datos históricos, análisis teóricos, opiniones informadas y las necesidades de las partes involucradas.
La identificación del riesgo se realiza determinando las causas, fuentes del riesgo y los eventos con base en el análisis del contexto para la entidad y del proceso, que pueden afectar el logro de los objetivos. Es importante centrarse en los riesgos más significativos para la entidad relacionados con los objetivos de los procesos y los objetivos institucionales.

13. ANÁLISIS Y DEFINICIÓN DE OBJETIVOS.

Le corresponde a la "Segunda Línea de Defensa" (servidores que tengan responsabilidades directas en monitoreo y evaluación de los controles y gestión del riesgo, como jefes de planeación, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, comité de contratación, Comité de Coordinación de Control Interno Institucional, entre otros) el análisis de los objetivos de la entidad tanto del orden estratégico como de procesos.
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.
Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: especifico, medible, alcanzable, relevante y proyectado en el tiempo.
Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero, además, se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de los procesos contribuyan a los objetivos estratégicos.

14. DESCRIPCIÓN DEL RIESGO.

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender, tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:



15. IDENTIFICACIÓN DEL RIESGO.

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la institución, para ello, se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso, que contempla su objetivo y alcance y, también, el análisis ante los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.
La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión de la institución, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características SMART:

- Específico.
- Medible.
- Alcanzable.
- Relevante.
- Temporal.

16. VALORACIÓN DEL RIESGO.

16.1 PROBABILIDAD.

Es la posibilidad de ocurrencia del riesgo. Ésta puede ser medida con criterios de Frecuencia o Factibilidad, donde la primera implica analizar el número de eventos en un periodo determinado (se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo); y la segunda implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo (se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda).

Para evaluar la probabilidad de ocurrencia, se debe hacer uso de los criterios enunciados en la siguiente tabla:

Tabla 5. CRITERIOS PARA DEFINIR LA 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%

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre al evento o riesgo identificado.

En caso de no contar con datos históricos, bajo el concepto de factibilidad se trabajará de acuerdo con la experiencia de los funcionarios que desarrollan el proceso y de sus factores internos y externos.

Cuando las actividades de un proceso o procedimiento son muy repetitivas, la frecuencia debe medirse en términos porcentuales ya que el valor absoluto pierde consistencia.

16.2 IMPACTO.

Son las consecuencias o efectos que puede ocasionar a la organización la materialización del riesgo.
El impacto se debe analizar y calificar, de acuerdo con las consecuencias o efectos, en la fase de identificación del riesgo, ubicándolo en el nivel resultante y llevarlo a la matriz de riesgos en la casilla correspondiente.

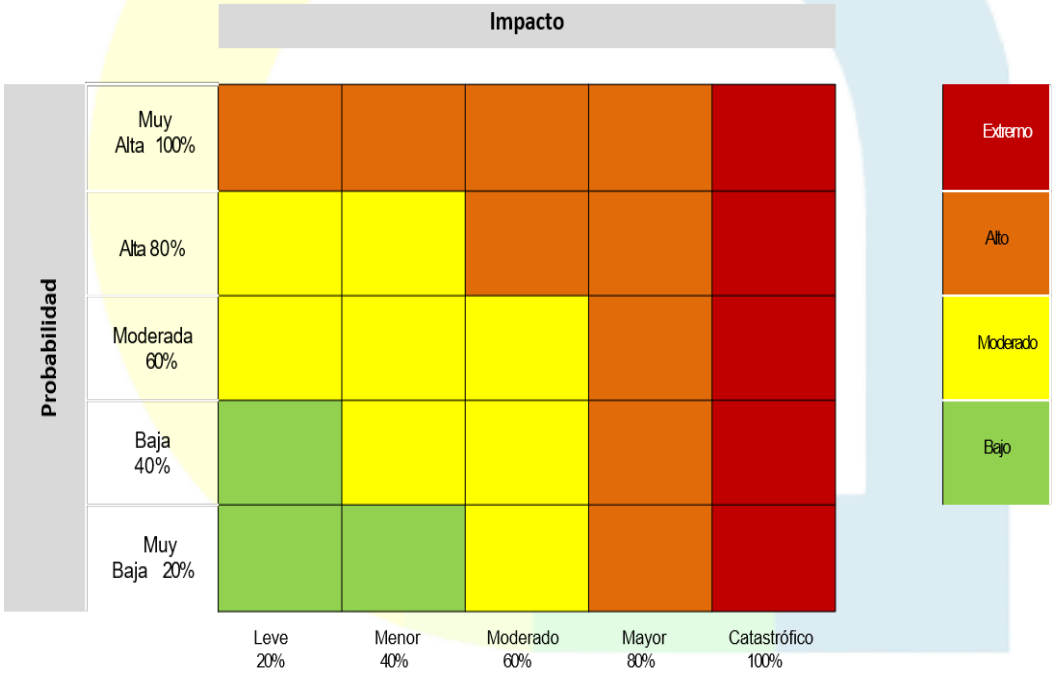
Tabla 6. Criterios para definir el impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Moderado 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.
Menor 60%	Entre 50 y 100 SMLM	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

16.3 ESTIMACIÓN DEL NIVEL DE SEVERIDAD INICIAL. La cuantificación de la severidad o nivel de riesgo inicial se obtendrá mediante el cruce de los valores asignados a la probabilidad y al impacto. La intersección de la fila y la columna correspondientes dentro del plano de la matriz de riesgo determinará de forma exacta la zona de severidad y el cuadrante institucional en el cual queda clasificada la amenaza identificada.

Tabla 7. Matriz de calor



CONCEPTUACIÓN DEL RIESGO INHERENTE. Este diagnóstico primario de la gestión se denomina formalmente Riesgo Inherente. Se define como la exposición a la amenaza que experimenta la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA - EICE ante la total ausencia de acciones, salvaguardas o controles institucionales, es decir,

antes de aplicar cualquier medida que posea la facultad de alterar su probabilidad de ocurrencia o la magnitud de sus consecuencias.

17. DEFINICIÓN Y DIRECTRICES GENERALES DE CONTROL.

Un control se concibe formalmente como toda medida, mecanismo o acción institucional orientada a reducir, mitigar o contener la probabilidad de ocurrencia o la magnitud del impacto de un riesgo identificado. Para su adecuada estructuración dentro de la Institución, se observarán las siguientes directrices:

17.1. Aplicación del Criterio Experto: La identificación y relevamiento de los controles se efectuará de forma directa para cada riesgo, mediante mesas de trabajo o entrevistas con los líderes de proceso y servidores públicos expertos en el desarrollo operativo de sus dependencias, validando la legitimidad del juicio técnico en esta fase.

17.2. Responsabilidad de Operación: Los líderes de cada proceso de la Entidad, en articulación y con el soporte de sus equipos de trabajo, serán los responsables directos de implementar, ejecutar y monitorear permanentemente la efectividad de los controles asignados a sus áreas.

18. ESTRUCTURA OBLIGATORIA PARA LA DESCRIPCIÓN DEL CONTROL.

Con el fin de estandarizar la documentación y facilitar la posterior evaluación de los atributos de los controles, toda salvaguarda que se incorpore en las matrices de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA - EICE deberá redactarse obligatoriamente atendiendo la siguiente estructura sintáctica:

18.1. Responsable de Ejecutar el Control: Especificar con claridad el cargo del servidor público que realiza la actividad de control. En los escenarios donde el control opere de manera totalmente automatizada, se consignará el nombre técnico del software o sistema de información que ejecuta la validación.

18.2. Acción: Determinación del control mediante el uso de verbos en infinitivo que denoten de forma precisa la actividad de revisión, verificación o validación que se lleva a cabo.

18.3. Complemento: Inclusión de los detalles operativos indispensables que permitan identificar sin ambigüedades el objeto, insumo o documento sobre el cual recae la acción de control.

19. TIPOLOGÍAS DE CONTROLES INSTITUCIONALES.

Los controles se clasificarán según el momento procesal en que se ejecutan frente a la cadena de valor o procedimiento, adoptando las siguientes categorías técnicas:

19.1. Control Preventivo: Aquel que se acciona en la fase de entrada del proceso o de manera previa a la realización de la actividad que origina el riesgo. Su propósito fundamental es fijar los requisitos y condiciones técnicas que garanticen el resultado final esperado, evitando la aparición de la amenaza.

19.2. Control Detectivo**:** Medida que se ejecuta de forma simultánea durante el desarrollo de las actividades del proceso. Estos mecanismos identifican la ocurrencia o desviación del riesgo en tiempo real, asumiendo la generación de reprocesos administrativos internos.

19.3. Control Correctivo: Salvaguarda operada en la fase de salida del proceso, una vez se ha materializado de forma efectiva el evento de riesgo. Su objetivo es restablecer las condiciones normales de la operación, conllevando costos implícitos para la entidad.

20. ATRIBUTOS DE DISEÑO Y PESOS DE EFICIENCIA.

La valoración de la calidad del diseño de los controles se efectuará midiendo sus características de eficiencia y automatización. Para el cálculo del peso porcentual de cada control dentro de las matrices municipales, se aplicarán estrictamente los siguientes valores paramétricos determinados por el DAFP:

Tabla No. 8: Criterios de Ponderación para el Diseño del Control

Característica de Eficiencia	**Tipología / Estado**	**Peso Asignado**
Tipo de Control *(Según su momento)*	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Modo de Implementación	Automático	25%
	Manual	15%

PARÁGRAFO. *De conformidad con los estándares de la Guía de Función Pública, la EDUNA – EICE no reconocerá la categoría de controles "semiautomáticos" en sus matrices; por ende, toda medida deberá tipificarse exclusivamente como Manual o Automática.*

21. CRITERIOS DE FORMALIZACIÓN DEL CONTROL.

Complementariamente al diseño, la evaluación evaluará el estado de formalización del control mediante el examen técnico de sus componentes de soporte, oportunidad y trazabilidad, conforme a las siguientes variables básicas:

21.1. Documentación: Valora el grado de soporte normativo u operativo del control, distinguiendo entre:

- *Procedimientos:* Controles estructurados e incorporados formalmente en los manuales de procedimiento y esquemas asociados del Modelo de Operación por Procesos de la Entidad.
- *Sistemas de Información:* Existencia y uso de aplicativos informáticos institucionales que sirvan de soporte directo a la ejecución del control.
- *Otros Esquemas:* Políticas de operación sectoriales, guías técnicas especiales o manuales específicos de la dependencia.

21.2. Frecuencia y Oportunidad: Mide la pertinencia temporal de la aplicación del control para asegurar que su ejecución ayude a prevenir o detectar desviaciones oportunamente. Se clasifica en:

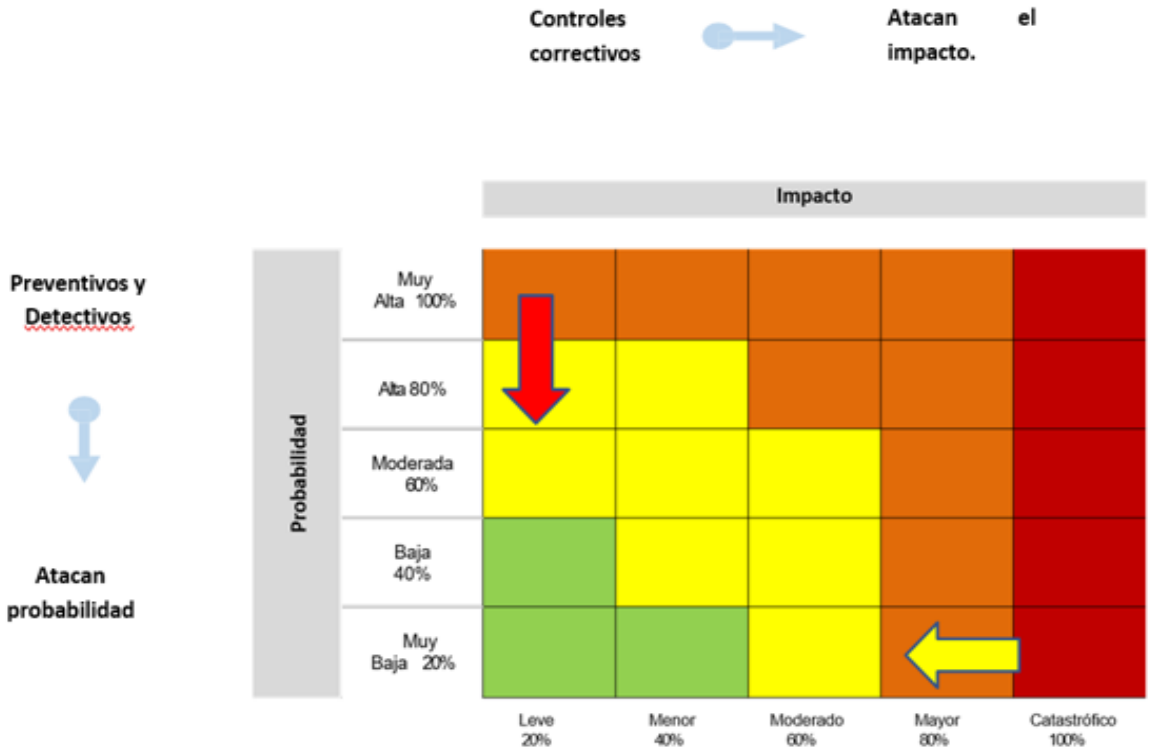
- *Siempre que se ejecuta la actividad.*
- *Periódicamente:* Ejecuciones programadas bajo lapsos definidos (diario, mensual, bimestral, trimestral, semestral o anual).

21.3. Evidencia (Trazabilidad de la Ejecución): Exigencia de dejar constancia o rastro verificable sobre la realización del control, pudiendo constar a través de un *Registro Manual* (firmas físicas, planillas, sellos) o un *Registro Electrónico* (logs de sistemas, correos, reportes digitales).

21.4. Ejecución (Fuentes de Información): Identificación del origen de los datos empleados para operar el control, clasificándose según la procedencia en:

- *Interna:* Formatos, reportes o bases de datos generados formalmente al interior de la alcaldía.
- *Externa:* Información provista por plataformas de terceros de alta confiabilidad (extractos bancarios oficiales, validaciones en SECOP, SIIF, SIGEP, consultas a entes de control, entre otros).
- *Mixta:* Ejecución del control mediante el cruce coordinado de datos provenientes tanto de fuentes internas como externas formales

Tabla N° 9: Movimiento en la Matriz de calor acorde con el tipo de control



22. RIESGO RESIDUAL Y ESTRATEGIAS DE TRATAMIENTO

22.1 CONCEPTUACIÓN DEL RIESGO RESIDUAL. El Riesgo Residual se define técnicamente como el nivel de exposición remanente u obtenido una vez se ha evaluado y aplicado el impacto de la efectividad de los controles institucionales sobre el Riesgo Inherente. Este valor refleja la vulnerabilidad real del proceso tras la ejecución de las salvaguardas diseñadas por la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA - EICE.

22.2 PRINCIPIO DE MITIGACIÓN ACUMULATIVA DE LOS CONTROLES. Para el cálculo técnico del Riesgo Residual dentro de las matrices de la EDUNA - EICE, se establece que los controles operan y mitigan las amenazas de forma acumulativa. En consecuencia, la formulación matemática de la efectividad responderá a las siguientes reglas:

- 22.2.1. Aplicación Sucesiva: Una vez que se aplica el valor de mitigación correspondiente al primer control evaluado, el porcentaje de efectividad del segundo control (y los subsiguientes) no se calculará sobre el valor inicial, sino sobre el valor neto remanente resultante de la aplicación del control inmediatamente anterior.
- 22.2.2. Impacto en la Severidad: El resultado de esta ponderación sucesiva determinará el reajuste final en las escalas de probabilidad o impacto de la amenaza.

22.3. CASO ILUSTRATIVO DE REDUCCIÓN Y RECLASIFICACIÓN RESIDUAL. Con el propósito de guiar a los líderes de proceso de la entidad en el análisis de la efectividad acumulativa, se complementa el caso práctico del proceso de *Gestión de Recursos* detallado en el Artículo 25 del presente instrumento:

22.3.1. Comportamiento de las Variables Residuales: Tras la identificación, documentación y validación de la eficiencia de los controles implementados por el área, se obtienen los siguientes resultados cuantitativos:

Probabilidad Residual: Se logra una contención de la variable, disminuyendo del sesenta por ciento (60% - Moderada) inicial a un **veinticinco coma dos por ciento (25,2% - Baja)**.

Impacto Residual: Se mantiene invariable frente a las secuelas institucionales, registrando una calificación del **ochenta por ciento (80% - Mayor)**.

22.3.2. Ubicación en la Matriz de Riesgo Residual: Al intersectar los nuevos valores en la herramienta técnica de calor, la **Zona de Riesgo Residual se consolida en la categoría Alta**.

22.4. Interpretación Gerencial: Aunque la clasificación final del riesgo se mantenga nominalmente dentro de la zona alta debido a la magnitud crítica de su impacto, el esfuerzo administrativo de los controles aplicados por la dependencia demuestra una mitigación efectiva y real al reducir significativamente la probabilidad de ocurrencia de la amenaza

A continuación, se presenta la estructuración formal de este apartado bajo la técnica normativa de articulado de política pública, adaptada de manera estricta y exclusiva para la **Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE**:

22.5 ADOPCIÓN DE ESTRATEGIAS DE TRATAMIENTO**.** Se entiende por estrategia de respuesta la determinación de carácter administrativo y técnico adoptada por la entidad ante un nivel de exposición específico. Para las operaciones y trámites institucionales que se encuentren en normal funcionamiento, la estrategia se seleccionará evaluando el resultado del **Riesgo Residual**; en contraposición, cuando se trate del diseño de programas, proyectos o procesos nuevos, la decisión se adoptará con fundamento directo en el diagnóstico del **Riesgo Inherente**. Las alternativas autorizadas para el tratamiento de las amenazas son: Aceptar, Reducir o Evitar.

22.6 DESARROLLO DE LA ESTRATEGIA DE REDUCCIÓN**.** Cuando la entidad determine que una amenaza debe ser objeto de intervención para disminuir su severidad, recurrirá a la estrategia de reducción a través de un Plan de Acción Institucional, utilizando las siguientes modalidades

- 22.6.1. Transferencia del Riesgo: Consiste en el traslado técnico y financiero de la carga económica de la amenaza mediante procesos de tercerización operativa o a través de la contratación de pólizas de seguros y coberturas de amparo con entidades del sector asegurador.

  PARÁGRAFO. *De conformidad con los estándares nacionales de administración pública, el uso de la modalidad de transferencia bajo ningún supuesto releva a la Entidad de su responsabilidad reputacional, institucional o de cara a la ciudadanía frente a la continuidad del servicio.*

- 22.6.2. Mitigación del Riesgo: Implica el diseño e implantación de acciones operativas concretas concebidas para menguar la probabilidad de ocurrencia o la fuerza del impacto de la amenaza. El desarrollo de estas medidas correctoras no supondrá de forma obligatoria la creación formal de un control adicional en la matriz, sino la optimización de los procedimientos vigentes.

22.7 CRITERIOS PARA LA ACEPTACIÓN O EVITACIÓN DEL RIESGO. El Comité Institucional de Gestión y Desempeño y los líderes de proceso podrán optar de manera excepcional por las siguientes determinaciones estratégicas:

- 22.7.1. Aceptar el Riesgo: Decisión razonada mediante la cual la institución determina asumir la exposición a la amenaza sin desplegar acciones de mitigación adicionales, reconociendo y cuantificando de forma anticipada las secuelas y efectos jurídicos, operativos y económicos en caso de una eventual materialización.
- 22.7.2. Evitar el Riesgo**:** Determinación de orden gerencial por medio de la cual, tras evaluar la severidad crítica de una amenaza y evidenciar la inviabilidad de su contención, la entidad resuelve suspender de forma definitiva o no iniciar la actividad, trámite o contratación pública que genera dicho escenario de peligro.

23. GESTIÓN INTEGRAL DEL RIESGO FISCAL

23.1 FINALIDAD Y LUCHA CONTRA EL DETRIMENTO PATRIMONIAL**.** Las directrices consagradas en este articulado tienen por objeto orientar el análisis operativo y contractual de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE para blindar los recursos del erario, identificando de manera oportuna aquellas amenazas con la aptitud de provocar un daño patrimonial a la entidad. De conformidad con lo estipulado en la Ley 610 de 2000 y el Decreto Ley 403 de 2020, el menoscabo fiscal se entiende como todo perjuicio, disminución, detrimento, pérdida, pérdida de rentas, deterioro o utilización indebida de los fondos estatales, bienes públicos o intereses patrimoniales de la entidad local.

23.2 ELEMENTOS CONSTITUTIVOS DE LA GESTIÓN FISCAL INSTITUCIONAL. Para efectos del control interno preventivo, la gestión fiscal en la Empresa de Desarrollo

Urbano del Norte de Antioquia EDUNA -EICE comprende las variables y responsabilidades consolidadas en el siguiente esquema técnico:

Tabla N° 11: Componentes de la Gestión Fiscal Institucional.

Interrogante Metodológico	**Definición y Alcance Normativo en la Entidad**
¿Qué es?	El conjunto armónico e integrado de actuaciones, procedimientos y actividades de orden económico, técnico, jurídico y tecnológico que implican la administración del erario.
¿Quién la realiza?	Todos los servidores públicos vinculados a la planta de la EDUNA - EICE, así como las personas naturales o jurídicas de derecho privado que, por mandato legal, contractual o delegación, administren o manejen recursos públicos de la entidad.
¿Qué actividades comprende?	Los procesos transversales de: planeación presupuestal, adquisición de bienes, conservación de activos, administración de inventarios, custodia de títulos, explotación de rentas, enajenación de bienes corporales, consumo de insumos, adjudicación contractual, ejecución del gasto, inversión social, disposición final de bienes, inversión financiera entre otros.
¿Para qué se ejecuta?	Con el objeto exclusivo de asegurar el cumplimiento cabal de los fines esenciales del estado y los cometidos en la visión y la misión de la entidad, bajo estricta sujeción a los principios de economía, eficiencia, eficacia, equidad, celeridad y valoración de costos ambientales vigentes (Ley 610 de 2000, art. 3).

23.3 EVOLUCIÓN DEL ENFOQUE CONSTITUCIONAL PREVENTIVO. En consonancia con lo establecido en los artículos 267 y 268 de la Constitución Política de Colombia, modificados por el Acto Legislativo 04 de 2019, la vigilancia del recurso público trasciende el examen puramente posterior y selectivo. En consecuencia, la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE adopta formalmente el enfoque del control preventivo y concomitante, operando de forma articulada con el Sistema de Control Interno para advertir y detener a tiempo escenarios latentes de daño patrimonial.

23.4 ARQUITECTURA DEL CONTROL FISCAL MULTINIVEL. Con el fin de estructurar una defensa robusta del patrimonio de la entidad, se implementa el modelo de Control Fiscal Multinivel, el cual propicia la interacción coordinada de tres componentes:

- **1. Primer Nivel de Control:** Representado por el Sistema de Control Interno de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE, actuando de forma inmediata en la contención de riesgos operativos.
- **2. Segundo Nivel de Control:** Constituido por el órgano de control fiscal externo competente (Contraloría General de Antioquia y Contraloría General de la República, según el origen de los recursos) a través de sus auditorías y mecanismos concomitantes.
- **3. Componente de Control Social:** Ejercido de forma participativa por la ciudadanía del municipio, las veedurías ciudadanas y los comités de desarrollo y control social.

23.5 DEL CONTROL FISCAL INTERNO (CFI). El Control Fiscal Interno se consagra como el primer eslabón técnico e institucional para velar por los recursos de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE y neutralizar los riesgos fiscales.

23.5.1. Naturaleza Jurídica: El CFI se encuentra integrado formalmente dentro del Sistema de Control Interno de la alcaldía municipal y la entidad, siendo su observancia obligatoria para el total de los servidores públicos de la planta y los contratistas o particulares que administren fondos o intereses patrimoniales locales.

23.5.2. Responsabilidad de las Líneas de Defensa: Su ejecución y monitoreo corresponderá rigurosamente a los responsables de cada línea de defensa en los ámbitos de su competencia legal.

23.5.3. Evaluación Externa: El desempeño y los resultados del Control Fiscal Interno de la entidad serán objeto de examen y auditoría por parte de los Entes de Control Externos competentes, constituyéndose este dictamen en un insumo técnico definitivo para el otorgamiento del fenecimiento de la cuenta fiscal de la entidad.

23.6 SALVAGUARDA JURÍDICA AL GESTOR PÚBLICO. El fortalecimiento del enfoque preventivo dentro del Sistema de Control Interno de la entidad tiene como propósito fundamental brindar seguridad jurídica y amparo normativo a la gestión de los ordenadores del gasto y administradores de recursos de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE.

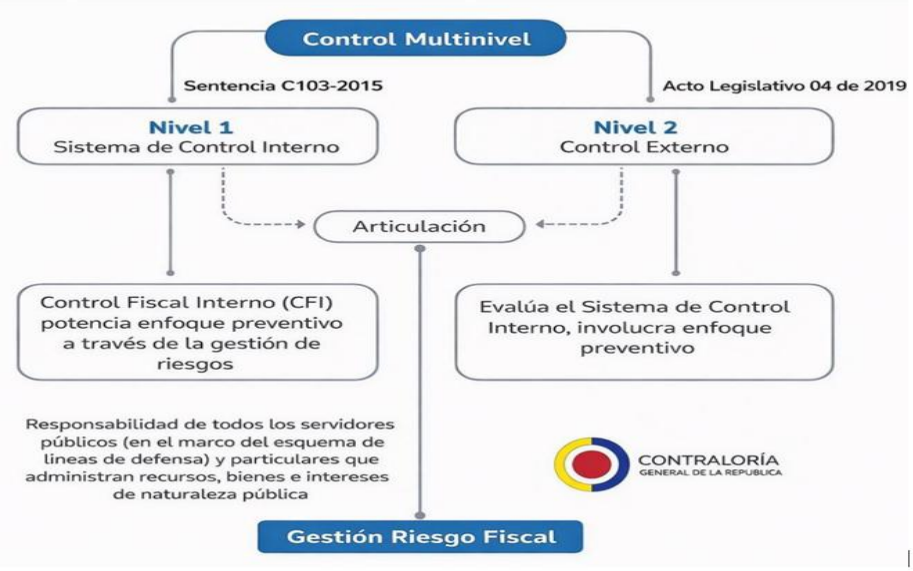
Mediante el mapa de riesgos fiscales actualizado, el sistema proporcionará alertas tempranas de protección para los siguientes roles institucionales:

- El Representante Legal de la Entidad como máxima autoridad.
- Los Servidores Públicos en su condición de ordenadores y ejecutores directos del gasto público.
- Los pagadores e interventores de cuentas.
- Los estructuradores técnicos, jurídicos y financieros de la planeación precontractual.

- Los supervisores e interventores de contratos, convenios y proyectos de la entidad.
- Los coordinadores y profesionales responsables de los procesos de cobro persuasivo, cobro coactivo, y fiscalización.

La correcta observancia y aplicación de estas directrices preventivas blindará la actuación de dichos gestores, evitando la configuración de fallos de responsabilidad fiscal, disciplinaria o penal

ARTICULACIÓN MODELO CONSTITUCIONAL CONTROL FISCAL Y SISTEMA DE CONTROL INTERNO.



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

24. DEFINICIÓN DE RIESGO FISCAL.

En armonía con la estructura metodológica de la *Guía para la Gestión Integral del Riesgo* y los estándares internacionales de la norma ISO 31000, la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE define el riesgo fiscal como el efecto dañoso que se genera sobre los recursos públicos, bienes o intereses patrimoniales de naturaleza pública a causa de la ocurrencia de un evento potencial.

24.1 ELEMENTOS INTEGRANTES DEL RIESGO FISCAL. Para la correcta identificación y gestión en el entorno de la entidad, se desglosan los siguientes elementos conceptuales:

- 24.1.1. Efecto Dañoso: Corresponde a la afectación, menoscabo o perjuicio que experimentarían los fondos presupuestales, activos o expectativas patrimoniales de la entidad si se concreta la amenaza.
- 24.1.2. Evento Potencial (Causa Raíz**):** Representa el conjunto de hechos inciertos, omisiones o acciones no deseadas que poseen la capacidad latente de desencadenar el detrimento del patrimonio público. Para efectos de la presente política, el evento potencial se considerará equivalente a la causa raíz.

24.2 DISTINCIÓN JURÍDICA ENTRE RIESGO FISCAL Y DAÑO PATRIMONIAL.

Los líderes de proceso y órganos de control de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE evitarán confundir el riesgo fiscal con la constitución definitiva del daño patrimonial. El riesgo fiscal se sitúa estrictamente en el plano de la incertidumbre y la potencialidad del efecto perjudicial sobre los recursos y bienes de la entidad; en contraposición, el daño patrimonial constituye una afectación real, concreta, cierta y consumada sobre el erario público, producto de una acción u omisión específica ya ejecutada.

PASO 1: IDENTIFICACIÓN DE LOS RIESGOS FISCALES. Esta fase inicial obliga a los responsables de los procesos de la entidad a caracterizar las amenazas que acechan el patrimonio local, cumpliendo con los siguientes requerimientos obligatorios:

- **1. Establecimiento de Puntos de Riesgo Fiscal:** Se catalogarán bajo esta categoría la totalidad de las actividades, trámites u operaciones institucionales que involucren actividades de gestión fiscal. Asimismo, se incorporarán de forma obligatoria aquellos hitos procedimentales de la entidad en los cuales agencias externas o controles previos hayan emitido advertencias, alertas, hallazgos administrativos con incidencia fiscal o fallos ejecutoriados con responsabilidad fiscal.
- **2. Determinación de Circunstancias Inmediatas:** Corresponde a las situaciones, entornos o modalidades específicas bajo las cuales se exterioriza la amenaza, aclarando que no constituyen el origen básico o la causa raíz del problema. La política reconoce que por cada punto de riesgo fiscal identificado en la dependencia pueden coexistir múltiples circunstancias inmediatas.

IDENTIFICACIÓN DE ÁREAS DE IMPACTO. En la matriz de riesgo fiscal de la entidad, el área de impacto se restringirá y asociará exclusivamente a una consecuencia de índole económica o financiera que afecte negativamente el patrimonio de Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE.

PARÁGRAFO. Los analistas del riesgo deberán considerar que, si bien no todas las contingencias que generan un efecto económico para la institución representan taxativamente un riesgo fiscal, todo riesgo fiscal (entendido como el efecto dañoso sobre recursos, bienes o intereses patrimoniales de la entidad) se traducirá obligatoriamente en un impacto económico medible.

DETERMINACIÓN DE LA CAUSA RAÍZ O HECHO GENERADOR. La causa raíz se define como cualquier acción u omisión que, de llegar a presentarse en la dinámica administrativa, provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de las posiciones patrimoniales de Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE.

La relación entre el hecho generador y el efecto dañoso es estrictamente de causa/efecto; por lo tanto, los líderes de proceso determinarán la causa raíz delimitando con precisión el acto lesivo o la conducta específica que vulnera la integridad de los recursos estatales. Este análisis exige rigurosidad técnica para diferenciar claramente qué factores actúan como causas eficientes y cuáles son meros contextos ambientales.

REGLAS GRAMATICALES PARA LA DESCRIPCIÓN DEL RIESGO FISCAL. La redacción formal de las amenazas en las matrices de la institución adoptará una estructura uniforme y de obligatoria observancia, compuesta por los siguientes cuatro componentes sintácticos:

- **1. Apertura:** El texto deberá dar inicio exclusivamente con la frase **"Posibilidad de..."**, denotando el carácter incierto del evento potencial.
- **2. Impacto (El Qué):** Descripción explícita del efecto dañoso o detrimento potencial que sufrirían los bienes, fondos o intereses del municipio (definiendo claramente el área de impacto económico).
- **3. Circunstancia Inmediata (El Cómo):** Detalle de la situación o el canal operativo a través del cual toma forma el riesgo, sin que constituya su origen base.
- **4. Causa Raíz (El Por qué):** Explicitación de la acción, omisión o conducta negligente que actúa como causa eficiente, generadora directa y condición necesaria para el nacimiento del daño, de tal forma que, si dicha conducta se suprime, la afectación patrimonial no se produce.

PASO 2: VALORACIÓN DEL RIESGO FISCAL INHERENTE. Una vez detectada y estructurada gramaticalmente la amenaza fiscal en la dependencia, se procederá a realizar la medición de su nivel de severidad inicial. Los servidores públicos responsables evaluarán los siguientes componentes técnicos:

- **1. Probabilidad:** Estimación de la viabilidad de ocurrencia del hecho generador.
- **2. Impacto:** Cuantificación del potencial daño económico sobre el erario local.
- **3. Severidad Inherente:** Cruce de las variables anteriores para establecer la ubicación de la amenaza dentro de los cuadrantes de la matriz institucional.

Para dar cumplimiento a estas asignaciones numéricas o cualitativas, los analistas se ceñirán estrictamente a los parámetros establecidos en las tablas y escalas de ponderación definidas previamente en este documento formal de política.

PASO 3: VALORACIÓN DE CONTROLES Y RIESGO RESIDUAL FISCAL. Con el propósito de hallar el índice real de exposición de la institución frente a las amenazas

patrimoniales, se llevará a cabo el examen y ponderación de los mecanismos de mitigación vigentes. Esta fase metodológica comprenderá:

- **1. Controles Identificados:** Relevamiento, caracterización y calificación de la eficiencia y formalización de las salvaguardas fiscales operadas por cada área.
- **2. Determinación del Riesgo Residual:** Cálculo del nivel de riesgo definitivo resultante tras aplicar la efectividad acumulativa de los controles validados frente a la severidad del riesgo inherente.

Los resultados analíticos y las calificaciones finales del Riesgo Residual Fiscal se computarán utilizando de forma obligatoria las matrices y tablas paramétricas dispuestas por la institución en la presente resolución de política pública.

25. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA (SIGRIP)

25.1 OBJETO Y ÁMBITO DE APLICACIÓN DEL SIGRIP. Establézcanse los lineamientos técnicos e institucionales para la implementación, operación, monitoreo y fortalecimiento continuo del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) en la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE, Este sistema es de aplicación obligatoria para la totalidad de los procesos, dependencias, servidores públicos, contratistas y demás actores que intervengan en el desarrollo de la gestión institucional de la entidad descentralizada territorial.

25.2 ENFOQUE TRANSVERSAL Y PREVENTIVO DEL SISTEMA. El SIGRIP se constituye como un enfoque actualizado, transversal y proactivo para la administración de las amenazas que afecten la integridad pública, entendida esta como la coherencia absoluta entre los valores, principios y actuaciones de los servidores públicos en el ejercicio de sus funciones. Su diseño metodológico trasciende la mera identificación de hechos de corrupción consumados, concentrando sus esfuerzos en la mitigación de aquellas condiciones institucionales, organizacionales y humanas que actúan como facilitadoras de conductas indebidas o contrarias a la ética pública y a los fines esenciales del Estado.

25.3 FACTORES DE VULNERABILIDAD Y MATERIALIZACIÓN. Para efectos del SIGRIP, se reconocerá que los riesgos de integridad y corrupción se materializan ante la coexistencia de incentivos indebidos, presiones internas o externas, oportunidades derivadas de la discrecionalidad administrativa o debilidades estructurales en los controles institucionales. Estas situaciones dan origen a prácticas lesivas como el abuso de poder, el favorecimiento indebido, los conflictos de interés no gestionados, la opacidad o falta de transparencia, el fraude, el soborno y el incumplimiento de los deberes funcionales.

25.4 ARTICULACIÓN SINCROLÓGICA CON OTROS ESQUEMAS DE RIESGO. El SIGRIP operará de manera armónica y complementaria con los demás sistemas de administración del riesgo adoptados por la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE, en especial con el Sistema de Administración del Riesgo de

Lavado de Activos y Financiación del Terrorismo (SARLAFT), cuando la naturaleza jurídica, misional y operativa de la dependencia así lo exija. Esta articulación tiene como fin evitar duplicidades, robustecer las salvaguardas existentes y asegurar la eficiencia presupuestal en procesos sensibles como la contratación pública, la ordenación del gasto, el relacionamiento con terceros y la toma de decisiones estratégicas.

25.5 ETAPAS DE LA GESTIÓN DEL RIESGO DE INTEGRIDAD**.** De conformidad con la *Guía para la Gestión Integral del Riesgo* del Departamento Administrativo de la Función Pública (DAFP) en su Versión 7, y el Modelo Integrado de Planeación y Gestión (MIPG), la administración de riesgos de integridad se desarrollará rigurosamente a través de las siguientes etapas:

- **1. Identificación del Riesgo:** Reconocimiento de actividades y decisiones vulnerables dentro del flujo de los procesos; determinación de las áreas de impacto (económico, reputacional, legal y de contagio) y distinción entre causas inmediatas y causas raíz.
- **2. Análisis del Riesgo Inherente:** Evaluación cuantitativa o cualitativa de la probabilidad de ocurrencia y el impacto potencial de la amenaza, determinando su severidad para priorizar el tratamiento institucional.
- **3. Tratamiento del Riesgo:** Diseño, validación e implantación de controles orientados a mitigar los factores generadores de la amenaza.
- **4. Valoración del Riesgo Residual:** Evaluación del nivel de exposición remanente tras la aplicación de los controles para confrontarlo con el apetito de riesgo institucional y determinar su aceptabilidad.
- **5. Seguimiento y Monitoreo:** Verificación permanente de la efectividad de las salvaguardas, actualización del inventario de riesgos y adopción de acciones de mejora continua.

25.6 CLASIFICACIÓN OPERATIVA DE LOS CONTROLES DE INTEGRIDAD**.** Las medidas de control diseñadas e implementadas por los líderes de proceso bajo el marco del SIGRIP se clasificarán en:

- **1. Controles Preventivos:** Diseñados para neutralizar las causas raíz antes de su ocurrencia, mediante la formalización de políticas institucionales claras, procedimientos documentados, segregación de funciones y acciones permanentes de formación en ética.
- **2. Controles Detectivos:** Orientados a identificar de manera oportuna la configuración de irregularidades o desviaciones mediante la ejecución de auditorías internas, revisiones de cumplimiento, conciliaciones y sistemas automatizados de monitoreo.
- **3. Controles Correctivos:** Concebidos para reaccionar ante el riesgo materializado, mitigando su impacto mediante la activación de procesos sancionatorios, acciones disciplinarias y medidas de reparación institucional.

25.7 ASIGNACIÓN COLECTIVA DE ROLES Y RESPONSABILIDADES. La operatividad del SIGRIP responde a un modelo de responsabilidad compartida, estructurado de la siguiente manera:

- **1. Representante Legal:** Responsable de definir el "tono ético" de la entidad, promover la cultura de legalidad y garantizar la asignación de recursos indispensables para el sistema.
- **2. Líderes de Proceso:** responsables técnicos de identificar, analizar, valorar y gestionar las amenazas de integridad dentro de sus respectivas dependencias operativas.
- **3. Instancias de Control Interno y/o quien haga sus veces:** Encargadas de ejercer el seguimiento continuo y la evaluación independiente sobre la eficacia y madurez del sistema.
- **4. Servidores Públicos y Contratistas:** Obligados a encuadrar su conducta diaria en los principios de transparencia, responsabilidad y honestidad, constituyendo de forma directa la primera barrera y el principal control del sistema.

25.8 FORTALECIMIENTO DE LA CULTURA DE INTEGRIDAD. La

Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE potenciará el SIGRIP a través de la apropiación obligatoria del Código de Integridad, la rendición pública de cuentas, la gestión estricta de conflictos de interés y la habilitación de canales de denuncia institucionales seguros que garanticen la confidencialidad y la protección del denunciante, articulando esfuerzos con la Secretaría de Transparencia de la Presidencia de la República y la Unidad de Información y Análisis Financiero (UIAF).

25.9 MATRIZ DE REFERENCIA PARA EL ANÁLISIS DE RIESGOS DE INTEGRIDAD Y CORRUPCIÓN. Para la formulación de las matrices institucionales, los líderes de proceso se guiarán por los siguientes parámetros conceptuales de causa/efecto:

Tabla N° 12: Referente Técnico para Análisis de Riesgos de Integridad

Manifestación del Riesgo	**Causa Inmediata / Conducta Asociada**	**Causa Raíz / Contexto del Proceso**	**Área de Impacto Institucional**
Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para	Deficiencias o vacíos en la descripción de la actividad específica dentro del flujo	Afectación de índole económica, detrimento financiero y/o menoscabo

Manifestación del Riesgo	Causa Inmediata / Conducta Asociada	Causa Raíz / Contexto del Proceso	Área de Impacto Institucional
	beneficio de carácter personal o de terceros.	del proceso analizado.	reputacional de la entidad.
Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (financiero o no), directa o indirectamente, en violación de la ley, como incentivo para actuar o abstenerse de actuar.	Deficiencias o vacíos en la descripción de la actividad específica dentro del flujo del proceso analizado.	Fenómenos transversales de corrupción con afectación económica y de confianza ciudadana.
Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (financiero o no), directa o indirectamente, en violación de la ley aplicable, como incentivo o recompensa.	Deficiencias o vacíos en la descripción de la actividad específica dentro del flujo del proceso analizado.	Fenómenos transversales de corrupción con afectación económica y de confianza ciudadana.
Conflicto de Interés	Decidir o intervenir en un asunto sobre el cual el servidor público tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su círculo familiar o de socios.	Deficiencias o vacíos en la descripción de la actividad específica dentro del flujo del proceso analizado.	Rompimiento de la imparcialidad con afectación reputacional y legal institucional.
Corrupción	Desviar deliberadamente la gestión administrativa o los recursos públicos y privados con el propósito de obtener un beneficio propio o para un tercero.	Deficiencias o vacíos en la descripción de la actividad específica dentro del flujo del proceso analizado.	Destrucción del valor público, afectación económica, legal y reputacional severa.

25.10 MATRIZ DE REFERENCIA PARA RIESGOS DE LAFT/FP. En los procesos identificados con exposición a riesgos de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP), se aplicará obligatoriamente la siguiente estructura técnica parametrizada:

Tabla No. 13: Esquema de Análisis para Riesgos LA/FT/FP

Componente Técnico	**Criterio de Identificación y Contenido Obligatorio**
Áreas de Impacto	Afectación multidimensional clasificada bajo las escalas de impacto Económico, Reputacional, Legal, Operativo o de Contagio Institucional.
Causa Inmediata	Instrumentación o utilización de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE para dar apariencia de legalidad a activos de origen ilícito, o para canalizar recursos hacia actividades terroristas o de proliferación de armas de destrucción masiva.
Causa Raíz	Descripción detallada y pormenorizada de la operación, trámite o transacción específica dentro del flujo del proceso donde radica la vulnerabilidad.

26. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

26.1 OBJETO Y MARCO CONTEXTUAL DE LA SEGURIDAD DIGITAL. Establézcanse las directrices para la gestión integral de los riesgos asociados al uso de las Tecnologías de la Información y las Comunicaciones (TIC) en la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA -EICE, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información, blindar los activos digitales, garantizar la continuidad de los servicios y sostener la confianza de la ciudadanía. La seguridad digital se reconoce como un componente estratégico interconectado con el Sistema de Control Interno y el MIPG.

26.2 METODOLOGÍA PARA EL INVENTARIO DE ACTIVOS DE INFORMACIÓN. Toda dependencia de la institución deberá identificar, clasificar y asociar sus activos de información (datos, sistemas, plataformas de recaudo, catastro, contratación, etc.) a los objetivos institucionales. Para la generación y actualización del inventario de activos, se

adoptará rigurosamente el procedimiento técnico establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2026):

- **Paso 1:** Listar de manera detallada los activos de información por cada proceso institucional.
- **Paso 2:** Identificar formalmente el dueño (responsable directo) y el custodio técnico del activo.
- **Paso 3:** Clasificar los activos de acuerdo con su tipo (hardware, software, red, etc.).
- **Paso 4:** Clasificar la información según los niveles de reserva y confidencialidad legal.
- **Paso 5:** Determinar técnicamente el nivel de criticidad del activo para la operación municipal.
- **Paso 6:** Identificar si el activo guarda relación o soporta alguna Infraestructura Crítica Cibernética Nacional.

26.3 RIESGOS INHERENTES DE SEGURIDAD DIGITAL. Para efectos de la matriz institucional de riesgos de TIC, se declaran y tipifican tres (3) riesgos inherentes de obligatoria evaluación:

- **1. Pérdida de la Confidencialidad:** Acceso no autorizado o divulgación deliberada o fortuita de datos e información reservada o sensible.
- **2. Pérdida de la Integridad:** Modificación, alteración, manipulación o destrucción no autorizada de la información, registros o bases de datos misionales.
- **3. Pérdida de la Disponibilidad:** Interrupción, degradación o caída de los sistemas y servicios digitales que impida la continuidad operativa de la alcaldía.

26.4 VINCULACIÓN ENTRE LA SEGURIDAD DIGITAL Y LOS RIESGOS DE INTEGRIDAD. Se reconoce normativamente que los incidentes de seguridad digital constituyen factores facilitadores de riesgos de corrupción e integridad. En consecuencia, los controles informáticos de acceso, segregación de funciones, pistas de auditoría y trazabilidad técnica deberán alinearse de manera complementaria con el SIGRIP para neutralizar la manipulación de información financiera, contractual o tributaria por parte de actores internos o terceros (proveedores y operadores tecnológicos bajo acuerdos de niveles de servicio - ANS/SLA).

26.5 COMPONENTE TÉCNICO DE AMENAZAS. De conformidad con el estándar internacional ISO/IEC 27001:2022 adoptado por el MinTIC, se identifican las causas potenciales de incidentes no deseados, clasificadas por su origen en Deliberadas (D), Fortuitas (F) o Ambientales (A):

Tabla No. 14: Catálogo de Amenazas de Seguridad Digital

Categoría de la Amenaza	Evento de Amenaza Específico	Origen Técnico
Daño Físico	Fuego, Agua, Contaminación, Accidente Importante, Destrucción del equipo o medios, Polvo, corrosión o congelamiento.	F, D, A
Eventos Naturales	Fenómenos climáticos, Fenómenos sísmicos, Fenómenos volcánicos, Fenómenos meteorológicos, Inundación.	A
Pérdida de Servicios Esenciales	Fallas en el sistema de suministro de agua o aire acondicionado, Pérdida de suministro de energía eléctrica.	A
Pérdida de Servicios Esenciales	Falla en equipo o redes de telecomunicaciones.	D, F
Perturbación por Radiación	Radiación electromagnética, Radiación térmica, Impulsos electromagnéticos.	D, F
Compromiso de la Información	Interceptación de señales de interferencia comprometida, Espionaje remoto, Escucha encubierta, Hurto de medios, documentos o equipos, Recuperación de medios reciclados o desechados.	D
Compromiso de la Información	Divulgación de datos, Procesamiento de datos provenientes de fuentes no confiables.	D, F
Compromiso de la Información	Manipulación con hardware, Manipulación con software.	D
Compromiso de la Información	Detección o rastreo de la posición.	D, F
Fallas Técnicas	Fallas o mal funcionamiento del equipo hardware, Saturación del sistema de información, Mal funcionamiento del software, Incumplimiento en el mantenimiento del sistema de información.	F

Categoría de la Amenaza	Evento de Amenaza Específico	Origen Técnico
Acciones no Autorizadas	Uso no autorizado del equipo, Copia fraudulenta de software, Uso de software falso o copiado, Corrupción deliberada de datos, Procesamiento ilegal de datos.	D
Compromiso de las Funciones	Error en el uso y operación de los sistemas.	D, F
Compromiso de las Funciones	Abuso de derechos de acceso, Falsificación de derechos, Negación de acciones, Incumplimiento o indisponibilidad del personal crítico.	D

26.6 COMPONENTE TÉCNICO DE VULNERABILIDADES. Se catalogan las debilidades inherentes a los activos o controles de la entidad que pueden ser explotadas por las amenazas descritas en el artículo anterior, clasificadas por su entorno:

Tabla No. 15: Catálogo de Vulnerabilidades en la Entidad

Entorno del Activo	Vulnerabilidades Específicas Catalogadas
Hardware	Mantenimiento insuficiente, Ausencia de esquemas de reemplazo periódico, Sensibilidad a la radiación electromagnética, Susceptibilidad a variaciones de temperatura (polvo y suciedad), Almacenamiento sin protección, Falta de cuidado en la disposición final, Copia no controlada.
Software	Ausencia o insuficiencia de pruebas de software, Ausencia de terminación de sesión automática, Ausencia de registros de auditoría (*logs*), Asignación errada de derechos de acceso, Interfaz de usuario compleja, Ausencia de documentación, Fechas incorrectas, Ausencia de mecanismos de identificación y autenticación de usuarios, Contraseñas sin protección, Software nuevo o inmaduro.
Red	Ausencia de pruebas de envío o recepción de mensajes, Líneas de comunicación sin protección, Conexión deficiente de cableado,

Entorno del Activo	Vulnerabilidades Específicas Catalogadas
	Tráfico sensible sin protección, Existencia de punto único de falla (*Single Point of Failure*).
Personal	Ausencia prolongada del personal, Entrenamiento insuficiente, Falta de conciencia en seguridad digital, Ausencia de políticas de uso aceptable, Trabajo no supervisado de personal externo o de empresas de limpieza.
Lugar / Planta Física	Uso inadecuado de los controles de acceso al edificio, Áreas físicas susceptibles a inundación, Red eléctrica inestable, Ausencia de protección física en puertas o ventanas.
Organización	Ausencia de procedimiento de registro/retiro de usuarios, Ausencia de proceso para supervisión periódica de derechos de acceso, Ausencia de control de los activos fuera de las instalaciones, Ausencia de acuerdos de nivel de servicio (ANS o SLA), Ausencia de mecanismos de monitoreo para brechas en la seguridad, Ausencia generalizada de procedimientos y políticas (uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia).

27. INDICADORES CLAVE DE RIESGO (KRI)

27.1 CONCEPTUALIZACIÓN Y NATURALEZA PREVENTIVA DE LOS KRI. Establézcanse los Indicadores Clave de Riesgo (KRI, por sus siglas en inglés *Key Risk Indicators*) como la herramienta estratégica, métrica y de carácter eminentemente preventivo para el monitoreo de las amenazas institucionales. A diferencia de los indicadores tradicionales de gestión, los KRI no se orientan a describir hechos consolidados o pasados, sino a advertir de manera anticipada sobre condiciones, comportamientos o tendencias variables que puedan derivar en la materialización de un riesgo, tanto por factores internos de la operación como por eventos o transformaciones del entorno externo.

27.2. ARTICULACIÓN ESTRATÉGICA ENTRE KPI Y KRI. Los KRI no podrán diseñarse de forma aislada, sino que deberán guardar una relación vinculante y directa con la plataforma estratégica de la institución (misión, visión, objetivos estratégicos, plan estratégico) y sus procesos. El sistema de control interno y/o quien haga sus veces adoptará una visión integrada que permita analizar simultáneamente el desempeño y el riesgo, articulando los KRI con los Indicadores Clave de Rendimiento o Desempeño (KPI):

Tabla No. 16: Alcance Comparativo de Aplicación entre KPI y KRI

Criterio Técnico	Indicadores Clave de Desempeño / Proceso (KPI)	Indicadores Clave de Riesgo (KRI)
Enfoque Temporal	Miden el rendimiento pasado (enfoque retrospectivo), ofreciendo información sobre qué tan bien se lograron las metas.	Se concentran en el pronóstico y tendencias futuras (enfoque prospectivo), anticipando problemas antes de su ocurrencia.
Propósito de Medición	Permiten medir periódicamente el desempeño general de la entidad y evaluar la ejecución de programas, planes y proyectos.	Proporcionan una señal temprana, oportuna y constante de una exposición creciente al riesgo en diversas áreas operativas.
Alineación Operativa	Se definen tomando como referencia las metas establecidas por procesos, unidades u operaciones clave de la organización.	Proporcionan información útil sobre riesgos emergentes y potenciales que pueden impactar los objetivos estratégicos.
Toma de Decisiones	Ofrecen información sobre aspectos críticos de la operación que requieren mayores recursos, mejorando la planificación.	Facilitan el proceso de generación de informes, el escalamiento de alertas y la aplicación de medidas de mitigación inmediatas.

28. ATRIBUTOS, BENEFICIOS Y LIMITACIONES DE LOS KRI

28.1 CARACTERÍSTICAS ESENCIALES DE LOS KRI. Para que un indicador sea validado dentro del inventario de riesgos institucional, deberá cumplir con las siguientes características como señal de alerta eficaz:

- **1. Relevancia:** Debe concentrarse exclusivamente en los riesgos críticos o prioritarios de la entidad, partiendo de los objetivos organizacionales.
- **2. Capacidad Predictiva:** Debe permitir la inferencia de escenarios futuros o desfavorables mediante la observación de tendencias.
- **3. Objetividad y Mensurabilidad:** Debe expresarse obligatoriamente de forma matemática o cuantitativa (montos, porcentajes, tasas, frecuencias) con valores determinables en el tiempo.
- **4. Claridad:** Debe ser comprensible, inequívoco y fácilmente entendible por la totalidad de los servidores públicos de la dependencia.

28.2 BENEFICIOS INSTITUCIONALES DE LA IMPLEMENTACIÓN**.** La adopción metódica de los KRI generará para la entidad los siguientes impactos positivos:

- **1.** Expresar y consolidar un fuerte compromiso del Representante Legal con la gestión proactiva del riesgo en todos los niveles institucionales.
- **2.** Facilitar las labores de monitoreo efectivo y oportuno, proveyendo un marco estructurado para el tratamiento de las amenazas antes de que afecten la estabilidad financiera o reputacional.
- **3.** Proporcionar señales de alerta temprana indispensables para prevenir pérdidas inminentes, protegiendo el crecimiento institucional y la sostenibilidad de los servicios a largo plazo.
- **4.** Servir de soporte técnico para las decisiones en los Comités de Gestión y Desempeño y Coordinación de Control Interno.

28.3 LIMITACIONES INHERENTES AL USO DE KRI. Al analizar e interpretar los resultados de los KRI, la Oficina de Control Interno y/o quién haga sus veces y los líderes de proceso deberán considerar las siguientes restricciones metodológicas:

- **1. No Sustitución del Conocimiento:** Un indicador aislado no reemplaza la comprensión integral y profunda del entorno y las dinámicas internas de la entidad territorial.
- **2. Dependencia de Fuentes:** La precisión de la métrica está supeditada a la calidad de la información provista por los sistemas origen; fuentes con errores o desactualizadas alterarán el resultado del indicador.
- **3. Vulnerabilidad de los Planes de Acción:** Si los planes de mitigación o las metodologías institucionales presentan fallas estructurales en su formulación, el KRI reflejará distorsiones en su efectividad.

28.4 REQUISITOS TÉCNICOS PARA LA CONSTRUCCIÓN DE INDICADORES. Todo KRI formalizado en la entidad deberá diseñarse de manera técnica, asegurando que sea medible, cuantificable, preciso y aplicable a riesgos específicos previamente tipificados en los mapas de riesgo institucionales.

28.5 ETAPAS SECUENCIALES PARA LA FORMULACIÓN DE UN KRI. Los líderes de proceso desarrollarán la construcción de los KRI atendiendo estrictamente el siguiente orden metodológico:

- **1. Definición del Objetivo del Indicador:** Establecer qué se pretende medir, asegurando su alineación estricta con los objetivos del proceso, plan, programa o proyecto evaluado.
- **2. Identificación del Riesgo Relacionado:** Determinar la amenaza específica del mapa de riesgos que se busca monitorear, analizando sus causas raíz y el histórico de eventos pasados.
- **3. Definición de Aspectos Operativos:** Fijar detalladamente la unidad de medida, la periodicidad de captura, y los factores internos o externos que alteran la métrica.
- **4. Análisis de la Línea Base (KPI):** Estudiar los indicadores de desempeño existentes del proceso para utilizarlos como fundamento de medición operativa.

- **5. Formulación Estructural del KRI:** Documentar formalmente la ficha técnica del indicador, la cual deberá contener como mínimo:
  - **a)** Nombre claro e inequívoco del indicador.
  - **b)** Descripción detallada del objeto de medición.
  - **c)** Fórmula matemática de cálculo.
  - **d)** Fuente oficial de información (sistemas internos, reportes de auditoría, bases de datos externas, etc.).
  - **e)** Frecuencia de medición, reporte y seguimiento.
  - **f)** Umbrales de alerta parametrizados (Escalas de tolerancia: Verde / Amarillo / Rojo).
- **6. Asignación de Responsabilidades:** Designar formalmente al servidor público encargado del cálculo, reporte y custodia del indicador.

28.6 DIRECTRICES PARA LA GESTIÓN EFICIENTE Y GOBERNANZA DE LOS KRI. Con el fin de garantizar la eficiencia operativa del sistema de alertas, la institución adoptará las siguientes reglas de gestión:

- **1. Criterio de Selectividad (Optimización):** Se limitará la cantidad de KRI institucionales. Las dependencias se concentrarán exclusivamente en aquellas métricas asociadas a riesgos de mayor impacto estratégico. No se trata de medir la totalidad de las actividades, sino de medir con alta calidad técnica.
- **2. Diversidad de Fuentes:** El diseño y revisión de los KRI deberá nutrirse tanto de variables internas como de datos del entorno externo sectorial para capturar riesgos emergentes no mapeados originalmente.
- **3. Automatización Progresiva:** Las dependencias TIC y de Planeación promoverán el uso de aplicativos informáticos y tableros de control automatizados que limiten la manipulación manual de datos, optimicen los tiempos de procesamiento y estandaricen los reportes.
- **4. Esquema de Comunicación y Escalabilidad:** Los resultados de los KRI deberán comunicarse periódicamente conforme a las Líneas de Defensa del Modelo Estándar de Control Interno (MECI). Los líderes de proceso gestionarán el riesgo en la operación diaria, mientras que las desviaciones críticas que superen los umbrales de tolerancia permitidos serán escaladas de forma obligatoria al Representante Legal para la adopción de ajustes estratégicos.

28.7 CATÁLOGO TÉCNICO DE REFERENCIA DE KRI POR PROCESOS.

Adóptense las siguientes métricas de referencia como parámetros mínimos obligatorios para el diseño de indicadores de riesgo en los macro procesos transversales de la entidad:

Tabla No. 17: Indicadores Clave de Riesgo Tipo por Macro proceso

Macro proceso / Proceso Asociado	Indicador Clave de Riesgo (KRI)	Métrica Técnica / Fórmula de Control
Tecnologías de la Información y las Comunicaciones (TIC)	Tiempo de interrupción de aplicativos o sistemas críticos en el mes.	Número total de horas acumuladas de indisponibilidad o caída de aplicativos críticos al mes.
Gestión Financiera	Reportes oficiales emitidos al regulador o entes de control fuera del tiempo legal establecido.	Número de reportes mensuales institucionales remitidos de forma extemporánea o fuera de términos.
Atención al Usuario / Ciudadano	Reclamos de usuarios por incumplimiento de términos de ley o reiteraciones de solicitudes por conceptos no adecuados.	**1.** Porcentaje (%) de solicitudes ciudadanas mensuales vencidas o fuera de términos legales. **2.** Porcentaje (%) de solicitudes reiteradas por el mismo tema o concepto.
Gestión Administrativa y Financiera	Errores en transacciones operativas y su impacto directo en la ejecución presupuestal de la vigencia.	Volumen total de transacciones erradas o corregidas al mes medidas sobre la capacidad operativa disponible.
Gestión del Talento Humano	Índice de rotación prematura de personal en la entidad municipal.	Porcentaje (%) de nuevos empleados o servidores que abandonan el puesto asignado dentro de los primeros seis (6) meses de vinculación.

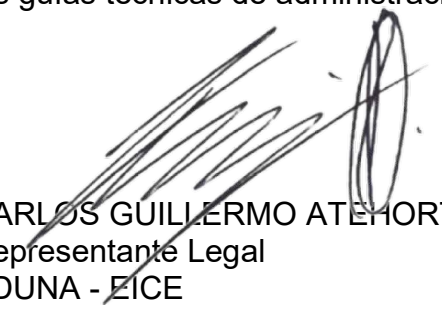
29. VIGENCIA Y DEROGATORIA.

RESOLUCIÓN GERENCIAL No. 143 DEL DIECISEIS (16) DE SEPTIEMBRE DE 2026.

"POR MEDIO DEL CUAL SE ACTUALIZA E IMPLEMENTA LA POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO PARA LA EMPRESA DE DESARROLLO URBANO DEL NORTE DE ANTIOQUIA EDUNA –EICE DE SANTA ROSA DE OSOS - ANTIOQUIA"

La presente Política para la Gestión Integral de Riesgos de la Empresa de Desarrollo Urbano del Norte de Antioquia EDUNA – EICE, rige a partir de la fecha de su expedición y publicación oficial en los canales institucionales de la entidad. Esta política deroga todas las disposiciones, decretos, resoluciones o lineamientos de carácter interno que le sean

contrarios, especialmente aquellas normas locales que adoptaron versiones anteriores de las guías técnicas de administración de riesgos.



CARLOS GUILLERMO ATEHORTÚA QUICENO
Representante Legal
EDUNA - EICE