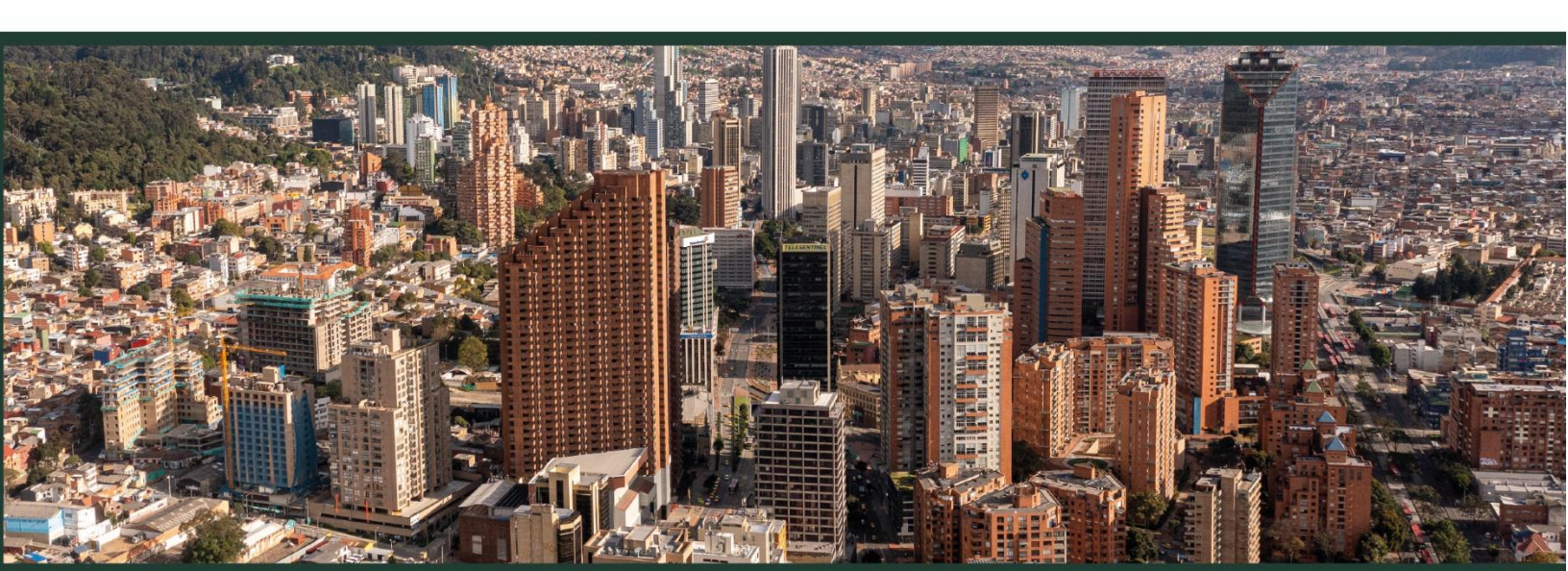




POLITICA DE ADMINISTRACIÓN DE RIESGOS

Unidad Administrativa Especial de Servicios Públicos UAESP

Oficina Asesora de Planeación

Noviembre de 2025



UAESP



Contenido

INTRODUCCIÓN.....	4
I. GENERALIDADES	6
1. MARCO NORMATIVO	6
2. TÉRMINOS Y DEFINICIONES	7
II. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO	22
1. OBJETIVOS	24
1.1. GENERAL.....	24
1.2. ESPECÍFICOS	24
2. ALCANCE	25
3. NIVELES DE MADUREZ PARA LA GESTIÓN DEL RIESGO	26
4. NIVELES DE ACEPTACIÓN	28
5. TRATAMIENTO DE RIESGOS.....	34
6. ROLES Y NIVELES DE RESPONSABILIDAD FRENTE AL RIESGO.....	35
6.1. LÍNEA ESTRATÉGICA.....	35
6.2. PRIMERA LÍNEA DE DEFENSA	37
6.3. SEGUNDA LÍNEA DE DEFENSA.....	38
6.4. TERCERA LÍNEA DE DEFENSA	40
7. METODOLOGÍA.....	42
III. DESARROLLO METODOLÓGICO.....	44
1. ANALISIS DEL CONTEXTO.....	44
2. IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO	49
2.1. IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO	49
IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN	50
2.2. IDENTIFICACIÓN DE ÁREAS DE IMPACTO	51
2.3. IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO.....	52
2.4. DESCRIPCIÓN DE RIESGOS	58

3.	ANÁLISIS DE RIESGO INHERENTE	62
3.1.	DETERMINAR LA PROBABILIDAD	63
3.2.	DETERMINAR EL IMPACTO	63
3.3.	ANÁLISIS DE SEVERIDAD.....	64
4.	DISEÑO Y ANÁLISIS DE CONTROLES	66
4.1.	ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL	66
4.2.	VALORACIÓN DE CONTROLES.....	68
5.	VALORACIÓN DE RIESGO RESIDUAL.....	70
5.1.	APLICACIÓN DE CONTROLES EN LA MATRIZ DE SEVERIDAD	70
5.2.	MAPA Y PLAN DE MANEJO DE RIESGOS Y OPORTUNIDADES CONSOLIDADO.....	73
6.	MONITOREO Y REVISIÓN	75
7.	RIESGOS MATERIALIZADOS	77
8.	DIVULGACIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS	80
9.	DIRECTRICES GENERALES DE LA DEBIDA DILIGENCIA	81
9.1.	REVISIÓN Y DETECCIÓN DE OPERACIONES SOSPECHOSAS DE LA/FT/FP	82
9.2.	POLÍTICAS DE MIPG RELACIONADAS DIRECTAMENTE CON LA PREVENCIÓN DE LA/FT/FP	83

INTRODUCCIÓN

En este documento se presenta la actualización de la política de administración del riesgo de la UAESP, teniendo en cuenta los nuevos lineamientos de la guía emitida por el Departamento Administrativo de la Función Pública (DAFP) Versión 7, en agosto de 2025¹, como el cumplimiento del requisito de la norma ISO 9001:2015, numeral 6.1, abordaje de riesgos y oportunidades.

En este documento encontrarán la política y la metodología de administración del riesgo, con la que la Unidad Administrativa Especial de Servicios Públicos - UAESP establece la manera cómo gestionarlos, teniendo en cuenta los diferentes lineamientos correspondientes a los riesgos de gestión, fiscales, seguridad de la información, desastres² y aquellos asociados al Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP, que incluye como amenazas el soborno, el fraude, la inadecuada gestión del conflicto de intereses, corrupción y Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP en la estructura de procesos de la UAESP.

Así mismo, se mantienen los lineamientos emitidos por la Secretaría General de la Alcaldía Mayor de Bogotá del Documento Técnico Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva en las entidades del Distrito Capital³, así como lineamientos de orden nacional respecto a la gestión del riesgo de desastres para las entidades públicas encargadas de la prestación de servicios públicos.

En la presente actualización se mantienen los lineamientos de gestión de los riesgos de desastre en el marco de la aplicación del Decreto 2157 de 2017 “Por medio del cual se

¹ <https://www.funcionpublica.gov.co/detalle-publicacion?entryId=963161>

² Decreto 2157 de 2017, artículo 2.3.1.5.2.1.1.

³ [Documento Técnico LA-FT Diciembre 2022.pdf](#)

adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de las entidades públicas y privadas en el marco del artículo 42 de la Ley 1523 de 2012.”

Es de resaltar que, todos los procesos deben la identificar y describir el riesgo, analizar el riesgo inherente, diseñar y hacer análisis de controles y valorar el riesgo residual, así como dar tratamiento a los riesgos para garantizar el cumplimiento de la misión y los objetivos institucionales, mediante:

- La identificación de los riesgos.
- Definición de los controles sobre los riesgos identificados.
- Formulación de acciones para tratar el riesgo residual.
- Formulación de plan de contingencia para actuar de manera oportuna, respecto a la materialización de los riesgos identificados.

Las anteriores acciones se estandarizan en un solo formato, el mapa y plan de manejo de riesgos y oportunidades, para dar eficiencia a su adecuada y efectiva gestión al riesgo, mitigando el impacto de ocurrencia y definiendo planes de contingencia ante la materialización del riesgo.

Esta política responde igualmente al Modelo Integrado de Planeación y Gestión (MIPG) establecido por el Decreto 1499 de 2017, y a la versión vigente del Manual Operativo del MIPG (Versión 6, diciembre de 2024), buscando reglamentar el alcance del Sistema de Gestión y su articulación con el Sistema de Control Interno, de tal manera que permita el aseguramiento de los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades del Estado.

I. GENERALIDADES

1. MARCO NORMATIVO

- **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 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 1186 de 2008:** Por medio de la cual se aprueba el “Memorando de entendimiento entre los Gobiernos de los Estados del Grupo de Acción Financiera de Sudamérica contra el lavado de activos (Gafisud)”
- **Ley 1474 de 2011:** Estatuto Anticorrupción Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” Reglamentado por el Decreto 1122 de 2024 “Por el cual se reglamenta el artículo 73 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”.
- **Ley 2195 de 2022:** Por la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción.
- **Decreto Nacional 1499 de 2017:** Se adopta el Modelo Integrado de Planeación y Gestión MIPG, como el nuevo marco de referencia para el diseño e implementación del SIGD, con el fin de fortalecer los mecanismos, métodos y procedimientos de gestión y control
- **Decreto Nacional 2157 de 2017:** Por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de las entidades públicas y privadas en el marco del artículo 42 de la Ley 1523 de 2012.

- **Decreto 1083 de 2015:** Decreto Único Reglamentario del Sector Función Pública, en lo relativo a la organización y funcionamiento del Sistema de Control Interno.
- **Decreto Distrital 221 de 2023:** Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital, se deroga el Decreto Distrital 807 de 2019 y se dictan otras disposiciones
- **Guía para la Gestión Integral del Riesgo en Entidades Públicas:** Establecida por el Departamento Administrativo de la Función Pública – DAFP, V7 (agosto de 2025).
- **ISO 31000:2018:** Norma Técnica Internacional Administración del Riesgo- Principios y orientaciones
- **ISO 9001:2015:** Norma Técnica Colombiana, elaborada por la Organización Internacional para la Estandarización (International Standardization Organization o ISO por sus siglas en inglés), determina los requisitos para un Sistema de Gestión de la Calidad.
- **CONPES 3793 de 2013:** Mediante el cual se definió y adoptó la “Política Nacional Antilavado de Activos y contra la Financiación del Terrorismo”.
- **CONPES 4042 de 2021:** Denominado Política Nacional Antilavado de Activos, contra la Financiación del Terrorismo y contra la financiación de la Proliferación de Armas de Destrucción Masiva.

2. TÉRMINOS Y DEFINICIONES⁴

⁴ Tomado y actualizado conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, DAFP – 2025, incorporando lineamientos y definiciones de versiones anteriores (V4, V5, V6) en lo que aún resultan aplicables y Modelo de Seguridad y Privacidad de la Información - MSPI

Administración de riesgos: La cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.

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

Alerta: Estado que se declara con anterioridad a la manifestación de un evento peligroso, con base en el monitoreo del comportamiento del respectivo fenómeno, con el fin de que las entidades y la población involucrada activen procedimientos de acción previamente establecidos, según Ley 1523 de 2012.

Amenaza: Peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales, según Ley 1523 de 2012.

Análisis y evaluación del riesgo: Implica la consideración de las causas y fuentes del riesgo, sus consecuencias y la probabilidad de que dichas consecuencias puedan ocurrir. Es el modelo mediante el cual se relaciona la amenaza y la vulnerabilidad de los elementos expuestos, con el fin de determinar los posibles efectos sociales, económicos y ambientales y sus probabilidades. Se estima el valor de los daños y las pérdidas potenciales, y se compara con criterios de seguridad establecidos, con el propósito de definir tipos de intervención y alcance de la reducción del riesgo y preparación para la respuesta y recuperación, según Ley 1523 de 2012.

Apetito de riesgo: Es el nivel de riesgo que la entidad está dispuesta a asumir, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe gestionar.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares. Estos se clasifican en bienes de uso público y bienes fiscales, definidos así: a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc. b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Calamidad pública: Es el resultado que se desencadena de la manifestación de uno o varios eventos naturales o antropogénicos no intencionales que al encontrar condiciones propicias de vulnerabilidad en las personas, los bienes, la infraestructura, los medios de subsistencia, la prestación de servicios o los recursos ambientales, causa daños o pérdidas humanas, materiales, económicas o ambientales, generando una alteración intensa, grave y extendida en las condiciones normales de funcionamiento de la población, en el respectivo territorio, que exige al municipio, distrito o departamento ejecutar acciones de respuesta a la emergencia, rehabilitación y reconstrucción, según Ley 1523 de 2012.

Capacidad del riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad (relacionado con la solvencia y liquidez).

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (pero se asocia a la misma causa inmediata).

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

Compartir o transferir el riesgo: Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

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

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)

Conocimiento del riesgo: Es el proceso de la gestión del riesgo compuesto por la identificación de escenarios de riesgo, el análisis y evaluación del riesgo, el monitoreo

y seguimiento del riesgo y sus componentes y la comunicación para promover una mayor conciencia del mismo que alimenta los procesos de reducción del riesgo y de manejo de desastre, según Ley 1523 de 2012.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

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

Contagio: Posibilidad de que la entidad pueda sufrir una afectación económica, reputacional o legal a causa de la acción propia de una entidad o de un individuo relacionado. El contagio se expresa cuando a partes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar a la entidad.

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

Control: Medida que permite reducir o mitigar un riesgo.

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

COSO – EMR: Modelo de gestión de riesgos empresariales (ERM) creado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO), centrado en el diseño e implementación de un marco de gestión de riesgos.

Debida diligencia: 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.

Desastre: Es el resultado que se desencadena de la manifestación de uno o varios eventos naturales o antropogénicos no intencionales que al encontrar condiciones propicias de vulnerabilidad en las personas, los bienes, la infraestructura, los medios de subsistencia, la prestación de servicios o los recursos ambientales, causa daños o pérdidas humanas, materiales, económicas o ambientales, generando una alteración intensa, grave y extendida en las condiciones normales de funcionamiento de la sociedad, que exige del Estado y del sistema nacional ejecutar acciones de respuesta a la emergencia, rehabilitación y reconstrucción, según Ley 1523 de 2012.

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

Emergencia: Situación caracterizada por la alteración o interrupción intensa y grave de las condiciones normales de funcionamiento u operación de una comunidad, causada por un evento adverso o por la inminencia del mismo, que obliga a una reacción inmediata y que requiere la respuesta de las instituciones del Estado, los medios de comunicación y de la comunidad en general, según Ley 1523 de 2012.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

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.

Financiación del Terrorismo (FT): El artículo 345 de la Ley 599 de 2000 (Modificado por el art. 16 de la Ley 1453 de 2011), define el delito de financiamiento del terrorismo y de grupos de delincuencia organizada y administración de recursos relacionados con actividades terroristas y de la delincuencia organizada 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.

- a) **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.
- b) **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.
- c) **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.

Fraude: Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025)

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

Gestión del riesgo: Es el proceso social de planeación, ejecución, seguimiento y evaluación de políticas y acciones permanentes para el conocimiento del riesgo y promoción de una mayor conciencia del mismo, impedir o evitar que se genere, reducirlo o controlarlo cuando ya existe y para prepararse y manejar las situaciones de desastre, así como para la posterior recuperación, entiéndase: rehabilitación y reconstrucción. Estas acciones tienen el propósito explícito de contribuir a la seguridad, el bienestar y calidad de vida de las personas y al desarrollo sostenible, según Ley 1523 de 2012.

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 o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines

esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)” . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

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 (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

Gobernanza del riesgo: Hace referencia a los arreglos institucionales y de control que aseguran que los riesgos sean conocidos, comunicados, gestionados y monitoreados en toda la entidad. La OCDE plantea que una adecuada gobernanza del riesgo requiere: Liderazgo claro y responsabilidad de la alta dirección. Marcos normativos y estructuras institucionales apropiadas. Evaluación y priorización de riesgos basada en evidencia. Coordinación interinstitucional y comunicación transparente.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptibles de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de

economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

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

- a) 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.
- b) 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.

- c) 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.
- d) 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.

Manejo de desastres: Es el proceso de la gestión del riesgo compuesto por la preparación para la respuesta a emergencias, la preparación para la recuperación posdesastre, la ejecución de dicha respuesta y la ejecución de la respectiva recuperación, entendiéndose: rehabilitación y recuperación, según Ley 1523 de 2012.

Modelo de control fiscal multinivel: Corresponde a la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

- El Control Fiscal Interno (CFI) se entiende como el primer nivel para la vigilancia fiscal de los recursos públicos, la prevención de riesgos fiscales y la defensa del patrimonio público. El Control Fiscal Interno hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de aseguramiento, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo puede ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Oficial de cumplimiento o equipo encargado: Es la persona natural o grupo designado por la entidad vigilada, encargada de promover, desarrollar y velar por el cumplimiento de los procedimientos específicos de prevención, actualización y mitigación del riesgo LA/FT/FP (Superintendencia de Sociedades de Colombia, 2021).

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

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.

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.

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 C340-07).

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

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

Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

Reducir el riesgo: Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de LA/FT/FP: Es la posibilidad de pérdida o daño económico o reputacional que puede sufrir una persona natural o jurídica, al ser utilizada para el lavado de activos,

financiación del terrorismo o de la proliferación de armas de destrucción masiva (DIAN, s.f.)

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

Riesgo fiscal: Es el efecto dañoso sobre los recursos públicos o los bienes 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).

- Efecto dañoso: es el daño que se generaría sobre los recursos, los bienes o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.
- Evento Potencial: hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos, los bienes o los intereses patrimoniales de naturaleza pública.
- Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso (Potencial Daño)

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 Legal: Es la posibilidad de pérdida en que incurre una entidad por sanciones o indemnizaciones de daños como resultado del incumplimiento normativo o de obligaciones contractuales. Se presenta de igual forma cuando existen fallas en los contratos y transacciones por actuaciones, negligencia o actos involuntarios.

Riesgo Operativo: Es la posibilidad de incurrir en pérdidas por fallas, deficiencias o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de eventos externos.

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

Riesgo Reputacional: Es la posibilidad de pérdida, disminución de ingresos o incremento en procesos judiciales en que incurre una entidad por desprestigio, mala imagen, publicidad negativa respecto de la institución y sus prácticas de negocios.

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

SARLAFT: Sistema de Administración de Riesgos de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.

Seguridad de la información: Conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

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

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.

Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

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

II. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Unidad Administrativa Especial de Servicios Públicos - UAESP, se compromete a identificar, gestionar y evaluar los riesgos de Gestión, Fiscales, Seguridad de la información, Desastres y aquellos asociados al Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP que incluye como amenazas el soborno, el fraude, la inadecuada gestión del conflicto de intereses, corrupción y Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP, cuando aplique; en todos los procesos de la entidad que puedan afectar los objetivos institucionales, a través del establecimiento del contexto interno y externo e implementación de controles y acciones para su prevención y mitigación y planes de contingencia ante su materialización, asegurando el incremento de su capacidad para alcanzar los objetivos, el fomento de la continuidad del servicio y la operación normal de la organización, y el fortalecimiento de la cultura de riesgos y control de la organización, con el fin de prevenir, reducir o eliminar los efectos indeseados, utilizando para tal fin la metodología del Departamento Administrativo de la Función Pública - DAFP.

De esta forma la Alta Dirección se compromete a:

- a. Integrar la gestión de los riesgos a sus procesos para mejorar la toma de decisiones.

- b. Proporcionar los recursos necesarios para la administración del riesgo.
- c. Fortalecer el enfoque basado en riesgos para la integración de sus Sistemas de Gestión.
- d. Definición de responsabilidad diferenciada basada en el modelo de las líneas de defensa.
- e. Articulación en la administración de los riesgos, para que estos sean gestionados de manera unificada durante el proceso de identificación, valoración, tratamiento y seguimiento de los riesgos.
- f. Determinar las medidas de intervención (planes de contingencia) derivados de su operación, resultado de la materialización del riesgo.
- g. Mejora continua a partir del monitoreo y seguimiento periódico de los riesgos asegurando la eficacia de los controles, que conlleven a la mitigación de la materialización de los riesgos.
- h. Revisar, por lo menos una vez al año, la política de administración del riesgo de acuerdo con los cambios en su contexto interno y externo y actualizar cuando se considere pertinente.
- i. Actualizar el procedimiento para la administración de riesgos en la Unidad, cada vez que cambien los lineamientos establecidos o por cambios que puedan afectar el SIG.
- j. Comunicar internamente los resultados de la evaluación de la gestión del riesgo.

La presente Política de Administración del Riesgo de la UAESP fue aprobada por el Comité Institucional de Coordinación de Control Interno – CICCÍ, según Acta No. 2 de fecha 27 de noviembre de 2025, y rige a partir de dicha aprobación, sin perjuicio de las actualizaciones que se determinen conforme a los cambios del contexto interno y externo ya los lineamientos del MIPG y del DAFP.

Esta política desarrolla y operacionaliza la Política de Gestión Integral de Riesgos del Modelo Integrado de Planeación y Gestión – MIPG, articulando los riesgos de gestión, fiscales, de desastres, de seguridad de la información y de integridad pública (SIGRIP) en un esquema único de administración del riesgo para la UAESP.

1. OBJETIVOS

1.1. GENERAL

Definir los parámetros de la administración del riesgo de la Unidad a través del establecimiento de mecanismos y herramientas que permitan la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos, con el fin de evitar su materialización y controlar los eventos que afecten los objetivos estratégicos de la entidad gestionándolos en un nivel aceptable, en concordancia con el Modelo Integrado de Planeación y Gestión – MIPG y las mejores prácticas internacionales de gestión de riesgos basadas en el marco COSO - EMR.

La política de administración de riesgos tiene como propósito facilitar la toma de decisiones de la alta dirección, propendiendo por la integridad, transparencia y eficiencia en el manejo de los recursos, manteniendo su gobernanza y dando a los procesos las herramientas necesarias para anticiparse a las situaciones que puedan representar un riesgo al cumplimiento de sus objetivos y misión, garantizando la mejora continua y el incremento en la confianza de las partes interesadas en la gestión de la UAESP.

1.2. ESPECÍFICOS

- Identificar los factores internos y externos que puedan generar riesgos para el cumplimiento de los objetivos estratégicos con el fin de orientar la toma de decisiones.
- Establecer los mecanismos y herramientas para la identificación, análisis, evaluación de los riesgos y su consolidación.
- Identificar y documentar los riesgos de gestión, fiscales, seguridad de la información, desastres y aquellos asociados al Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP que incluye como amenazas el soborno, el fraude, la inadecuada gestión del conflicto de intereses, corrupción y Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP, para gestionar su

administración, tratamiento, seguimiento y evaluación con el fin de facilitar una gestión pública eficaz y eficiente con el compromiso de todas las líneas de defensa.

- Establecer los roles y responsabilidades de cada una de las líneas de defensa en la administración de los riesgos de la entidad.
- Fortalecer la cultura de los colaboradores de la Entidad alrededor de la gestión de los riesgos, con el fin de prevenir y detectar desviaciones para efectuar los correctivos necesarios para el cumplimiento de los resultados propuestos.
- Implementar el plan de manejo de riesgos para mitigar la materialización de estos.
- Dar respuesta oportuna a amenazas internas o externas que puedan generar eventos de riesgo.
- Definir las acciones para prevenir la ocurrencia de riesgos y mitigar los efectos ocasionados en el evento de su materialización.

2. ALCANCE

La Política de administración de riesgos es aplicable a todos los procesos de la Unidad y en todos sus niveles y sedes.

La totalidad de los riesgos se tratarán por los lineamientos generales señalados en este documento.

El tratamiento de los riesgos de seguridad de la información se complementará con los lineamientos específicos para Modelo de Seguridad y Privacidad de la Información - MSPI.

El tratamiento de los riesgos de SARLAFT se complementará de manera específica con los lineamientos de los documentos Técnicos de la Secretaría General de la Alcaldía Mayor de Bogotá- y la Ruta Metodológica para la Implementación del SARLAFT en Entidades Distritales, así mismo se tendrán en cuenta los lineamientos de tratamiento establecidos en SIGRIP.

3. NIVELES DE MADUREZ PARA LA GESTIÓN DEL RIESGO

Para establecer el nivel de madurez de la gestión del riesgo de la UAESP se usa la estructura que consta de cinco componentes interrelacionados de la gestión del riesgo empresarial y su relación con la misión, visión y valores clave de la entidad así:

Gobierno y Cultura: El gobierno y cultura juntos forman una base para todos los demás componentes de la gestión del riesgo. El gobierno marca el tono de la entidad, reforzando la importancia de la gestión del riesgo y estableciendo responsabilidades de supervisión al respecto. La cultura se refleja en la toma de decisiones.

Establecimiento de la estrategia y objetivos: La gestión del riesgo se integra en el plan estratégico de la entidad en concordancia con los objetivos de la Unidad. Con un conocimiento profundo del contexto interno y externo y sus efectos en el riesgo.

Desempeño: La UAESP identifica y evalúa los riesgos que pueden afectar su capacidad para cumplir el plan estratégico y sus objetivos, seleccionando las respuestas al riesgo y efectuando el seguimiento del desempeño considerando posibles cambios.

Revisión y monitorización: Al examinar las capacidades y técnicas de gestión del riesgo, y el desempeño de la entidad en relación con sus objetivos.

Información, Comunicación y Reporte: La comunicación es el proceso continuo e iterativo de obtener y compartir información en toda la entidad. La UAESP utiliza información pertinente de fuentes internas y externas para facilitar la gestión del riesgo, aprovechando los sistemas de información para capturar, procesar y gestionar datos e información. Al utilizar información que se aplica a todos los componentes, la UAESP informa sobre el riesgo, la cultura y el desempeño. (Basado en: IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.11, 12).

En este entendido, la UAESP aplica el instrumento vigente de autodiagnóstico de nivel de madurez vigente del Departamento Administrativo de Función Pública integrado a los autodiagnósticos de la Política de Planeación Institucional del MIPG, respondiendo

las preguntas asociadas a cada componente y principio de acuerdo con la siguiente tabla:

TABLA 1 COMPONENTES Y PRINCIPIOS EVALUABLES MODELO DE MADUREZ

COMPONENTE	PRINCIPIOS
Gobierno y Cultura	• Supervisión de riesgos a través del consejo de administración • Establece estructuras operativas • Define la cultura deseada • Demuestra compromiso con valores clave • Atrae, desarrolla y retiene a profesionales capacitados
Establecimiento de la estrategia y objetivos	• Analiza el contexto (externo e interno) • Define el apetito del riesgo • Evalúa estrategias alternativas • Formula objetivos estratégicos y operacionales
Desempeño	• Identifica y describe el riesgo • Evalúa el riesgo inherente • Diseña controles efectivos • Prioriza riesgos • Desarrolla visión integral
Análisis y monitorización	• Evalúa los cambios significativos • Revisa el riesgo y el desempeño • Persigue la mejora de la gestión del riesgo
Información, Comunicación y Reporte	• Aprovecha la información y la tecnología • Comunica información sobre riesgos • Informa sobre el riesgo, la cultura y el desempeño

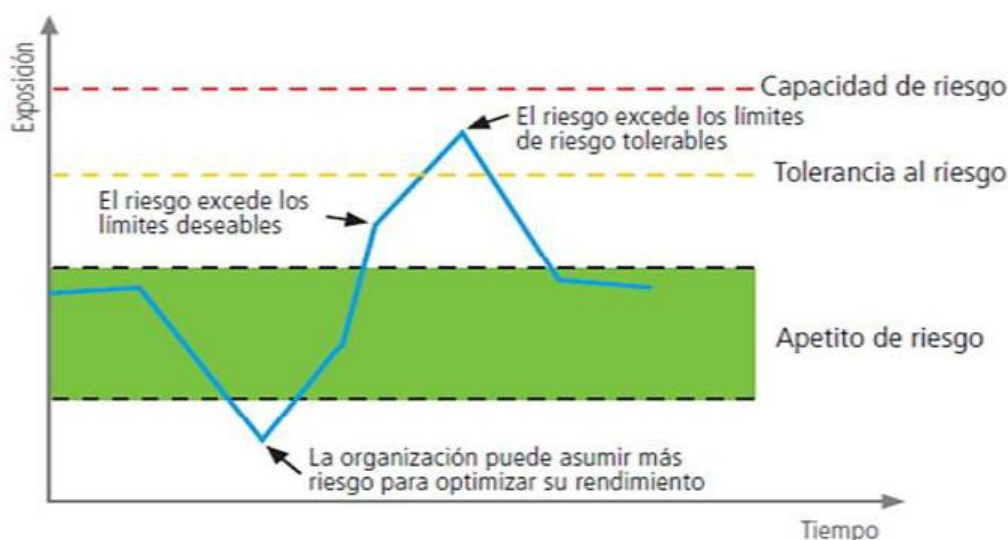
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7, DAFP – agosto de 2025

La UAESP realizará el autodiagnóstico de nivel de madurez en gestión de riesgos por lo menos una vez al año, utilizando el instrumento vigente del DAFP, e incorporará sus resultados en los informes del MIPG y en la planeación institucional.

4. NIVELES DE ACEPTACIÓN

Acogiendo los lineamientos del DAFP en la Guía de administración del riesgo V.7, se establecen las siguientes categorías conceptuales para determinar los niveles de Aceptación del riesgo en la UAESP.

ILUSTRACIÓN 1 DEFINICIONES DE APETITO, TOLERANCIA Y CAPACIDAD DE RIESGO



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7, DAFP – agosto de 2025

NIVEL DE RIESGO: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

APETITO DE RIESGO: Es el nivel de riesgo que la Unidad puede aceptar, en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe

gestionar. La UAESP declara que, del límite de apetito de riesgo, se encuentran aquellos que, después de aplicarse controles, se ubican en la zona de severidad de riesgo BAJA (verde en el mapa de calor). Se debe tener en cuenta que los riesgos asociados al Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP que incluye como amenazas el soborno, el fraude, la inadecuada gestión del conflicto de intereses, corrupción y Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP son inaceptables.

En coherencia con la Política de Integridad, el Programa de Transparencia y Ética Pública (artículo 73 de la Ley 1474 de 2011, reglamentado por el Decreto 1122 de 2024) y los lineamientos del SIGRIP, la UAESP declara que los riesgos asociados al soborno, al fraude, a la inadecuada gestión del conflicto de intereses, a la corrupción y al LA/FT/FP son riesgos inaceptables, por lo cual su apetito de riesgo es cero.

TOLERANCIA AL RIESGO: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. La UAESP declara que el límite de tolerancia de riesgo, se encuentran en aquellos que, después de aplicarse controles, se ubican en la zona de severidad de riesgo MEDIA (amarillo en el mapa de calor) y ALTA (naranja en el mapa de calor).

CAPACIDAD DE RIESGO: Es el máximo valor del nivel de riesgo que una entidad puede soportar, y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad. La UAESP declara que el límite de capacidad de riesgo, se encuentran en aquellos que, después de aplicarse controles, se ubican en la zona de severidad de riesgo EXTREMO (rojo en el mapa de calor).

Una relación sencilla entre los anteriores conceptos es la siguiente: “El apetito es el nivel de riesgo que la empresa quiere aceptar y su tolerancia es la desviación respecto

a este nivel. La capacidad es el máximo de riesgo que una organización puede soportar en la persecución de sus objetivos.”⁵

TABLA 2 NIVELES DE ACEPTACIÓN DEL RIESGO

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVELES DE ACEPTACIÓN	ACCIÓN A TOMAR
Riesgos de Gestión, Fiscales, Desastres y de Seguridad de la información	Baja	Apetito del Riesgo	Se ASUMIRÁ el riesgo y se administra por medio de los controles definidos en los procesos y procedimientos. El Proceso como primera línea de defensa hace el seguimiento mensual del riesgo, a través de ejercicios de autocontrol y autoevaluación documentados. Realiza el reporte trimestral de su desempeño a la Oficina de Planeación como segunda línea de defensa.
	Moderada	Tolerancia del riesgo	Se establecen acciones de control y acciones de plan de manejo que permitan REDUCIR la probabilidad de ocurrencia del riesgo. El Proceso como primera línea

⁵ <https://incp.org.co/diferencia-entre-apetito-de-riesgo-y-tolerancia-al-riesgo/>

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVELES DE ACEPTACIÓN	ACCIÓN A TOMAR
			de defensa hace el seguimiento mensual del riesgo, a través de ejercicios de autocontrol y autoevaluación documentados. Realiza el reporte trimestral de su desempeño a la Oficina de Planeación como segunda línea de defensa. Se define un plan de contingencia en caso de materialización para garantizar la continuidad de las operaciones.
	Alto	Tolerancia del riesgo	Se establecen mecanismos de control y acciones de plan de manejo para REDUCIR o EVITAR la probabilidad o el impacto de ocurrencia del riesgo. El proceso evalúa la posibilidad de sustituir las actividades que dan origen al riesgo. Se monitorea mensualmente a través de ejercicios de autocontrol y autoevaluación documentados. Se define un

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVELES DE ACEPTACIÓN	ACCIÓN A TOMAR
			plan de contingencia en caso de materialización para garantizar la continuidad de las operaciones. COMPARTIR o TRANSFERIR el riesgo, el cual involucra la contratación de una tercera parte, que permita mitigar el riesgo, junto con la evaluación correspondiente ya sea mensual o una vez terminada la gestión del riesgo.
	Extremo	Tolerancia del riesgo al límite de la capacidad del riesgo	Este es el nivel extremo, por lo cual se debe: REDUCIR el riesgo por medio de la aplicación de controles y acciones de plan de manejo, haciendo seguimiento mensual o una vez terminado el control, COMPARTIR o TRANSFERIR el riesgo, el cual involucra la contratación de una tercera parte, que permita mitigar el riesgo, junto con la evaluación

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVELES DE ACEPTACIÓN	ACCIÓN A TOMAR
			correspondiente ya sea mensual o una vez terminada la gestión del riesgo. Y, por último EVITAR el riesgo generando líneas alternativas, o eliminando las acciones que generen el riesgo y seguimiento mensual o una vez terminado el control, Cabe resaltar que los controles aplicables deben ser adelantados en el menor tiempo posible, en el entendido que hay una alta exposición de la Entidad a la pérdida de capacidad de servicio o de información. Se debe definir previamente un plan de contingencia para el evento en que ocurra la materialización de un riesgo de estas características, para garantizar la continuidad de las operaciones.

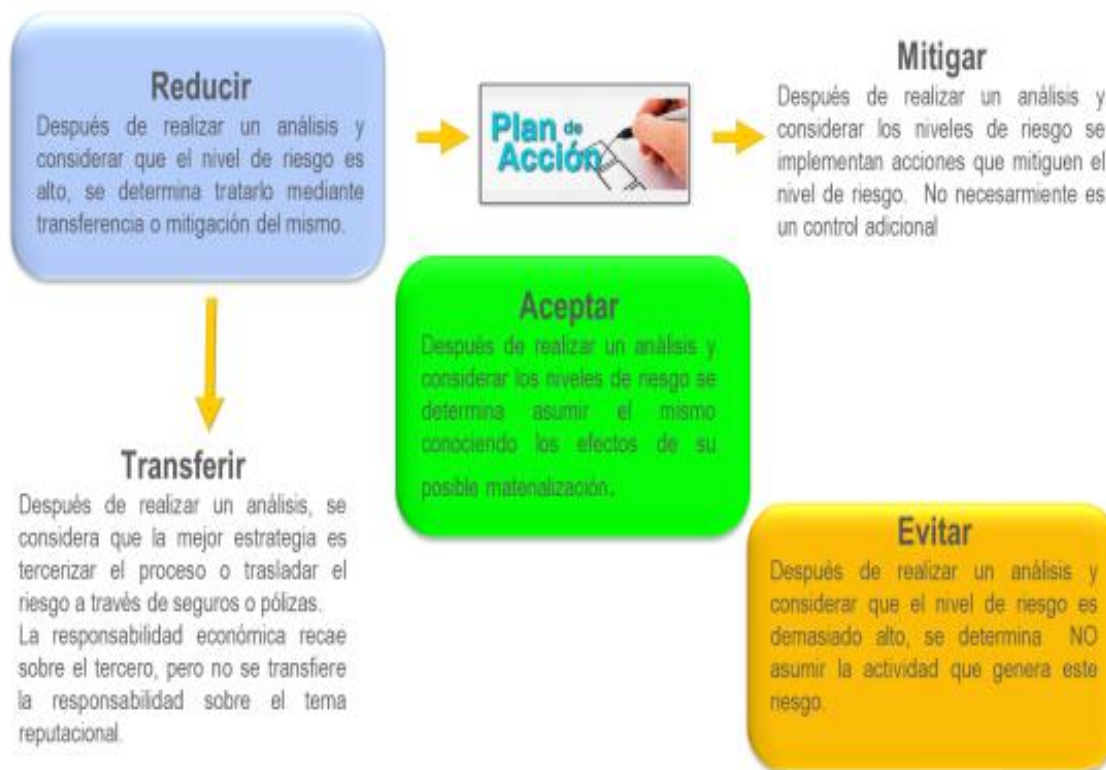
Fuente: UAESP

Para los riesgos asociados al Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP que incluye como amenazas el soborno, el fraude, la inadecuada gestión del conflicto de intereses, corrupción y Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP es inaceptable.

5. TRATAMIENTO DE RIESGOS

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar y se analiza frente al riesgo residual.

ILUSTRACIÓN 2 ESTRATEGIAS PARA COMBATIR EL RIESGO



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6, DAFP - noviembre de 2022

Es importante aclarar que el control hace referencia actividades rutinarias que se ejecutan en el desarrollo de la prestación de un servicio o la ejecución de una actividad, para evitar la materialización del riesgo (inherente), el plan de manejo hace referencia

Unidad Administrativa Especial de Servicios Públicos

Cra 10 No. 17-72 L-119

PBX: (+57) 601 358 0400

www.uaesp.gov.co

a actividades adicionales no rutinarias que ayudan a evitar la materialización del riesgo residual, y que requieren un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

6. ROLES Y NIVELES DE RESPONSABILIDAD FRENTE AL RIESGO

A continuación, se relacionan los niveles de responsabilidad⁶ y autoridad establecidos para la administración del riesgo determinados por líneas de defensa, teniendo en cuenta lo establecido en el Manual operativo MIPG V5 y la guía de administración del riesgo de la Función pública V7. Igualmente se pueden concretar en otros instrumentos con relación a aspectos clave para el éxito de gestión de la entidad, acudiendo a diversas herramientas, como por ejemplo los mapas de aseguramiento⁷.

Las líneas de defensa hacen referencia a un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control de la entidad, proporcionando el aseguramiento de la gestión para prevenir la materialización de los riesgos en todo su ámbito⁸.

6.1. LÍNEA ESTRATÉGICA

Los responsables de esta línea son la Alta dirección y el Comité Institucional de Coordinación de control Interno, las responsabilidades de esta línea son las siguientes:

- Definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno.
- Definir el marco general para la gestión del riesgo y el control, y supervisar su cumplimiento.

⁶ Los roles institucionales de la entidad para la atención de emergencias, calamidades y desastres serán considerados conforme al nivel de autoridad y de competencia en el nivel de la emergencia de acuerdo con lo establecido en la EDRE, EIR y en el PGRDEPP.

⁷ Circular 103 de 2020 de la Secretaría General de Bogotá.

⁸ Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4 – DAFP.

- Revisar el cumplimiento de los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando.
- Analizar los cambios en el entorno interno y externo que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles.
- Definir los procesos, programas o proyectos susceptibles de posibles actos de corrupción acorde con el análisis del entorno interno y externo.
- Analizar los riesgos y amenazas institucionales a la luz del cumplimiento de los planes estratégicos.
- Realizar el seguimiento a riesgos críticos aplicando el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de la 2ª línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.
- Definir y hacer seguimiento a los niveles de aceptabilidad del riesgo.
- Realizar seguimiento y análisis trimestral de los riesgos institucionales y en cuanto a los riesgos materializados, se revisarán las causas que les dieron origen, y los planes de acción establecidos para enfrentarlos, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
- Evaluar las debilidades en los controles y emitir instrucciones sobre las acciones apropiadas para la mejora.
- Hacer seguimiento periódico a los resultados de las evaluaciones realizadas por Control Interno.
- Analizar los riesgos asociados a las actividades tercerizadas u otras figuras externas que afecten la prestación de los servicios, con base en los informes de la segunda y tercera línea de defensa.
- Solicitar las intervenciones e informes necesarios a las diferentes dependencias con el fin de facilitar la toma de decisiones

- Evaluar el estado del sistema de control interno, acorde con la información generada por parte de las instancias de 2° línea identificadas de acuerdo con el tema del cual son responsables, a fin de generar acciones y una toma de decisiones con enfoque preventivo.

6.2. PRIMERA LÍNEA DE DEFENSA

Los responsables de esta línea son líderes de proceso y gerentes de proyectos, las responsabilidades de esta línea son las siguientes:

- Monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos incluyendo los indicadores de desempeño, a fin de establecer los posibles riesgos que se están materializando y propiciar una adecuada gestión de riesgos.
- Identificar, analizar, valorar y monitorear los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo, alineados con las metas y objetivos de la entidad, incluyendo los riesgos de corrupción, y actualizarlos cuando se requiera, así como la matriz de riesgos de su proceso
- Identificar los riesgos de servicios o actividades tercerizados, cuando aplique.
- Revisar como parte de los procedimientos de supervisión, el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos
- Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados, alineados con las metas y objetivos de la entidad, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo).
- Definir, aplicar y hacer seguimiento a las acciones para mitigar los riesgos residuales identificados y planes de contingencia y de continuidad de las operaciones, frente a los riesgos materializados, para reducir el impacto y permitir el cumplimiento de los objetivos institucionales.

- Realizar la formulación del mapa y plan de manejo de riesgos y oportunidades, y revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas.
- Desarrollar ejercicios mensuales de autocontrol para establecer la eficacia de los controles y de las acciones formuladas e implementar mejoras si se requieren y reportar en la herramienta disponible.
- Proponer mejoras a la gestión del riesgo de su proceso.
- Reportar trimestralmente el estado de la gestión de los riesgos de los procesos de los cuales es responsable, así como informar los riesgos materializados a la Oficina Asesora de Planeación, incluyendo las causas que dieron origen a esos eventos.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
- Revisar y hacer análisis y atención de los informes de evaluación y auditoría para la actualización de los riesgos del proceso.

6.3. SEGUNDA LÍNEA DE DEFENSA

Las responsabilidades de la Oficina Asesora de Planeación en la gestión de los riesgos, respecto a la segunda línea de defensa son las siguientes:

- Establecer directrices y lineamientos que faciliten la identificación, análisis, evaluación y tratamiento de los riesgos.
- Proponer al Comité Institucional de Coordinación de Control Interno para la consulta y observaciones las propuestas de actualización y mejora de políticas, instrumentos o lineamientos relacionados con la gestión del riesgo.
- Revisar y registrar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar la actualización de las matrices de riesgos y oportunidades a los procesos.

- Revisar la adecuada definición de los objetivos estratégicos y su concreción con los objetivos de los procesos, cuyo análisis han servido de base para llevar a cabo la identificación de los riesgos y oportunidades, y realizar las recomendaciones a que haya lugar.
- Orientar a los responsables de los procesos en el análisis del contexto interno y externo, la identificación y descripción del riesgo, análisis del riesgo inherente, diseño y análisis de controles y valoración del riesgo residual, para todos los riesgos aplicables a la entidad, así como en la aplicación de técnicas y metodologías de análisis e identificación en coordinación con la tercera línea de defensa.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos.
- Hacer seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos verificando que se encuentren documentadas y actualizadas en los procedimientos.
- Promover ejercicios de autoevaluación para establecer la eficacia de los controles.
- Revisar el valor de los riesgos inherentes y residuales por cada proceso y pronunciarse sobre cualquier riesgo que, a pesar de la aplicación de controles, permanezca en un nivel alto o extremo y comprometa el cumplimiento de los objetivos de la entidad.
- Consolidar el mapa y plan de manejo de riesgos y oportunidades y presentarlo para evaluación ante el Comité Institucional de Gestión y Desempeño o el Comité Institucional de Coordinación de Control Interno CICCI, para su análisis y toma de decisiones y su posterior socialización y publicación en la página web.
- Hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes al mapa y plan de manejo de riesgos y oportunidades, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo

que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los líderes de los procesos y sus equipos para la mejora de este tema.

- Monitorear trimestralmente los riesgos, oportunidades identificadas y los controles establecidos por la primera línea de defensa y registrar el resultado en el informe para la alta dirección y demás instancias interesadas.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento de los objetivos.
- Verificar el análisis de los informes de evaluación y auditoria para la actualización de los riesgos y oportunidades del proceso realizado por la primera línea de defensa.
- Consolidar y analizar información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar la materialización de los riesgos.

Así mismo, tienen funciones de segunda línea de defensa los líderes del proceso de Gestión de Asuntos Legales, Gestión Financiera, Gestión de Talento Humano, Gestión Tecnológica y de la Información, Servicio al Ciudadano, Gestión de las Comunicaciones, Gestión del Conocimiento y Gestión Documental y los supervisores de contrato de la Entidad, con las siguientes responsabilidades:

- Acompañar, orientar y entrenar a los líderes de procesos (primera línea de defensa) en la identificación, análisis, y valoración del riesgo, oportunidades y definición de controles, relacionados con los temas a su cargo.
- Monitorear los riesgos y oportunidades identificadas y los controles establecidos por la primera línea de defensa relacionados con los temas a su cargo.

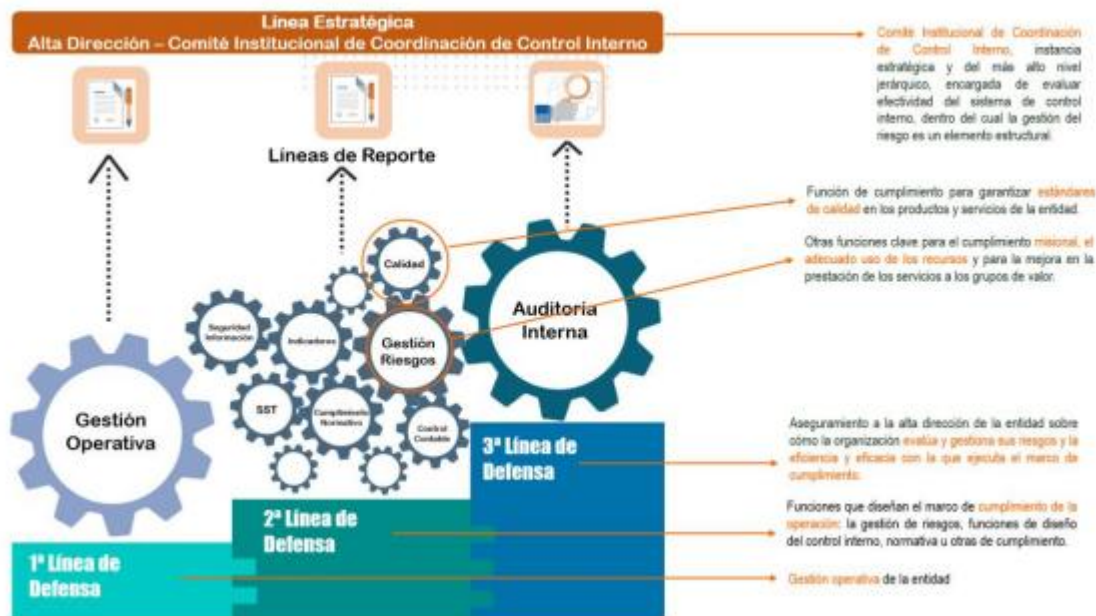
6.4. TERCERA LÍNEA DE DEFENSA

El responsable de esta línea de defensa es la Oficina de Control Interno, las responsabilidades de esta línea son las siguientes:

- Asesorar a la UAESP acerca de las metodologías, herramientas y técnicas para la identificación y administración de los riesgos, oportunidades y controles en coordinación con la segunda línea de defensa.
- Identificar y evaluar cambios que podrían tener impacto significativo en el sistema de control interno durante las evaluaciones periódicas de riesgos y oportunidades en los trabajos de auditoría interna.
- Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y cómo estos puedan generar nuevos riesgos y oportunidades o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se evalúen y actualicen la política de administración del riesgo, la identificación de los riesgos, oportunidades y sus controles y las matrices de riesgos por parte de los responsables.
- Revisar de manera independiente la adecuada definición de los objetivos estratégicos y su concreción con los objetivos de los procesos, cuyo análisis ha servido de base para llevar a cabo la identificación de los riesgos y oportunidades, y realizar las recomendaciones a que haya lugar.
- Llevar a cabo la evaluación independiente de la gestión de los riesgos y oportunidades de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional de Coordinación de Control Interno CICCÍ y publicarlos en el sitio web.
- Revisar cuatrimestralmente el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos y registrar el resultado del seguimiento a la gestión de los riesgos en el mapa y plan de manejo de riesgos.
- Revisar el valor de los riesgos inherentes y residuales por cada proceso y pronunciarse sobre cualquier riesgo que, pese a la aplicación de controles, permanezca en un nivel alto o extremo y comprometa el cumplimiento de los objetivos de la entidad.
- Promover ejercicios de autocontrol para que cada proceso monitoree los niveles de eficacia de los controles.

- Informar sobre las auditorías basadas en riesgos que se ejecuten, con énfasis en riesgos fiscales.

ILUSTRACIÓN 3 OPERATIVIDAD ESQUEMA DE LÍNEAS DE DEFENSA



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6, DAFP - noviembre de 2022

7. METODOLOGÍA

La metodología corresponde a la establecida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 7 de agosto de 2025 del DAFP, concretada en las etapas señaladas en el presente documento.

Las etapas de esta metodología se llevarán de manera secuencial en el formato DES-FM-12 Mapa y plan de manejo de riesgos y oportunidades de la UAESP, el cual acoge el modelo propuesto por el DAFP aplicando el procedimiento: DES-PC-07 Administración riesgos y oportunidades. En términos generales la administración del riesgo que se realizará es:

- **Análisis del contexto:** Es necesario desplegar un análisis interno y externo específico para la entidad, donde se expliquen mediante información institucional formalizada y datos específicos relacionados, teniendo en cuenta los siguientes elementos:
 - Contexto Interno: estructura organizacional, cultura institucional, capacidad tecnológica, talento humano, procesos internos, recursos financieros, políticas internas y marco normativo aplicable.
 - Contexto Externo: entorno político, económico, social, ambiental y tecnológico; Grupos de valor o partes interesadas: actores del sector, reguladores, organismos de control, ciudadanos y partes interesadas, así como riesgos asociados a cambios normativos y eventos externos. Sector donde opera la entidad y su relacionamiento con otras entidades e instancias necesarias para su gestión, así como entorno de desarrollo territorial.
- **Identificación y descripción del riesgo:** Elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo, se compone de definición de causas y consecuencias y clasificación del riesgo.
 - Identificación de los puntos de riesgo
 - Identificación de áreas de impacto
 - Identificación de áreas de factores de riesgo
 - Descripción del riesgo

Para los riesgos fiscales se tendrá en cuenta la siguiente estructura

- Identificación puntos de riesgo y circunstancias inmediatas
- Identificación del área de impacto
- Identificación del efecto económico
- Identificación de la causa raíz
- Descripción del Riesgo Fiscal

Para los riesgos de seguridad de la información, en la identificación de los puntos de riesgo se deberá realizar:

- Identificación de activos de información
- Análisis de riesgo inherente: Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar los niveles de severidad (Riesgo inherente).
 - Determinar la probabilidad
 - Determinar el impacto
 - Análisis de severidad
- Diseño y análisis de controles: Las actividades de control son acciones concretas, rutinarias y documentadas en políticas, procedimientos u otras directrices o documentos institucionales e implementadas con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos.
 - Estructura para la descripción del control
 - Valoración de controles
- Valoración del riesgo residual: Es el resultado de aplicar la efectividad de los controles al riesgo inherente
 - Aplicación efectiva de los controles – desplazamiento en matriz de severidad
 - Mapa y plan de manejo de riesgos y oportunidades consolidado
- Monitoreo y seguimiento: Se realizará el monitoreo por parte de los procesos de manera mensual, el seguimiento trimestral por parte de la segunda línea de defensa y el seguimiento cuatrimestral por parte de la tercera línea de defensa. Los resultados serán llevados al CIGD y al CICCÍ según se ha establecido. Asimismo, los resultados del monitoreo y la revisión de la gestión de riesgos formarán parte de los informes de seguimiento al MIPG, de los informes del Sistema de Control Interno y de los informes de gestión que la UAESP presenta a los organismos de control y a sus grupos de valor.

III. DESARROLLO METODOLÓGICO

1. ANALISIS DEL CONTEXTO

Los riesgos y oportunidades identificadas deben tener impacto en el cumplimiento de objetivos estratégicos de la entidad, y su concreción en los objetivos de sus procesos. Los objetivos estratégicos deben estar alineados con la misión y la visión institucional, y deben desdoblarse en los objetivos de los procesos.

Los factores internos y externos se han adecuado a la complejidad y naturaleza de la entidad, determinando los factores relacionados que pueden afectar a los objetivos institucionales de la Unidad. Entre los aspectos que pueden contemplarse en este análisis, se encuentran los siguientes:

TABLA 3 FACTORES POR CATEGORÍA DEL CONTEXTO

Tipo	Factores
Externo	Políticos: Cambios de gobierno, legislación, políticas públicas, regulación.
	Económicos y financieros: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Sociales y culturales: Demografía, responsabilidad social, orden público.
	Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno digital.
	Ambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Cambio Climático: Identificar como el cambio climático impacta la calidad en todos los aspectos de la prestación del servicio y como el servicio prestado impacta positiva o negativamente este fenómeno.
	Grupos de valor o partes interesadas: Se debe hacer especial énfasis en identificar aquellos que pueden considerarse contrapartes, es decir, partes con las que se tienen interacciones, entendidas estas como cualquier tipo de vinculación que involucre la prestación o entrega de un producto, o el intercambio de recursos. Actores del

Tipo	Factores
	sector, reguladores, organismos de control, ciudadanos y partes interesadas. Incluye los clientes internos y externos.
	Sector donde opera la entidad y su relacionamiento con otras entidades e instancias necesarias para su gestión, así como EL entorno de desarrollo territorial.
	Amenazas: a) Elementos expuestos entorno de la actividad y la relacionada con el área de afectación probable (personas, medios de subsistencia, servicios ambientales y recursos económicos y sociales, bienes culturales e infraestructura), acorde a la información disponible por las entidades pertinentes. b) Descripción del entorno del establecimiento/actividad en relación a sus condiciones biofísicas y de localización. c) Identificación de instalaciones que puedan originar amenazas o producir efecto dominó mediante análisis cualitativo de acuerdo con la información disponible por las entidades pertinentes. d) La información pertinente definida en los instrumentos de planificación del desarrollo y para la gestión existentes, tales como: Planes de Ordenación y Manejo de Cuencas Hidrográficas (Pomca), Planes de Ordenación y Manejo de Unidades Ambientales Costeras (Pomiuac), Planes de Ordenamiento Territorial (POT), Planes Municipales de Gestión del Riesgo (PMGRD), Estrategias Municipales de Respuesta (EMRE), Planes territoriales y sectoriales de cambio climático, Estrategia Distrital de Respuesta (EDRE), entre otros de acuerdo con los requerimientos de la entidad. e) Amenazas climáticas: avenidas torrenciales, inundaciones, movimientos en masa, incendios forestales y escenarios de riesgos identificados en Bogotá Sísmico, Inundación, Movimientos en Masa,

Tipo	Factores
	Avenidas Torrenciales, Incendios Forestales, de Origen Tecnológico, por Actividad de la Construcción y por Aglomeraciones de Público ⁹ .
	Legales y reglamentarios: Normatividad externa (leyes, decretos, ordenanzas y acuerdos)
Interno	Recursos financieros: Presupuesto de funcionamiento e inversión, infraestructura.
	Talento humano: Competencia del personal, disponibilidad del personal, seguridad y salud en el trabajo, trabajo en equipo y liderazgo.
	Procesos internos: Capacidad, diseño, ejecución, caracterización de cada proceso, que contempla su objetivo y alcance, proveedores, entradas, salidas, gestión del conocimiento.
	Capacidad tecnológica: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción,
	Estructura organizacional: Funciones de la entidad, dependencias e interacciones.
	Cultura Organizacional: Tono de control o estilo de dirección que establece la alta dirección, frente a la gestión del riesgo y ética proactiva y orientada a la integridad para incorporar la gestión de riesgos en los procesos de planeación, ejecución y seguimiento institucional.
	Marco normativo aplicable: Regulaciones internas como Resoluciones, acuerdos entre otros.
	Políticas internas: Lineamientos internos como procedimientos, circulares, políticas entre otras
Proceso	Responsables del proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.

⁹ De acuerdo con lo establecido en la Estrategia Distrital para la Respuesta a Emergencias EDRE 2023.

Tipo	Factores
	Hallazgos fiscales: Hallazgos con incidencia fiscal en los últimos 5 años.
	Activos de seguridad de la información del proceso: Información, aplicaciones, hardware entre otros, que se debe proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.
	Gestión del riesgo de desastres: analizar como mínimo a) Responsabilidades, roles y estructura. b) Actividades de gestión del riesgo de desastres que se van a implementar. c) Precisar el proyecto o el proceso en función del tiempo y la localización. d) Las relaciones entre un proyecto o actividad particular y otros proyectos o actividades de la organización. e) Definir las metodologías de valoración del riesgo. f) Identificar los estudios necesarios para la elaboración del proyecto de intervención del riesgo. g) Desarrollo y ejecución de los procesos de gestión del riesgo: conocimiento del riesgo, reducción del riesgo y manejo de desastres. h) Identificación y análisis de los escenarios de riesgo, los servicios y funciones de respuesta de acuerdo con lo establecido en la EDRE.
	Descripción de producción o servicio: Resaltando la actividad que pueda generar riesgo de desastre para la sociedad, listado general y la descripción, cantidad de procesos, de sustancias químicas, de maquinaria que pueden ser fuente de desastres.
	Eventos de Lavado de activos y financiamiento del terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva: Cuando se habla de los eventos, estos se pueden identificar teniendo en cuenta la fuente de los riesgos y las áreas afectadas, pero además

Tipo	Factores
	la presencia de circunstancias, ocurrencias y sucesos asociados al riesgo de LA/FT/FP, que se pueden obtener aplicando herramientas como las entrevistas, los cuestionarios, la experiencia colectiva sobre el contexto y el desarrollo del negocio respecto de la interacción entre entradas, salidas y responsabilidades de los procesos de la entidad. Para identificar la exposición al riesgo del LA/FT/FP que puede tener la entidad, se pueden utilizar herramientas orientadoras con preguntas para identificar de manera general el grado de vulnerabilidad al que puede estar expuesta la entidad en el desarrollo de sus funciones, y que puede ser complementado en la medida que se integren los procesos existentes en la entidad.

Fuente: Tomado de la Guía de Administración del Riesgo del DAFP, 2018 y 2025, adaptada a requerimientos LA/FT/FP y Decreto 2157 de 2017

2. IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos y oportunidades que estén o no bajo el control de la organización, 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, las funciones de la entidad, la estructura organizacional, grupos de valor que atiende, recursos y otras particularidades que permiten cumplir con la misionalidad, y, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas. (NTC ISO31000, Numeral 2.15).

2.1. IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO

En esta etapa se busca la identificación de los riesgos clave y la asociación de estos frente a los objetivos de los procesos. Para llevar a cabo este análisis se debe considerar, adicional al objetivo del proceso, su estructura y actividades clave contempladas en la caracterización del proceso y la forma como participa dentro del mapa de procesos.

Así mismo, es importante tener en cuenta la documentación del proceso: contexto estratégico, procedimientos, guías, protocolos, manuales, instructivos, documentos soporte y formatos, entre otros. Así como, la cadena de valor público, desde insumos, procesos, productos, servicios, resultados, efectos e impactos y el cumplimiento de los objetivos (eficacia y eficiencia).

Por último, se deben considerar las actividades dentro del flujo de los procesos que implican un intercambio de recursos, bien sea porque la entidad recibe un bien o servicio por el cual paga un precio, o porque entrega un bien o servicio por el cual le pagan un precio.

IDENTIFICACIÓN DE LOS PUNTOS DE RIESGOS FISCAL Y CIRCUNSTANCIAS INMEDIATAS

Los puntos de riesgo son eventos en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal de los últimos 5 años.

En cuanto a las circunstancias inmediatas son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo. Por cada punto de riesgo, con frecuencia existen múltiples circunstancias inmediatas.

IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Como primer paso para la identificación de riesgos de seguridad de la información es necesario que cada proceso identifique sus activos de información de acuerdo con lo establecido en el procedimiento GTI-PC-04 Activos de Información.

Según el nivel de criticidad de los activos se realiza el análisis y gestión de riesgos, con respecto al activo de información se registran los siguientes datos:

Proceso: Proceso al cual se encuentra asignado el activo de información.

Referencia: Es el número del ítem del activo de información.

Activo de Información: Es el nombre del activo de información.

Tipo de Activo: Corresponde a una de las categorías establecidas en el formato GTI-FM-08 Inventario de Activos de Información y cuadro de caracterización documental

2.2. IDENTIFICACIÓN DE ÁREAS DE IMPACTO

El área de impacto es la consecuencia negativa en el cumplimiento de los objetivos de los procesos en caso de la materialización de un riesgo la cual puede ser económica o reputacional. En materia de seguridad de la información, el área de impacto también corresponde a la que por causa de incidentes de seguridad de la información tenga consecuencias en la gestión de la entidad.

En cuanto a los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio. Las consecuencias legales y de contagio, para efectos de determinar el impacto del riesgo, deben analizarse en términos de afectación económica.

RIESGOS FISCALES

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público. Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública.

2.3. IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Las cuales hacen referencia a las fuentes generadoras de riesgos que puede tener una entidad. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición. La Guía para la administración de riesgos DAFP V7, señala a manera de ejemplo, las siguientes:

TABLA 4 FACTORES DE RIESGO

FACTOR	DEFINICIÓN	DESCRIPTORES
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	• Falta de aplicación de los procedimientos • Falta segregación de funciones • Errores de grabación, autorización • Falta de supervisión o interventoría • Errores en cálculos para pagos internos y externos • Alta rotación o insuficiencia de personal • Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo • Acciones contrarias a las leyes o acuerdos contractuales • Falta de capacitación y otros temas relacionados con el personal

FACTOR	DEFINICIÓN	DESCRIPTORES
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 • Hurto de activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad	• Daño de equipos • Caída de sistemas de información y aplicaciones • Caída de redes • Errores en hardware o software • Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad	• Derrumbes • Incendios • Inundaciones • Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad	• Fraude Externo • Suplantación de identidad • Asalto a la oficina

FACTOR	DEFINICIÓN	DESCRIPTORES
		Atentados, vandalismo, orden público

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7, DAFP – agosto de 2025

Frente al factor del talento humano es importante resaltar que este se asocia a la integridad pública y que el factor de Infraestructura se asocia a los riesgos de desastre, para los cuales se tendrán en cuenta los escenarios de riesgos identificados y definidos en la Estrategia Distrital de Respuesta a Emergencias- EDRE 2023, de acuerdo con los servicios y funciones de respuesta establecidos y adoptados en la Estrategia Institucional de Respuesta de la UAESP.

Escenarios de riesgos identificados para la ciudad de Bogotá:

- Escenario de Riesgo Sísmico.
- Escenario de Riesgo por Inundación.
- Escenario de Riesgo por Movimientos en Masa.
- Escenario de Riesgo por Avenidas Torrenciales.
- Escenario de Riesgo por Incendios Forestales.
- Escenario de Riesgo de Origen Tecnológico.
- Escenario de Riesgo por Actividad de la Construcción.
- Escenario de Riesgo por Aglomeraciones de Público.

Igualmente, la gestión de riesgos de seguridad de la información en la UAESP debe tener en cuenta los lineamientos generales señalados en el documento de Políticas de seguridad y privacidad de la información, que hace parte del Sistema integrado de gestión (SIG) de la entidad.

Así mismo se deberán identificar dos elementos importantes: Amenazas (Causa Inmediata) y Vulnerabilidades (Causa raíz), las amenazas pueden tener origen deliberado, fortuito o ambiental. Se debe señalar que la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una

debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

TABLA 5 AMENAZAS COMUNES

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Pérdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F

TIPO	AMENAZA	ORIGEN
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7,

DAFP – agosto de 2025

TABLA 6 AMENAZAS COMUNES

TIPO	VULNERABILIDADES
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al 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
	Ausencia de registros de auditoría
	Asignación errada de los 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

Unidad Administrativa Especial de Servicios Públicos

Cra 10 No. 17-72 L-119

PBX: (+57) 601 358 0400

www.uaesp.gov.co

TIPO	VULNERABILIDADES
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran 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 de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7,
DAFP – agosto de 2025

IDENTIFICACIÓN DEL EFECTO ECONÓMICO RIESGO FISCAL

Es el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público. Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes: (i) Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones. (ii) Los efectos económicos generados por causas

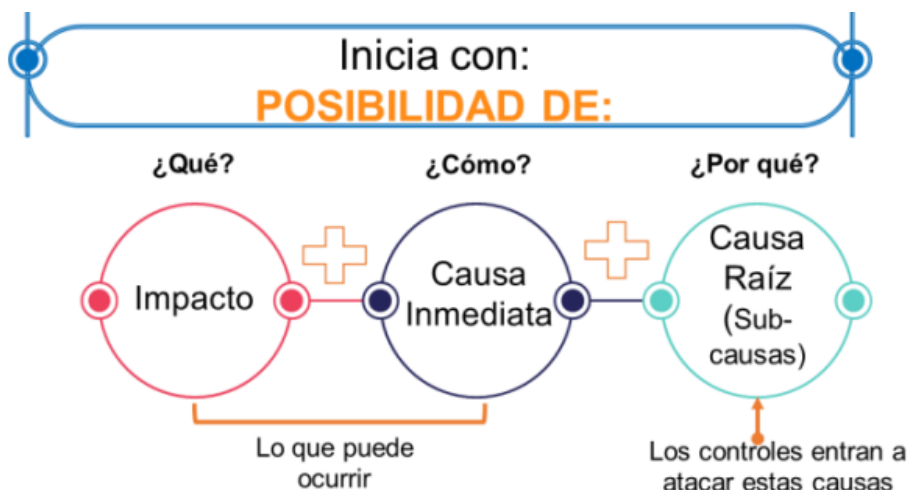
exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público (iii) Multas impuestas por hechos que no comportan gestión fiscal (iv) Existencia de actuación de cobro coactivo por parte de la entidad. (v) Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural. (vi) Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su “normal uso” (máquinas eléctricas, computadores, celulares, etc.). (Contraloría General de la República, 2023, p. 12)

2.4. DESCRIPCIÓN DE RIESGOS

A partir del punto de riesgo, área de impacto y área(s) de factor(es) de riesgo identificados, se debe proceder con la 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:

ILUSTRACIÓN 4 ESTRUCTURA PROPUESTA PARA LA REDACCIÓN DEL RIESGO



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7,
DAFP – agosto de 2025

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa inmediata:** circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Estos dos elementos permiten plantear el evento no deseado ¿qué puede ocurrir?, es decir la situación, acción, condición o suceso incierto que, si ocurre, podría afectar el logro de los objetivos de la entidad.

Características clave: Debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar

- **Causa raíz:** es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo ¿por qué puede ocurrir?, son la base para la definición

de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Características clave: Identificar causas raíz y condiciones contribuyentes que pueden clasificarse en: humanas, tecnológicas, normativas, ambientales, organizacionales.

En la definición del riesgo se debe evitar iniciar con palabras negativas como: “No...”, “Que no...”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en...”

No describir como riesgos omisiones ni desviaciones del control. Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

No describir causas como riesgos Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

No describir riesgos como la negación de un control. Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

No existen riesgos transversales, lo que pueden existir son causas transversales. Ejemplo: pérdida de expedientes.

Así las cosas, el modelo de descripción del riesgo contiene los siguientes elementos:
Evento no deseado y sus posibles consecuencias: ¿Qué puede pasar?

Causas: ¿Por qué puede pasar?

Tipología: ¿A qué categoría pertenece?

Factor de riesgo: ¿Qué condición aumenta su probabilidad?

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para los riesgos de seguridad de la información se debe incluir el tipo de riesgo y la clasificación del riesgo.

Tipo de Riesgo: Este campo solo admite uno de estos 3 valores:

- Pérdida de Disponibilidad
- Pérdida de Integridad
- Pérdida de Confidencialidad

Clasificación del Riesgo: Este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad.

RIESGOS PARA LA INTEGRIDAD

Las causas inmediatas de los riesgos para la integridad pública podrán ser el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP.

IDENTIFICAR LA CAUSA RAÍZ Y DESCRIPCION DEL RIESGO FISCAL

Para redactar un riesgo fiscal se debe tener en cuenta:

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

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:

ILUSTRACIÓN 5 ESTRUCTURA PROPUESTA PARA LA REDACCIÓN DE RIESGOS FISCALES



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7, DAFP – agosto de 2025

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

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal (efecto dañoso). Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales. Al ser la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador. Es fundamental entonces, deslindar el hecho que ocasiona el daño (evento potencial o causa raíz), del daño propiamente dicho (efecto dañoso)

3. ANALISIS DE RIESGO INHERENTE

Esta etapa se realiza para establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de establecer los niveles de severidad o inherente, lo cual se deberá diligenciar en el formato DES-FM-12 Mapa y plan de manejo de riesgos y oportunidades de la UAESP, en el cual se tienen formulados y especificados estos criterios.

3.1. DETERMINAR LA PROBABILIDAD

La probabilidad constituye la exposición al riesgo del proceso, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

ILUSTRACIÓN 6 CRITERIOS PARA DEFINIR EL NIVEL DE PROBABILIDAD

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7,
DAFP – agosto de 2025

3.2. DETERMINAR EL IMPACTO

El impacto se medirá frente a dos factores principales: económico (ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal, entre otras) y reputacional (afectación a la imagen

institucional por vulneraciones a la información o por fallas en la prestación del servicio, entre otras).

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles, se debe tomar el nivel más alto entre ellos.

ILUSTRACIÓN 7 CRITERIOS PARA DEFINIR EL NIVEL DE IMPACTO

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

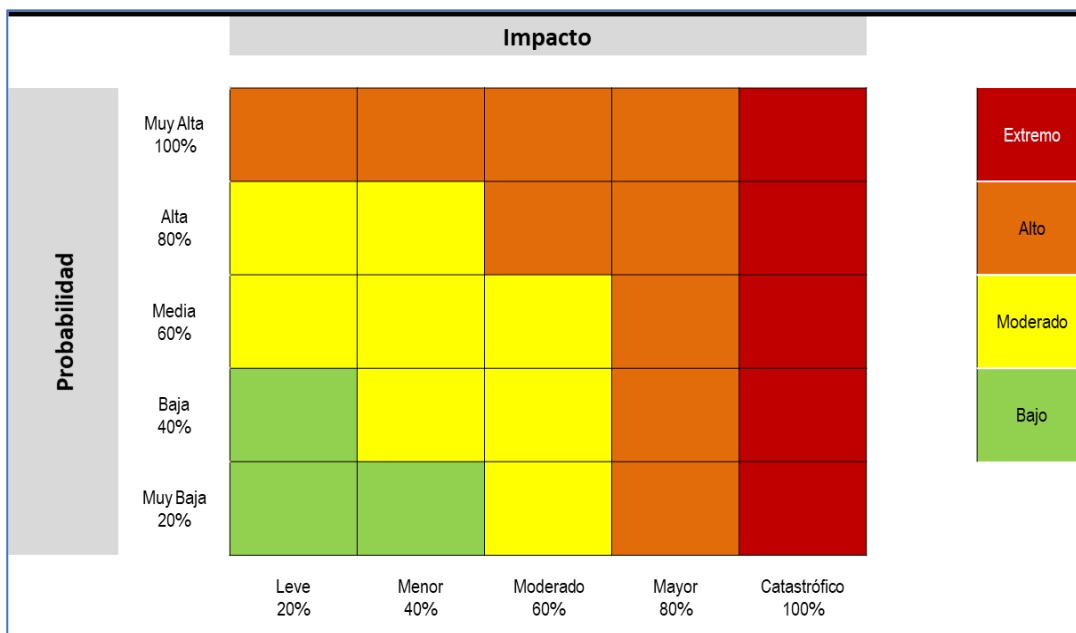
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7,
DAFP – agosto de 2025

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso recae sobre un bien, recurso o interés patrimonial de naturaleza pública.

3.3. ANÁLISIS DE SEVERIDAD

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar los niveles de severidad (RIESGO INHERENTE), ubicándolo en una de cuatro zonas de severidad: Bajo, moderado, alto, extremo. En un mapa de calor:

ILUSTRACIÓN 8 MAPA DE CALOR



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7, DAFP – agosto de 2025

El mapa de calor permite visualizar los riesgos en las zonas definidas (Bajo, Moderado, Alto Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a buscar o retener (apetito del riesgo) en función del impacto de estos en la Entidad.

Esta matriz de 5 x 5, traza en su eje X el impacto y en su eje Y la probabilidad de ocurrencia.

Los riesgos que se encuentran en las zonas más altas o de mayor gravedad son los que se priorizan, disminuyéndose el nivel de aceptación. Es importante determinar para estos tipos de riesgos el plan de contingencia¹⁰ que defina las actividades de control (correctivas) que ataquen las causas del riesgo, cuando éste se llegue a materializar.

¹⁰ Para la gestión de riesgos de desastres corresponde a los Planes de Emergencias y Contingencia- PEC

Esto ayuda a la Entidad a mejorar su administración de riesgos, priorizando los esfuerzos y acciones sobre los riesgos potencialmente de mayor impacto.

4. DISEÑO Y ANÁLISIS DE CONTROLES

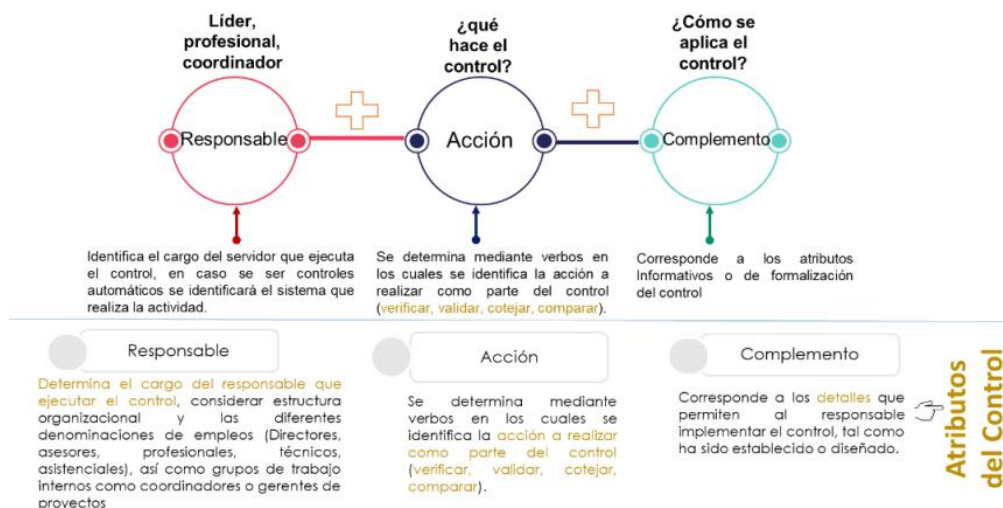
Para realizar el tratamiento de los riesgos se formularán los controles por proceso a fin de atender el riesgo inherente, dejando como resultado el riesgo residual, el cual deberá abordarse a través de acciones no rutinarias del proceso es decir acciones de plan de manejo.

Los controles son acciones concretas y rutinarias documentadas los cuales deberán atender las causas raíz identificadas y enfocarse en la gestión de los factores de riesgo previamente identificados.

4.1. ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL

Para el diseño del control se tendrán en cuenta la siguiente estructura:

ILUSTRACIÓN 9 ESTRUCTURA PARA LA REDACCIÓN DE CONTROLES



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7,
DAFP – agosto de 2025

- Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad y el responsable de su calibración o parametrización periódica.
- Acción: Se determina mediante verbos que indican la acción que deben realizar como parte del control. Se utilizar verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar.
- Complemento: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos:
 - Documentación: Se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
 - Frecuencia: Corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
 - Evidencia: Permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
 - Ejecución: Permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten. Puede darse a través de la comparación con información interna, externa o mixta.

NOTA PARA EL DISEÑO DE CONTROLES DE RIESGOS DE SEGURIDAD DE LA INFORMACION

De acuerdo con la Guía de Riesgos DAFP v.7 las entidades podrán mitigar/tratar los riesgos de seguridad de la información empleando los controles del Anexo A de la ISO/IEC 27001:2022, siempre y cuando se ajusten al análisis de riesgos.

a. Tipología de los controles: Según etapa del ciclo del proceso (entrada → Ejecución → salida)

- Preventivos: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Va a las causas del riesgo, atacan la probabilidad de ocurrencia.
- Detectivos: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, y devuelve el proceso a los controles preventivos, por lo que generan reprocesos. atacan la probabilidad de ocurrencia.
- Correctivos: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Atacan el impacto frente a la materialización del riesgo.

b. Tipología de los controles: Según forma de ejecución:

- Manual: Controles que son ejecutados por personas.
- Automático: Son ejecutados por un sistema o software previamente programado o diseñado.

4.2. VALORACIÓN DE CONTROLES

La valoración de controles determina la forma como se califican los atributos o características de Eficiencia, los demás atributos informativos o de formalización del control no cuentan con valoración, pero deben analizarse para garantizar su el diseño.

TABLA 7 VALORACIÓN DE CONTROLES

CARACTERÍSTICAS DE EFICIENCIA		PESO
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación	Automático	25%

CARACTERÍSTICAS DE EFICIENCIA		PESO
*Nota: En implementación no se tienen controles semiautomáticos.	Manual	15%

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7, DAFP – agosto de 2025

TABLA 8 ANÁLISIS ATRIBUTOS FORMALIZACIÓN DEL CONTROL

CARACTERÍSTICAS DE EFICIENCIA		DESCRIPCIÓN
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen)
	Otros Esquemas	Políticas de operación, manuales o guías específicas
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	

CARACTERÍSTICAS DE EFICIENCIA		DESCRIPCIÓN
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos)
	Mixta	Combinación de datos de fuentes internas y externas formales

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7, DAFP – agosto de 2025

5. VALORACIÓN DE RIESGO RESIDUAL

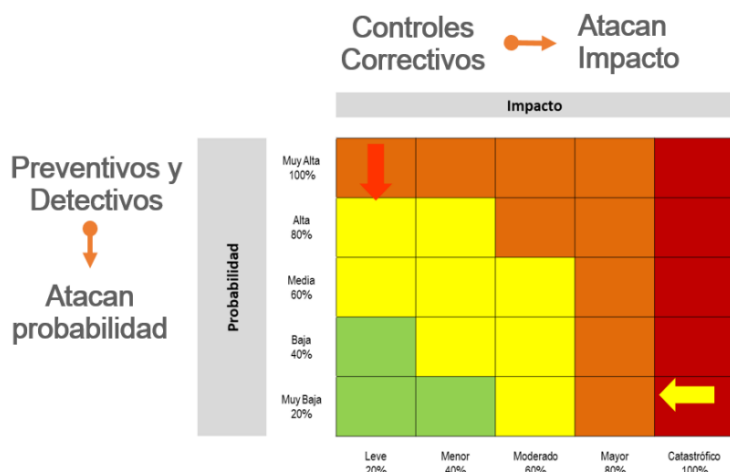
Sobre un mismo riesgo puede haber diversos controles, y estos operan de manera acumulativa sobre el riesgo, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. La sumatoria de los controles no podría dar 100%, ya que eso significaría que se ha eliminado el riesgo, lo cual no ocurre en realidad.

5.1. APLICACIÓN DE CONTROLES EN LA MATRIZ DE SEVERIDAD

Teniendo en cuenta que a partir de los controles se dará el movimiento en la matriz de calor, respecto al análisis de severidad, a continuación, se muestra cuál es el

movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

ILUSTRACIÓN 10 MOVIMIENTO EN LA MATRIZ DE CALOR ACORDE AL TIPO DE CONTROL



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7, DAFP – agosto de 2025

A modo de ejemplo se muestran a continuación los cálculos requeridos para la aplicación de 2 controles, uno preventivo y uno detectivo, para el caso no se cuenta con controles correctivos.

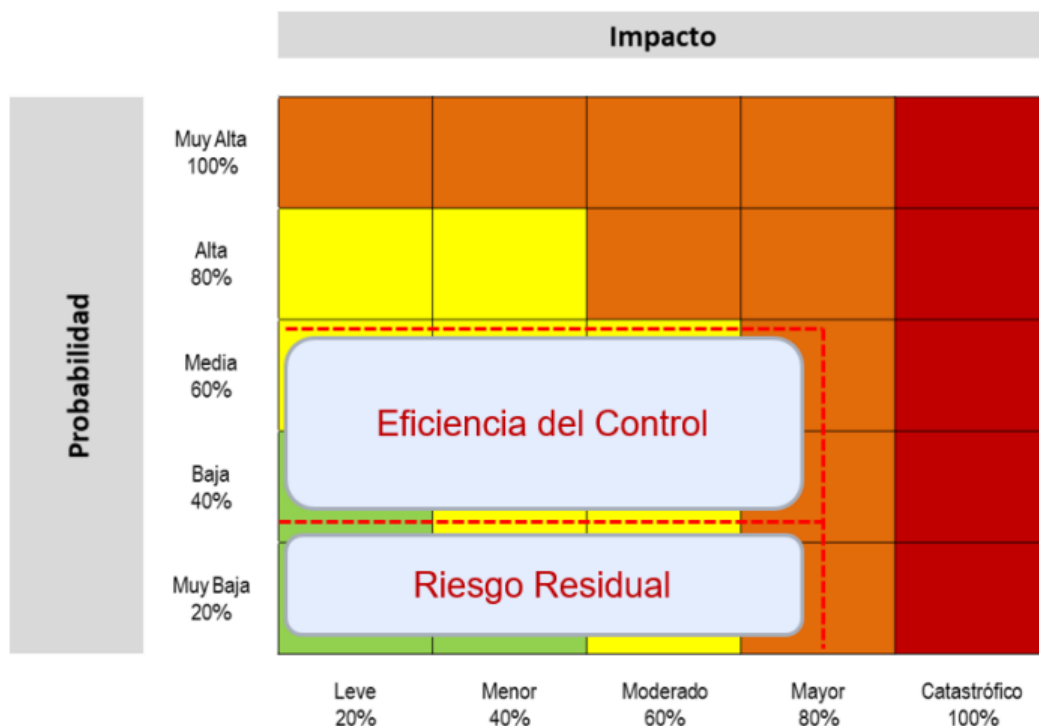
ILUSTRACIÓN 11 APLICACIÓN DE CONTROLES PARA ESTABLECER EL RIESGO RESIDUAL

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2º control				36%
	Valoración control 2 detectivo			30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual				25,2%
	Valoración de Impacto				
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual				80%

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7,
DAFP – agosto de 2025

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente en el riesgo inherente, por lo que no será posible su movimiento en la matriz para el eje de impacto.

ILUSTRACIÓN 12 MOVIMIENTO EN LA MATRIZ DE CALOR CON EL EJEMPLO PROPUESTO



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7,
DAFP – agosto de 2025

5.2. MAPA Y PLAN DE MANEJO DE RIESGOS Y OPORTUNIDADES CONSOLIDADO

El desarrollo metodológico se adelanta en el formato DES-FM-12 Mapa y plan de manejo de riesgos y oportunidades para cada proceso, vinculando las tipologías de riesgo aplicables, de acuerdo con las características de cada proceso, su complejidad, interacción con otros procesos, recursos, productos y servicios que gestiona y usuarios que atiende, ya seas internos o externos, garantizando la integralidad del análisis.

Igualmente se debe aplicar el procedimiento: DES-PC-07 Administración de riesgos y oportunidades, documento del SIG de la UAESP, que tiene por objeto: Definir las actividades para la administración del riesgo y las oportunidades, mediante la aplicación de la Política de administración del riesgo de la UAESP, a partir de la identificación y

valoración de los riesgos (análisis, evaluación, monitoreo y revisión), que permitan establecer los controles e implementar acciones para mitigar los impactos que afecten el cumplimiento de los objetivos institucionales y de proceso y abordar las oportunidades identificadas en el análisis del contexto de los procesos de la Unidad Administrativa Especial de Servicios Públicos – UAESP.

De acuerdo con la guía DAFP V7, además del mapa de riesgos, la UAESP puede acudir a otras herramientas para la administración del riesgo a saber:

- Revisión histórica de eventos materializados
- Indicadores claves de Riesgo (Key Risk Indicators- KRI)
- Hallazgos con incidencia fiscal

Así mismo la entidad puede acudir a la herramienta “mapas de aseguramiento”¹¹, para identificar riesgos con relación a aspectos clave para el éxito de gestión de la entidad, caso en el cual deben recibir el tratamiento establecido en esta política.

Los Indicadores Clave de Riesgos (KRI), hacen referencia a los datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No necesariamente indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente.

Teniendo en cuenta que los indicadores clave de riesgos requieren, al igual que los indicadores de gestión el desarrollo de los siguientes temas: Nombre del indicador, una descripción de lo que se va a medir, la fórmula de cálculo, la fuente de información para el cálculo del indicador, por ejemplo: sistemas internos, reportes de auditoría, bases de datos internas o externas u otras fuentes, la frecuencia de medición y seguimiento y los umbrales de alerta, estos indicadores se formularán en el marco de la implementación del procedimiento DES-PC-08 Indicadores de Gestión utilizando el formato DES-FM-09 Hoja de Vida del Indicador.

¹¹ Circular 103 de 2020 de la Secretaría General de Bogotá.

Sin embargo, para definir los umbrales de alerta se debe tomar como base el apetito del riesgo así:

- Valor del KRI dentro del apetito al riesgo: Significa que la operación de la entidad, y por ende el riesgo se sigue moviendo dentro de lo que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección.
- Valor del KRI que excede el apetito al riesgo: Significa que el riesgo ha superado el umbral que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. En este caso se deben tomar acciones correctivas o de mitigación para llevar el riesgo de nuevo hacia un rango tolerable.
- Valor del KRI se acerca al umbral de alerta definido: Revela que el riesgo se ha ido aumentando y que podría salir del umbral de alerta si continua así.

6. MONITOREO Y REVISIÓN

Los riesgos de la UAESP se revisarán y validarán mínimo una vez al año con el acompañamiento de la Oficina Asesora de Planeación y la asesoría de la Oficina de Control Interno, sin embargo, se podrán actualizar en cualquier momento considerando las condiciones de operación internas o externas. Cada líder de proceso actualiza el análisis de contexto, riesgos y controles como resultado de los ejercicios de autocontrol, autoevaluación, evaluación independiente o por decisión del CICCÍ según estime conveniente para asegurar el cumplimiento de los objetivos del proceso.

El proceso realizará el seguimiento mensual a sus controles y acciones, reportándolo en el espacio definido del trimestre para el seguimiento de la segunda línea de defensa a través el mapa y plan de manejo de riesgos y oportunidades, el seguimiento incluye el estado de la gestión de las acciones y controles formulados junto con las evidencias correspondientes, describiendo concretamente si hubo o no riesgos materializados.

Si se identifican riesgos materializados por cualquiera de las líneas de defensa, de manera inmediata se ejecutan las acciones del plan de contingencia, previamente formulado, para su tratamiento realizando el análisis de causas correspondiente.

La segunda línea de defensa realizará el seguimiento trimestral y lo consignará en el mapa y plan de manejo de riesgos y en el informe que presente al Comité institucional de Gestión y Desempeño.

Por su parte la Oficina de Control Interno como tercera línea de defensa evalúa los riesgos a través de las auditorías, evaluaciones y seguimientos en desarrollo del plan anual de auditorías y seguimientos definidos para la vigencia. La evaluación de los riesgos por la tercera línea de defensa deberá realizarse tres veces al año así:

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.

- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

Frente a los riesgos de lavado de activos y financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva se recomienda tener en cuenta lo siguiente:

ILUSTRACIÓN 13 AMBIENTE DE CONTROL EN LA/FT/FP

Aspectos a considerar con respecto a Ambiente de Control

- **Cultura organizacional:** integrar lenguaje y operatividad.
- **Plan Institucional de Capacitación:** fortalecer aptitudes para prevención LA/FT en la Entidad.
- **Código de Ética:** complementar reglas de conducta y acciones frente a posibles inobservancias.
- **Gestión de conflictos de interés:** integrar lineamientos para la prevención y resolución.
- **Mecanismos de Debida Diligencia.**
 - Definir **roles y responsabilidades** en la gestión y prevención de LA/FT
 - Diseño e Implementación de estrategias y actividades, e integrarlas en el **Programa de Transparencia y Ética Pública**

Fuente: Documento Técnico Lavado de Activos y Financiación del Terrorismo

7. RIESGOS MATERIALIZADOS

Cuando se detecte la materialización de los riesgos, se establece los siguientes pasos a realizar por tipos de riesgos:

- a. Materialización de riesgos detectada por parte del líder del proceso (primera línea de defensa):

- Si el riesgo es contra la integridad pública se deberá informar a la Alta Dirección sobre el hecho encontrado. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo y poner en conocimiento a la Oficina Control Disciplinario Interno.
 - Si el riesgo es de gestión, desastre¹², fiscal y de seguridad de la información, se deberá realizar el análisis de causas y determinar acciones preventivas y de mejora. Análisis y actualización del mapa de riesgos.
 - Si el riesgo es contra la integridad pública por Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva se deberá informar a la Alta Dirección sobre el hecho encontrado, este deberá denunciarse a través del reporte de operaciones inusuales (interno) y reporte de operaciones sospechosas que deben ser reportadas a la UIAF (Unidad de Información y Análisis Financiero. Así mismo, deberá poner en conocimiento a la Oficina Control Disciplinario Interno.
- b. Materialización de riesgos detectada por la Oficina Asesora de Planeación (segunda línea de defensa):
- En los casos de riesgos contra la integridad pública detectado por la segunda Línea de defensa, se debe informar sobre el hecho encontrado a la Oficina de Control Interno y a la Oficina Control Disciplinario Interno, para lo de su competencia, de considerarlo necesario, realizar la denuncia ante el ente de control respectivo y a la Alta Dirección sobre el hallazgo y las acciones tomadas, informar al líder del proceso, para revisar el mapa de riesgos y sus controles asociados y verificar que se tomaron las acciones y se actualizó el mapa de riesgos.

¹² Ante la materialización de los riesgos de desastre se deberá llevar a cabo la implementación para la respuesta a emergencias definido en el Plan de Gestión del Riesgo de Desastres de las Entidades Públicas y Privadas- PGRDEPP y la Estrategia Institucional de Respuesta- EIR de la entidad

- En los casos de riesgo contra la integridad pública por Lavado de Activos, Financiación del terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva detectado por la segunda Línea de defensa, se debe comunicar a la Oficina de Control Interno y a la Oficina Control Disciplinario Interno, para lo de su competencia y al líder del proceso sobre el hecho encontrado, para que realice la revisión, análisis y acciones correspondientes para resolver el hecho, verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente e informar a la Alta Dirección sobre el hallazgo y las acciones tomadas, de igual manera deberá denunciarse a través del reporte de operaciones inusuales (interno) y reporte de operaciones sospechosas que deben ser reportadas a la UIAF (Unidad de Información y Análisis Financiero).
- En los casos de riesgos de gestión desastre¹³, fiscal y de seguridad de la información, detectado por la segunda Línea de defensa, se debe comunicar a la Oficina de Control Interno, para lo de su competencia y al líder del proceso sobre el hecho encontrado, para que realice la revisión, análisis y acciones correspondientes para resolver el hecho, verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente e informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.
- c. Materialización de riesgos detectada por parte de la Oficina de Control Interno (tercera línea de defensa):
 - Si el riesgo es contra la integridad pública, debe poner en conocimiento a la Oficina Control Disciplinario Interno y al representante legal, asimismo, se deberá convocar al Comité Institucional de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. Dependiendo del alcance (normativa asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. Facilitar el inicio de las acciones correspondientes con el líder del

¹³ Idem

proceso, para revisar el mapa de riesgos y sus controles asociados. Verificar si se tomaron las acciones y si se actualizó el mapa de riesgos.

- En los casos de riesgo contra la integridad pública por Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva detectado por la tercera línea de defensa, se debe comunicar a la Oficina Control Disciplinario Interno, para lo de su competencia y al líder del proceso sobre el hecho encontrado, para que realice la revisión, análisis y acciones correspondientes para resolver el hecho, verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente e informar a la Alta Dirección sobre el hallazgo y las acciones tomadas, de igual manera deberá denunciarse a través del reporte de operaciones inusuales (interno) y reporte de operaciones sospechosas que deben ser reportadas a la UIAF (Unidad de Información y Análisis Financiero).
- Si el riesgo es de gestión, desastre¹⁴, fiscal o de seguridad de la información, informar al líder del proceso sobre el hecho encontrado y orientarlo frente a la revisión, análisis y acciones correspondientes para resolver el hecho. Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada.

8. DIVULGACIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Oficina Asesora de Planeación, en su calidad de Administrador del Modelo Integrado de Planeación y Gestión es el encargado de liderar y asesorar en los lineamientos impartidos para el fortalecimiento del Sistema de Control Interno en la Unidad Administrativa Especial de Servicios Públicos, con el acompañamiento de la Oficina de Control Interno a los líderes, gestores y equipo de cada proceso, con el fin de que conozcan y fortalezcan las líneas de defensa que permitirá generar tratamientos eficientes y efectivos a los riesgos que puedan afectar los objetivos institucionales.

¹⁴ Idem

Esta política debe ser publicada por la segunda línea de defensa en la página web de la entidad y comunicada a todos los servidores públicos, a través de las herramientas de comunicación interna con las que cuenta la entidad, encaminadas a la apropiación de esta política. En todo caso, todas las dependencias de la entidad realizarán la socialización y capacitación de esta política y sus componentes a los servidores adscritos a cada una de ellas a fin de dinamizar la cultura del riesgo en todas las operaciones institucionales.

El mapa de riesgos de corrupción se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.

En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación

Las excepciones a la publicación de información solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

9. DIRECTRICES GENERALES DE LA DEBIDA DILIGENCIA

La debida diligencia es la identificación de la persona natural o jurídica que celebra el contrato, identificación del beneficiario final, objetivo del contrato estatal e identificación de fuentes de fondos, perfil de riesgo y actividad comercial.

En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, se debe desarrollar el principio de debida diligencia en todas las interacciones con contrapartes, en las que exista una exposición a riesgos para la integridad pública, es

decir, en aquellas interacciones en que se haya identificado un riesgo de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.

Este principio debe aplicarse en concordancia con el principio de razonabilidad utilizando mecanismos adecuados para los fines que persigue y necesarios para alcanzarlos, y el principio de proporcionalidad utilizando mecanismos se apliquen desde un enfoque basado en riesgos.

9.1. REVISION Y DETECCION DE OPERACIONES SOSPECHOSAS DE LA/FT/FP

La revisión y detección de operaciones sospechosas tiene como finalidad identificar las actividades, hechos y operaciones, que por sus características no son razonables respecto de una actividad económica o sector y que las hace sospechosas. Con el propósito de generar un ambiente de detección, la entidad debe definir mecanismos específicos para dar cumplimiento a las medidas aquí sugeridas con las siguientes acciones:

- Comprobar
- Supervisar
- Observar críticamente
- Registrar los procesos derivados de una nueva actividad, acción o sistema

En un primer nivel, ello permite identificar las operaciones inusuales que fueron generadas en el proceso de monitoreo respecto del control detectivo y que sugieren ser evaluadas. Es decir, se debe detectar las operaciones inusuales con base en el registro de usuarios o clientes, Personas Públicamente Expuestas (PEP's) proveedores y la existencia de cambios atípicos en las operaciones como los montos y el número de transacciones relacionadas con los productos, bienes o servicios ofrecidos por la entidad distrital.

Detectadas las operaciones inusuales, se analizan y se determinan los criterios objetivos que le otorgan características sospechosas de LA/FT/FP catalogándolas como importantes y significativas por su grado de complejidad, debido a que se salen de los patrones habituales sin fundamento a fin de remitirlas a la UIAF de manera oportuna.

9.2. POLITICAS DE MIPG RELACIONADAS DIRECTAMENTE CON LA PREVENCIÓN DE LA/FT/FP

Política de Planeación Institucional

Política que permite orientar a las entidades para que establezcan mecanismos para organizar, articular y alinear en forma coherente las acciones y los recursos, para el cumplimiento de su propósito fundamental. Es desde la planeación cuando las entidades definen las políticas que se adopten para permitir el eficiente, efectivo y oportuno funcionamiento del SARLAFT y traducirse en reglas de conducta y procedimientos que orienten la actuación de la entidad y de sus colaboradores frente a la prevención del LA/FT/FP.

Política de Gestión Estratégica de Talento Humano

A través de los servidores públicos las entidades distritales realizan la ejecución de sus actividades o productos, siendo estos los actores principales para la implementación de mecanismos o herramientas de gestión y control; por otra parte, la GETH plantea la necesidad de alinear las prácticas de talento humano con los objetivos y el propósito fundamental de la entidad, establece el ciclo de vida laboral y los componentes del talento humano, lo cual permite alinear dentro de estas

etapas los procesos de capacitación, inducción y reinducción. En lo referente al LA/FT/FP, las entidades distritales deben diseñar, programar y coordinar planes de capacitación sobre el SARLAFT dirigidos a todos los procesos de la entidad.

Política de transparencia,
acceso a la información pública
y lucha contra la corrupción

La política de transparencia y acceso a la información pública se basa en garantizar un flujo efectivo y constante de información; asimismo, promueve el seguimiento a su gestión y el logro de los objetivos institucionales, al tiempo que fortalece la confianza de la ciudadanía en la entidad y en la gestión pública. Este mecanismo se fortalece a través de la implementación del sistema SARLAFT en las entidades distritales. La principal herramienta de esta política es el Programa de Transparencia y Ética Pública – PTEP.

Política de Integridad

Política que propende por la construcción y fortalecimiento de una cultura de integridad en el servicio público, desde un marco de valores y principios referentes que contribuyan a un enfoque de prevención en la lucha contra la corrupción, orientando la actuación de los funcionarios de cada entidad para el funcionamiento del SARLAFT, con énfasis en la gestión y manejo de conflicto de intereses; todo esto fortalece el rechazo a los comportamientos

indebidos que afecten negativamente los recursos de la gestión pública Distrital.

Política de gestión documental

La gestión documental permite preservar y acceder a los documentos que soportan la información esencial de las entidades. Con su aplicación se busca mayor eficacia administrativa, la promoción de la transparencia y el acceso a la información pública y la protección del patrimonio documental. Esta se articula desde dos perspectivas: por un lado, dando la línea para la conservación de los soportes, informes, reportes y demás documentos originados en cualquier etapa del SARLAFT; por otro lado, como activo orientado a la garantía del derecho de acceso a la información pública.

Política de fortalecimiento organizacional y simplificación de proceso

Esta política de gestión busca identificar la dinámica organizacional, en relación con su cadena de valor, para establecer escenarios de mejora basados en la estandarización y la optimización de las actividades institucionales. Permitirá la estructuración del organigrama, manuales, procedimientos y controles, entre otros, para la implementación del SARLAFT.

Política de Seguimiento y Evaluación del desempeño institucional

Esta política genera lineamientos para que la entidad realice seguimiento y evaluación a su gestión y desempeño, monitoreando permanentemente sus metas, tiempos y recursos,

coadyuvando al desarrollo de una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua. Se articula con el SARLAFT como mecanismo de monitoreo y seguimiento a los perfiles de riesgo relacionados con el LA/FT/FP.

Política de Control Interno

De acuerdo con la Ley 87 de 1993, el Sistema de Control Interno está integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación, requeridos para determinar que todas las actividades, operaciones y actuaciones de las entidades, se realicen de acuerdo con las normas constitucionales y legales. En este orden de ideas el SARLAFT se relaciona directamente con los componentes del MIPG, que se homologan a las etapas del SARLAFT, llevando a cabo la detección de operaciones inusuales o sospechosas, acorde a los procedimientos y controles establecidos por cada entidad.

CONTROL DE CAMBIOS:

TABLA 9 CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
01	24/05/2019	Aprobado en el Comité Institucional de Coordinación de Control Interno, Acta No 2, reunión extraordinaria del 24 de mayo de 2019.

Versión	Fecha	Descripción de la modificación
02	29/01/2021	Se actualizan términos que fueron derogados como el MTO, se incluye el marco normativo de la política y se elimina el tema de desastres debido a que la Política de administración de riesgos de la función pública versión 4 2018, no lo incluye. La actualización se realiza teniendo en cuenta la guía de administración de riesgos versión 4 2018.
03	29/12/2021	Se actualiza de acuerdo con lo definido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020 del DAFP, la guía para desarrollar el mapa de aseguramiento y el Manual operativo del MIPG V4, y la Norma ISO 9001:2015.
04	31/01/2023	Se actualiza de acuerdo con lo definido por el Documento Técnico de Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital. de la Secretaría General de la Alcaldía Mayor de Bogotá- diciembre 2022, la Ruta metodológica para la Implementación del SARLAFT en las Entidades Distritales, y se articula con la Guía para la administración del riesgo y el diseño de controles en entidades públicas – versión 5- diciembre 2020 del DAFP en la identificación, medición y evaluación, control y monitoreo de los riesgos.
05	19/09/2023	Se realiza el ajuste de la estructura de la política conforme a lo establecido en la versión 6 de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, incluyendo lo pertinente a la administración de riesgos fiscales y riesgos de desastres contemplados en el Decreto 2157 de 2017.

Versión	Fecha	Descripción de la modificación
06	27/11/2025	Se realiza el ajuste de la estructura de la política conforme a lo establecido en la versión 7 de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, incluyendo lo pertinente a la administración de riesgos contra la integridad pública y la estandarización del análisis del riesgo inherente.

Fuente: UAESP

AUTORIZACIONES:

TABLA 10 AUTORIZACIONES

	NOMBRE	CARGO	FIRMA
Elaboró	Aida Yolima Zarate Aguillón	Técnico Oficina de Planeación	Acta No 02 del 27/11/2025 Comité del Comité Institucional de Coordinación de Control Interno - CICCI
Revisó	Luz Mary Palacios Castillo	Profesional Universitario Oficina de Planeación	
Revisó y Aprobó	Comité Institucional de Coordinación de Control Interno		