POLITICA DE ADMINISTRACIÓN DEL RIESGO

Unidad Administrativa

Especial de Servicios Públicos

Septiembre de 2023

ALCALDÍA MAYOR DE BOGOTÁ D.C.

UAESP
Unidad Administrativa Especial de Servicios Públicos

BOGOTÁ

Contenido

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 6, en noviembre de 2022[1], Igualmente busca 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 gestionar los riesgos, teniendo en cuenta los diferentes lineamientos correspondientes a los riesgos de gestión, fiscales, corrupción, seguridad de la información, desastres[2] y lavado de activos y financiamiento del terrorismo en la estructura de procesos de la UAESP.

Para la vigencia 2023 surge la necesidad de actualizar los documentos del Sistema de Gestión enfocados en la Gestión del Riesgo, por cuanto es deber de la entidad incorporar los nuevos lineamientos emitidos por la Secretaría General de la Alcaldía Mayor de Bogotá a partir del Documento Técnico Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital[3], 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.

La incorporación de los nuevos lineamientos para LA/FT y desastres no modifica los lineamientos ya emitidos a través de la guía de riesgos establecida por el Departamento Administrativo de la Función Pública (DAFP) Versión 6, en noviembre de 2022. Dichos

[1] https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf/50bff85a-70c6-dd15-68f5-6cd2ea2a8707?t=1677003002032

[2] Decreto 2157 de 2017, artículo 2.3.1.5.2.1.1.

[3] Documento_Técnico_LA-FT_Diciembre_2022.pdf

lineamientos serán articulados en materia de identificación, medición y evaluación, control y monitoreo siguiendo la metodología ya aplicada para los riesgos de corrupción en la estructura de procesos de la UAESP.

Así mismo, en la presente actualización se incorporan 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 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 identificar, analizar, valorar y 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 5, marzo de 2023), 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.

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). Artículo2 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 Artículo73. "Plan Anticorrupción y de Atención al Ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.
- **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 Distrital 807 de 2019:** Reglamenta el sistema de gestión en el Distrito Capital.
- **Guía de administración del riesgo**: establecida por el Departamento Administrativo de la Función Pública – DAFP, V 6 (noviembre de 2022).
- **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 Standarization 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 adopto 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 DEFINICIONES[4]

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.

[4] Tomado de la Guía para la Administración del riesgo y el diseño de controles en entidades pública V4, V5 y V6 y Modelo de Seguridad y Privacidad de la Información - MSPI

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 puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea 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.

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 (Causa 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.

Causa Raíz (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.

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.

Control: Medida que permite reducir o mitigar un riesgo.

Debida diligencia: Es el proceso mediante el cual la entidad adopta medidas para el conocimiento de la contraparte, de su negocio, operaciones, y productos y el volumen de sus transacciones (Superintendencia de Sociedades de Colombia, 2021).

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 del Terrorismo (FT): Corresponde al conjunto de acciones que permiten la circulación de recursos que tienen como finalidad la realización de actividades terroristas o que pretenden el ocultamiento de activos provenientes de dichas actividades. Así mismo, está relacionada con los fondos, bienes o recursos a los que acceden las organizaciones terroristas o los terroristas para poder costear sus actividades (UIAF, 2013).

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)4 ” . 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.

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 susceptible 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): Es un delito que consiste en dar una apariencia lícita o de legalidad a bienes, dinerarios o no, que en realidad son productos o "ganancias" de delitos como tráfico ilícito de drogas, trata de personas, corrupción, secuestros y otros (UNODC, 2021).

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, entiéndase: rehabilitación y recuperación, según Ley 1523 de 2012.

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 (Superintendencia de Sociedades de Colombia, 2021).

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 Contagio: Es la posibilidad de pérdida en que incurre una entidad por una acción o experiencia de un vinculado, entendido este como el relacionado o asociado, incluyendo a las personas naturales o jurídicas que ejercen influencia sobre la entidad.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de LA/FT-FPADM: 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).

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.

SARLAFT: Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo.

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.

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.

3. 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, Corrupción, Seguridad de la información, Desastres y Lavado de Activos y Financiación del Terrorismo LA/FT, cuando aplique; en los procesos estratégicos, misionales de apoyo, evaluación y mejora que puedan afectar los objetivos institucionales de la Unidad, a través del establecimiento del contexto interno y externo, la identificación, valoración y seguimiento de los riesgos e implementación de controles y acciones para su prevención y mitigación y planes de contingencia ante su materialización, asegurando la capacidad para lograr los resultados del Modelo Integrado de Planeación y Gestión, la continuidad de las operaciones, el logro de los objetivos y metas institucionales 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 cuatro 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.

3.1. OBJETIVOS

3.1.1. GENERAL

Definir los parámetros de la administración del riesgo de la Unidad a través del establecimiento de mecanismos y herramientas que permitan la identificación, valoración, manejo y seguimiento 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.

3.1.2. 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, corrupción, seguridad de la información, desastres y Lavado de Activos y Financiación del Terrorismo LA/FT 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.

3.2. ALCANCE

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

Los riesgos de gestión, fiscales, corrupción y de desastres se tratarán por los lineamientos generales señalados en este documento.

Los riesgos de seguridad de la información se tratarán de acuerdo con los lineamientos generales de este documento, y los específicos para Modelo de Seguridad y Privacidad de la Información -MSPI.

Los riesgos de Lavado de Activos y Financiación del Terrorismo se tratarán de acuerdo con los documentos Técnicos de la secretaria general de la Alcaldía Mayor de Bogotá- y la Ruta Metodológica para la Implementación del SARLAFT en Entidades Distritales.

3.3. NIVELES DE ACEPTACIÓN

Acogiendo los lineamientos del DAFP en la Guía de administración del riesgo V.6, 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 administración del riesgo y el diseño de controles en entidades públicas - Versión 6, DAFP – noviembre de 2022

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 o desea 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 de corrupción y de Lavado de activos y Financiamiento del terrorismo LA/FT son inaceptables.

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]

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

Ilustración 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 de defensa hace el seguimiento mensual del riesgo, a través de ejercicios

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVELES DE ACEPTACIÓN	ACCIÓN A TOMAR
			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 plan de contingencia en caso de materialización para

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVELES DE ACEPTACIÓN	ACCIÓN A TOMAR
			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 correspondiente ya sea

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVELES DE ACEPTACIÓN	ACCIÓN A TOMAR
			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.

Para los riesgos de corrupción y de Lavado de activos y Financiamiento del terrorismo LA/FT es inaceptable.

3.4. 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 3 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 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.

3.5. METODOLOGÍA

La metodología corresponde a la establecida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 de noviembre de 2022 del DAFP, concretada en las etapas señaladas en el presente documento.

Los riesgos de Lavado de Activos y Financiación del Terrorismo se tratarán de acuerdo con el documento Técnico- diciembre de 2022 de la Secretaría General de la Alcaldía Mayor de Bogotá- (acápite 2, pags 36 y ss).

Los riesgos de desastres serán atendidos según los lineamientos establecidos en el Decreto 2157 de 2017.

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 y aplicando el procedimiento: “DES-FM-16 V3, Administración del riesgo”

En términos generales la administración del riesgo que se realizará es:

- Identificación 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.
    - Análisis de objetivos estratégicos y de los procesos
    - Identificación de los puntos de riesgo
    - Identificación de áreas de impacto
    - Identificación de áreas de factores de riesgo
    - Descripción del riesgo

  - Clasificación del riesgo
- Valoración: Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo inherente). Está integrada por el análisis y la evaluación del riesgo.
  - Análisis: Establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo inherente). Es decir, riesgo inicial a partir de la calificación de probabilidad e impacto e identificación de controles.
  - Evaluación: Confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo residual). Es decir, valoración del riesgo residual a partir de la calificación de probabilidad e impacto frente a los controles implementados.
- 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 CICCI según se ha establecido.

3.6. ROLES Y NIVELES DE RESPONSABILIDAD FRENTE AL RIESGO

A continuación, se relacionan los niveles de responsabilidad[6] 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 V6. 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 aseguramiento[7].

[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.

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 ámbito[8].

3.6.1. 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.
- 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

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

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

3.6.2. 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
- Aplicación efectiva de los controles, 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 auditoria para la actualización de los riesgos del proceso.

3.6.3. 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, análisis y valoración del riesgo, 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 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.

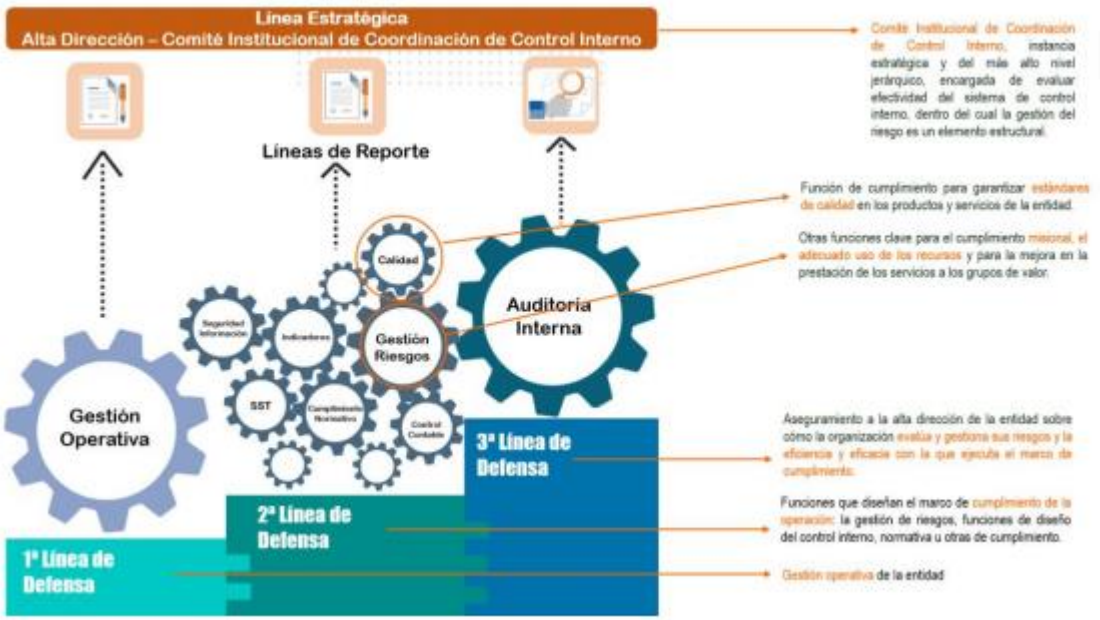
3.6.4. TERCERA LÍNEA DE DEFENSA

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 Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno CICCI 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.

Ilustración 4 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

4. IDENTIFICACIÓN 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 y, también, 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).

4.1. ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS, PARA IDENTIFICACIÓN DE LOS RIESGOS

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

4.1.1. ESTABLECIMIENTO DEL CONTEXTO - FACTORES INTERNOS Y EXTERNOS

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:

Ilustración 5 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.
	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

Tipo	Factores
	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, 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	Financieros: Presupuesto de funcionamiento e inversión, infraestructura.
	Personal: Competencia del personal, disponibilidad del personal, seguridad y salud en el trabajo, trabajo en equipo y liderazgo.
	Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción,
	Estratégicos: Planeación estratégica.
	Comunicación interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
	Infraestructura física: Área total construida, área libre, disposición de edificaciones, número de pisos, año de licencia de construcción, tipo de espacios y número, espacios comunitarios y equipamiento para emergencias existente, horario de funcionamiento, población expuesta al interior de la instalación evaluada.

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

Tipo	Factores
Proceso	Diseño del proceso: Claridad en la descripción del alcance y objetivo del proceso.
	Interacciones con otros procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios y clientes.
	Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	Procedimientos asociados: Pertinencia en los procedimientos que desarrollan los procesos.
	Responsables del proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación entre los procesos: Efectividad en los flujos de información determinados en la interacción de los procesos
	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.

Tipo	Factores
	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: Cuando se habla de los eventos, estos se pueden identificar teniendo en cuenta la fuente de los riesgos y las áreas afectadas, pero además la presencia de circunstancias, ocurrencias y sucesos asociados al riesgo de LA/FT, 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/FPADM 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, adaptada a requerimientos LA/FT y Decreto 2157 de 2017

4.2. IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO

Actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgos de gestión, desastres, fiscales, corrupción,

LA/FT y seguridad de la información los cuales se deben mantener bajo control para asegurar que el proceso cumpla con su objetivo.

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

LOS PUNTOS DE RIESGOS FISCAL son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas, es decir son todas las 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.

4.3. IDENTIFICACIÓN DE ÁREAS DE IMPACTO

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

RIESGOS FISCALES: 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 riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones. (ii) Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos,

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).

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.

4.4. IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Las cuales hacen referencia a las fuentes generadoras de riesgos que puede tener una entidad. La Guía para la administración de riesgos DAFP V6, señala a manera de ejemplo, las siguientes:

Ilustración 6 Factores de Riesgo

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caida de aplicaciones
			Caida de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

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

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.

Igualmente, la gestión de riesgos de seguridad de la información en la UAESP debe tener en cuenta los lineamientos generales señalados en el documento GTI-MN-01-Manual de políticas de seguridad y privacidad de la información, que hace parte del Sistema integrado de gestión (SIG) de la entidad.

4.5. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

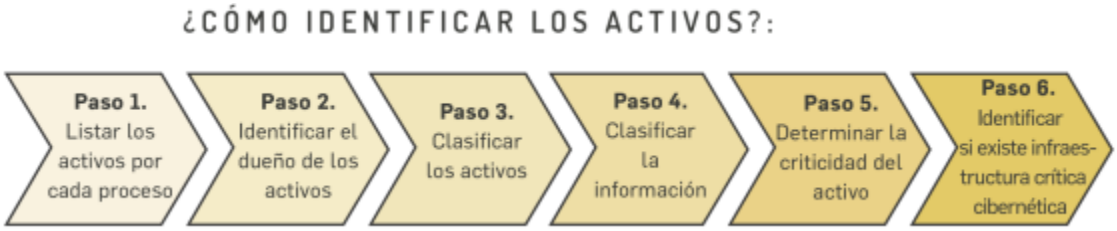
Como primer paso para la identificación de riesgos de seguridad de la información es necesario que cada proceso identifique sus activos de información.

Ilustración 7 Activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización -Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

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

Ilustración 8 Pasos para la identificación de activos



Fuente: Guía administración del riesgo DAFP V5./ Figura 21 Pasos para la identificación de activos

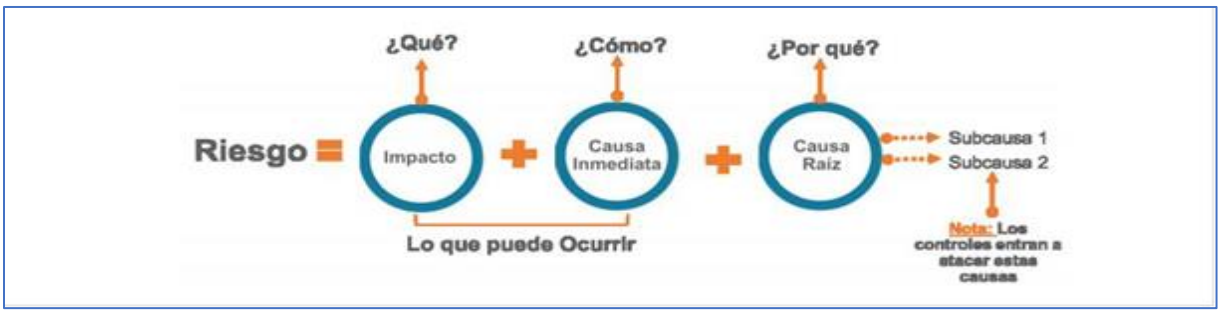
4.6. DESCRIPCIÓN DE RIESGOS

La identificación del riesgo se realiza determinando las causas, con base en el contexto interno, externo y del proceso ya analizado, y que pueden afectar el logro de los objetivos.

4.6.1. RIESGO DE GESTIÓN, DESASTRE Y SEGURIDAD DE LA INFORMACIÓN

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 9 Estructura propuesta para la redacción del riesgo



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

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.
- **Causa raíz:** es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

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.

4.6.2. RIESGO DE CORRUPCIÓN Y DE LAVADO DE ACTIVOS Y FINANCIACION DEL TERRORISNO

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. “Esto implica que las prácticas corruptas son realizadas por actores públicos o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (CONPES N° 167 de 2013).

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así: ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Los riesgos de corrupción se establecen sobre procesos.

4.6.3. DESCRIPCION DEL RIESGO FISCAL

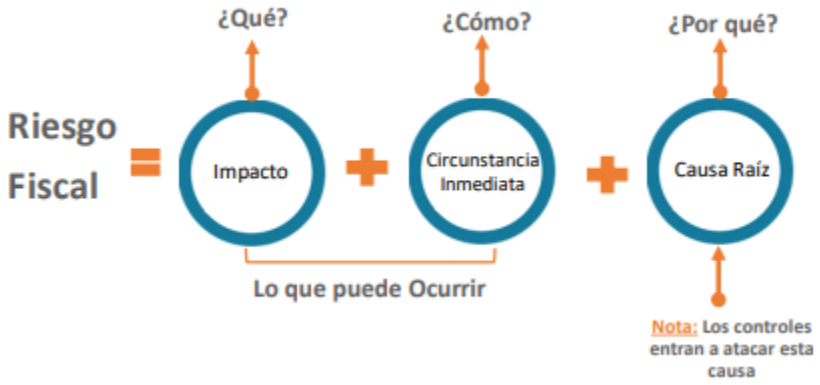
Para redactar un riesgo fiscal se debe tener en cuenta:

- 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 10 Estructura propuesta para la redacción de riesgos fiscales



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

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.

4.7. CLASIFICACIÓN DEL RIESGO

La Unidad adoptó los tipos de riesgos definidos en la Guía de administración de riesgos V6 - DAFP:

4.7.1. RIESGOS DE GESTION, DESASTRES, FISCALES Y CORRUPCIÓN

Ilustración 11 Clasificación de riesgos

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

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

Para la clasificación de los riesgos de desastres de la entidad, 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.

4.7.2. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para calificación de riesgos de seguridad de la información, sólo se podrán identificar los siguientes tres (3) riesgos:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones[10].

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 a la Guía de Riesgos del DAFP, a saber “Modelo nacional de gestión de riesgos de

[10] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

seguridad de la información para entidades públicas"[11] donde se encuentran las siguientes tablas necesarias para este análisis:

Tabla 5. Tabla de amenazas comunes

Tabla 6. Tabla de amenazas dirigida por el hombre

Tabla 7. Tabla de vulnerabilidades comunes

Igualmente, la UAESP cuenta con el manual GTI-MN-02 Clasificación de Activos de Información, en su Sistema Integrado de Gestión (SIG), y el procedimiento GTI-PC-04-Activos de información, donde se sintetizan los contenidos fundamentales de los anteriores documentos. Todas las áreas tienen que realizar la identificación y valoración de los activos de información y enviarlos a la OTIC, para que dicha área desarrolle los riesgos de seguridad en la matriz de riesgos.

Por otra parte, 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.

"Las variables de confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de la Tecnologías de Información y las Comunicaciones"

Ilustración 12 Amenazas y vulnerabilidades de acuerdo con el tipo de activo

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS

[11]https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba-00bc-58f801d3657b

Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

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

4.7.3. RIESGOS LAVADO DE ACTIVOS Y FINANCIACIÓN DE TERRORISMO

Dada la particularidad estos riesgos tendrá la clasificación independiente al fraude interno y externo quedando así:

- Lavado de activos
- Financiación de terrorismo

5. VALORACIÓN DEL RIESGO

La valoración del riesgo se realiza para establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto. Está integrada por el análisis del riesgo (con el fin de establecer la zona de riesgo inicial o inherente) y la evaluación del riesgo (con el fin de estimar la zona de riesgo final o residual, es decir aquel que subsiste después de aplicado un control).

5.1. ANÁLISIS DE RIESGOS

A continuación, se definen los lineamientos para determinar la probabilidad y nivel de impacto de los riesgos identificados, 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.

5.1.1. PROBABILIDAD

5.1.1.1. RIESGOS DE GESTIÓN, FISCALES, DESASATRES, SEGURIDAD DE LA INFORMACIÓN

Para estos riesgos 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 13 Criterios para Definir el Nivel de Probabilidad

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

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

5.1.1.2. RIESGOS DE CORRUPCIÓN Y LAVADO DE ACTIVOS Y FINANCIACIÓN DE TERRORISMO

En materia de riesgos de corrupción, cambia la escala para determinar su probabilidad, en relación a la metodología general.

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de **frecuencia** o **factibilidad**, donde **frecuencia** implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Para los riesgos de corrupción la probabilidad se calificará de acuerdo con la siguiente valoración:

Ilustración 14 Criterios para calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

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

5.1.2. 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.

5.1.2.1. RIESGOS DE GESTIÓN, FISCALES, DESASATRES, SEGURIDAD DE LA INFORMACIÓN

Ilustración 15 Criterios para Definir el Nivel de Impacto

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

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

5.1.2.2. RIESGOS DE CORRUPCIÓN Y LAVADO DE ACTIVOS Y FINANCIACIÓN DE TERRORISMO

El impacto en los riesgos de corrupción se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Para cada uno de los riesgos de corrupción identificados, se calificará el impacto de acuerdo con la siguiente tabla:

Ilustración 16 Criterios para Definir el Nivel de Impacto – Riesgos de Corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Nivel de impacto MAYOR

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

Nota: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico[12].

5.2. EVALUACIÓN DEL RIESGO

Busca afrontar los resultados del análisis del riesgo inicial o inherente, mediante la aplicación de controles, con el fin de determinar la zona de riesgo final (riesgo residual), y las acciones a tomar según el nivel de aceptación de riesgos de la entidad.

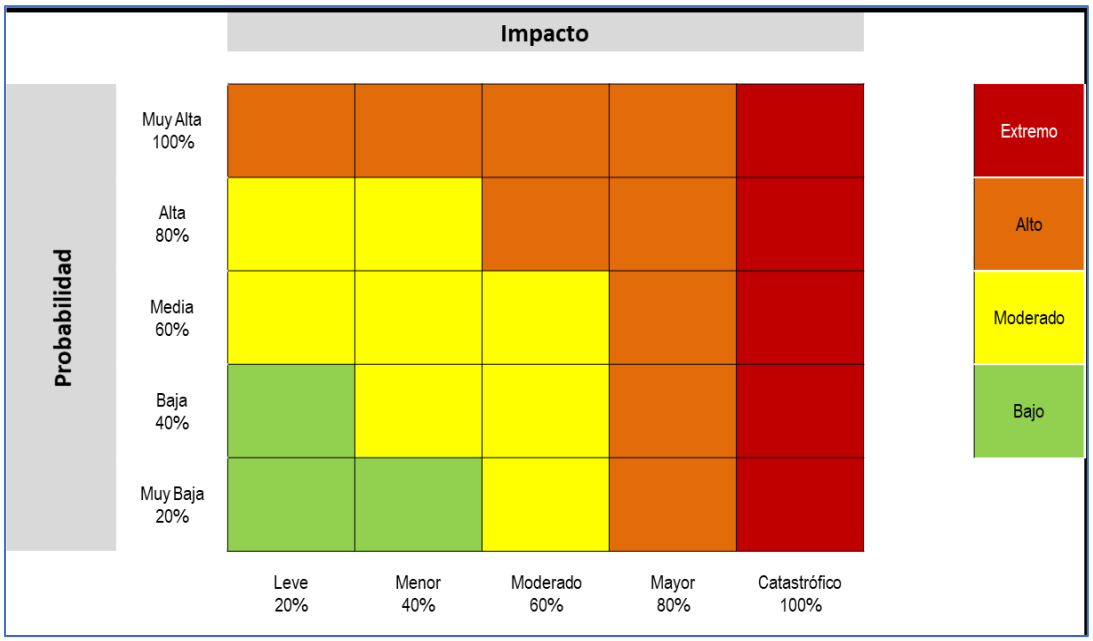
5.2.1. ANÁLISIS PRELIMINAR (RIESGO INHERENTE)

5.2.1.1. RIESGOS DE GESTIÓN, FISCALES, DESASATRES, SEGURIDAD DE LA INFORMACIÓN

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

[12] "En concordancia con los objetivos y enfoques desarrollados por la UNGRD, en Bogotá se establecen las siguientes prioridades de atención, como factor para la toma decisiones en la respuesta a emergencias, calamidades y desastres: 1. Proteger la vida, bienes y ambiente de la población, 2. Prestar los servicios básicos a la población, 3. Evitar mayores daños y pérdidas y 4. Mantener la gobernabilidad" según Prioridades y enfoque para el manejo de la EDRE V3, 2023.

Ilustración 17 Mapa de Calor de Riesgo de Gestión y Riesgos de Seguridad de la Información



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

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 contingencia[13] que defina las actividades de control (correctivas) que ataquen las causas del riesgo, cuando éste se llegue a materializar.

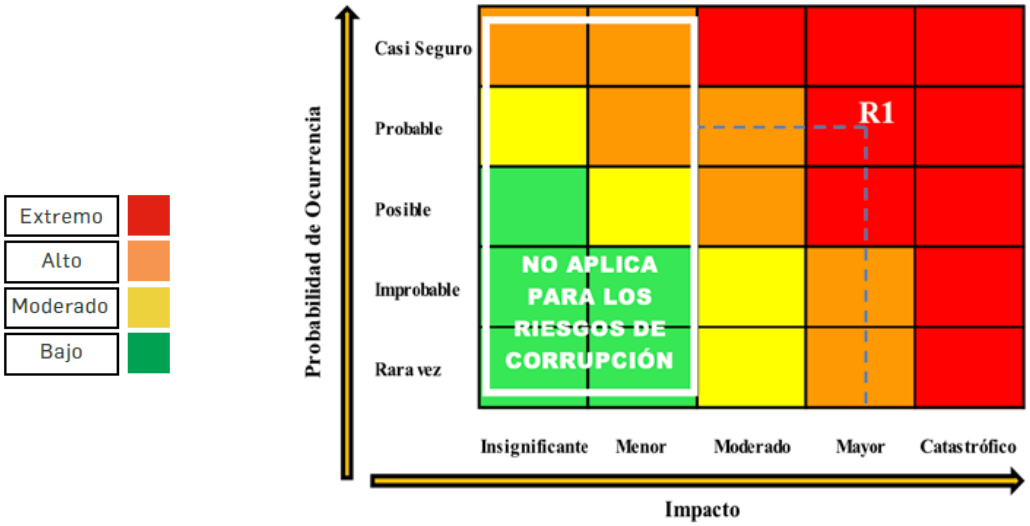
[13] Para la gestión de riesgos de desastres corresponde a los Planes de Emergencias y Contingencia- PEC

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

5.2.1.2. RIESGOS DE CORRUPCIÓN Y LAVADO DE ACTIVOS Y FINANCIACIÓN DE TERRORISMO

Para riesgos de corrupción, la valoración del impacto en el mapa de calor será el siguiente:

Ilustración 18 Mapa de Calor de Riesgo de Corrupción



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

Para los riesgos de corrupción y Lavado de Activos y Financiamiento del Terrorismo, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos. Esto se debe a que estos riesgos no admiten aceptación, es decir, el impacto de ningún riesgo de corrupción y Lavado de Activos y Financiamiento del Terrorismo, por su propia naturaleza, se considera

insignificante o menor. En otras palabras, en las entidades públicas colombianas el “apetito de riesgo”, en materia de riesgos de corrupción y Lavado de Activos y Financiamiento del Terrorismo, es nulo. Por lo tanto, las zonas del mapa de calor que corresponden a estos niveles de la escala de impactos no son utilizable para este tipo de riesgos. En esa medida los riesgos de corrupción siempre deben tener un tratamiento.

5.2.2. VALORACION 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.

5.2.2.1. RIESGOS DE GESTIÓN, FISCALES, DESASATRES, SEGURIDAD DE LA INFORMACIÓN

A. DISEÑO DE LOS CONTROLES

Para el diseño del control y valoración para este tipo de riesgos se tendrán en cuenta los siguientes parámetros

a. Propósito del control: En el desarrollo del diseño del control, un factor relevante para la suscripción del actuar del mismo consiste en su intencionalidad, la cual, debe estar asociada a acciones de verificación, validación, conciliación, comparación o revisión; que le permita prevenir o detectar la materialización del riesgo definido.
b. Periodicidad: Se debe describir de manera específica el ciclo con el cual se debe ejecutar el control definido, con el fin de gestionar el riesgo.
c. Formalización o descripción del control: Para formalizar el control, debe estar expresado de manera explícita en la documentación asociada al proceso en función de sus procedimientos, guías o manuales, etc. Igualmente, debe contener en su estructura los siguientes elementos:

- 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.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.
- Enunciar la evidencia, efecto de la ejecución del control.

d. Tipología de los controles: los controles pueden ser

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.

Según forma de ejecución:

- Manual: controles que son ejecutados por personas.
- Automático: son ejecutados por un sistema.

Nota. La definición de los controles ataca las causas identificadas en el marco de actuar del riesgo analizado. Los controles intervienen en generar efectos en la probabilidad de ocurrencia o del impacto, que pueda conllevar a la materialización de riesgo.

B. ANÁLISIS Y EVALUACIÓN DE LOS CONTROLES

De acuerdo con la Guía DAFP V6, el diseño del control tiene unos atributos teniendo en cuenta características relacionadas con la eficiencia y la formalización.

Ilustración 19 Atributos para el diseño del control

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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

Sobre un mismo riesgo puede haber diversos controles, y estos operan de manera acumulativa sobre el riesgo. 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.

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

De acuerdo con la Guía de Riesgos DAFP v.5 las entidades podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4 a la Guía de Riesgos DAFP v.5. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración. Se citan de la mencionada Guía, algunos ejemplos de controles y los dominios a los que pertenecen. La lista completa se encuentra en el documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Ilustración 20 Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

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

5.2.2.2. RIESGOS DE CORRUPCIÓN Y LAVADO DE ACTIVOS Y FINANCIACIÓN DE TERRORISMO

Para el diseño de controles, siguen vigentes los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes. Se presenta la siguiente síntesis:

1). Se establece el riesgo inherente, según lo señalado en el punto anterior.
2). Se definen causas o fallas que pueden dar origen a la materialización del riesgo
3). Se diseñan los controles y se evalúan para determinar si están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados, según las pautas que se señalan a continuación.
4). A partir de la anterior evaluación, se determina el riesgo después de controles (riesgo residual)

A. DISEÑO DE LOS CONTROLES

En la Guía de Riesgos del DAFP v.4 (2018), se establecen los siguientes pasos

Paso 1: Debe tener definido el responsable de llevar a cabo la actividad de control.

Paso 2: Debe tener una periodicidad definida para su ejecución.

Paso 3: Debe indicar cuál es el propósito del control.

Paso 4: Debe establecer el cómo se realiza la actividad de control.

Paso 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control

Paso 6: Debe dejar evidencia de la ejecución del control.

B. EVALUACIÓN DE CONTROLES

Lo anterior determina una serie de aspectos a evaluar en el diseño de controles con una ponderación específica señalada en la Guía:

La Guía de Riesgos del DAFP v.4 (2018), solo establece dos tipos de controles preventivos y detectivos.

Ilustración 21 Análisis y evaluación de los controles para la mitigación de los riesgos

Análisis y evaluación del diseño del control de acuerdo con las seis (6) variables establecidas:

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o detectar	No es un control
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	No confiable
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	No se investigan y resuelven oportunamente.
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta / no existe

Fuente: Guía administración del riesgo DAFP V4 (2018)

Ilustración 22 Peso o participación de cada variable en el diseño del control para la mitigación del riesgo

CRITERIO DE EVALUACIÓN.	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1.1 Asignación del responsable	Asignado	15
	No Asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

Fuente: Guía administración del riesgo DAFP V4 (2018)

Lo anterior conduce a una evaluación de los riesgos de corrupción en los siguientes términos:

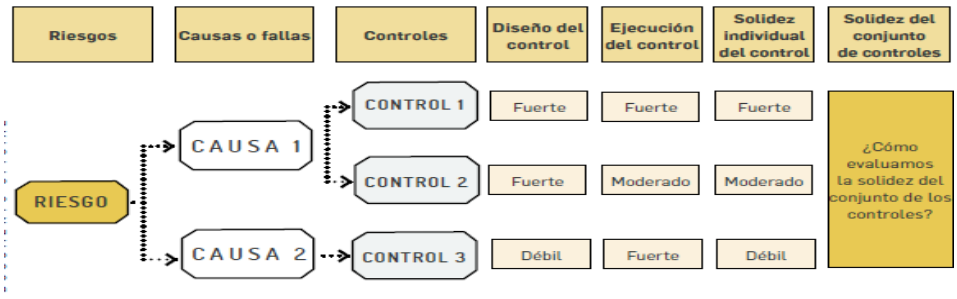
RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO - PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO - PESO DE LA EJECUCIÓN DEL CONTROL -
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Fuente: Guía administración del riesgo DAFP V4 (2018)

Cuando para el mismo riesgo se establecen varios controles (que atacan las diversas causas que generan el hecho configurador del riesgo), la evaluación de los controles debe hacerse de manera conjunta.

Ilustración 23 Solidez del conjunto de controles



IMPORTANTE
La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Fuente: Guía administración del riesgo DAFP V4 (2018)

Para ampliar la información sobre el diseño de controles y su evaluación, para el caso de los riesgos de corrupción, se debe consultar la Guía de riesgos del DAFP V.4 (2018).

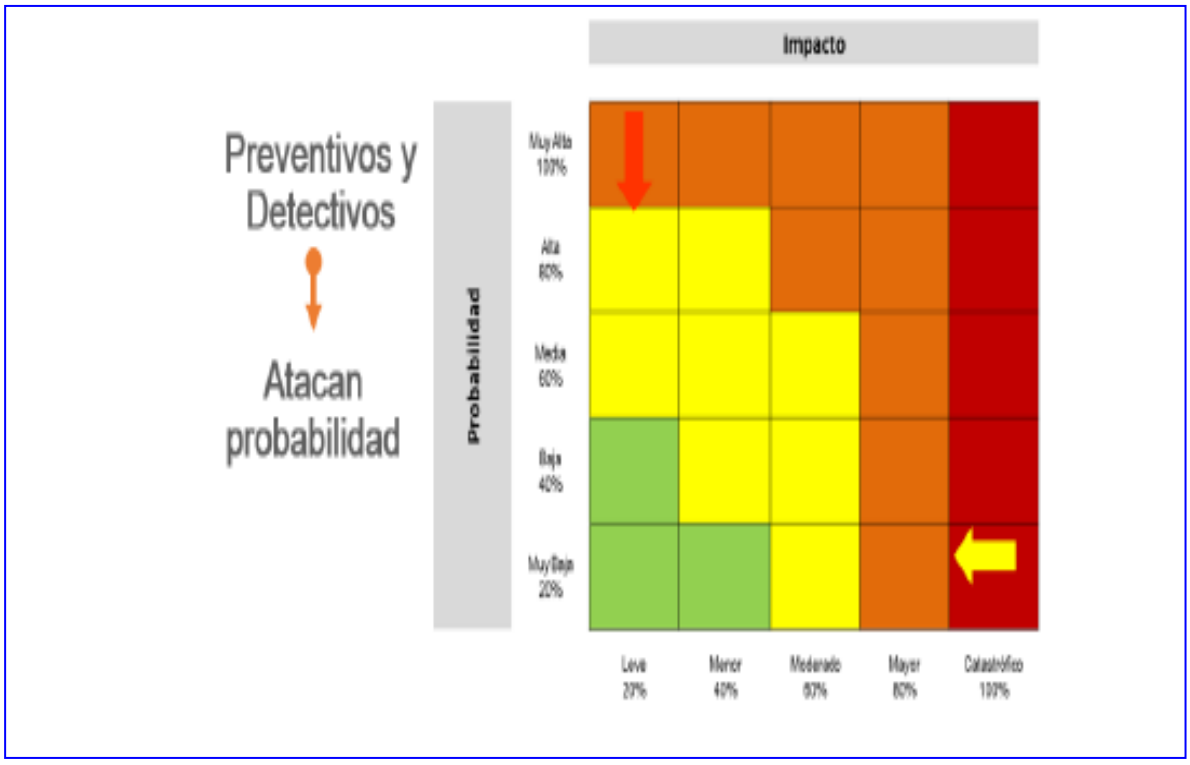
5.2.3. NIVEL DE RIESGO RESIDUAL

Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

5.2.3.1. RIESGOS DE GESTIÓN, FISCALES, DESASATRES, SEGURIDAD DE LA INFORMACIÓN

A partir de dicha aplicación se dará el movimiento en la matriz de calor tanto en el eje de probabilidad, como en el eje de impacto de acuerdo con los tipos de controles.

Ilustración 24 Movimiento en la matriz de calor acorde al tipo de control



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

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, 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.

Ilustración 25 Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
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 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	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 administración del riesgo y el diseño de controles en entidades públicas - Versión 6, DAFP - noviembre de 2022

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.

5.2.3.2. RIESGOS DE CORRUPCIÓN Y LAVADO DE ACTIVOS Y FINANCIACIÓN DE TERRORISMO

A partir de la anterior evaluación del control, y dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

Ilustración 26 Resultados de los posibles desplazamientos de la probabilidad del impacto de los riesgos

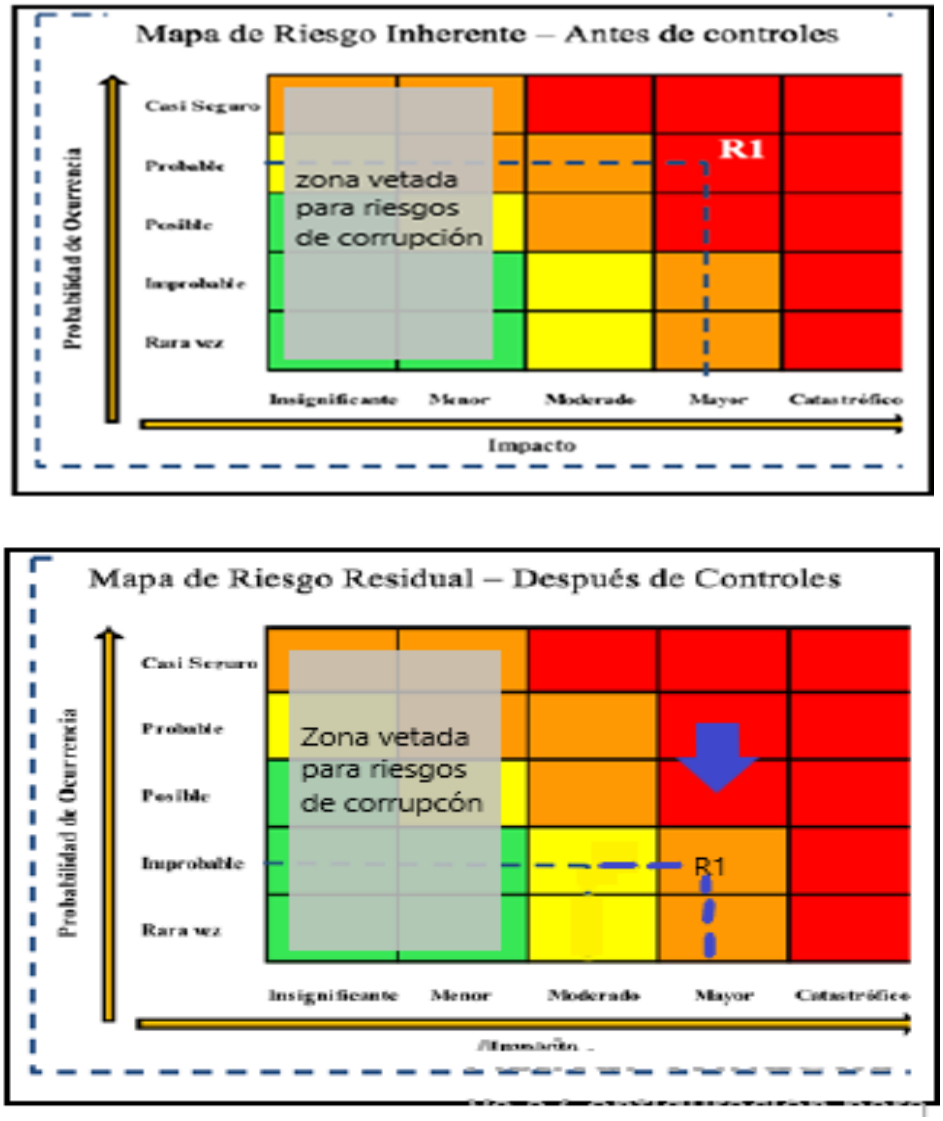
SOLIDEZ DEL CONJUNTO DE LOS CONTROLES.	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
fuerte	directamente	directamente	2	2
fuerte	directamente	indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	Indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

Fuente: Guía administración del riesgo DAFP V4 (2018)

Sin embargo, para efectos de los riesgos de corrupción la guía de riesgos del DAFP V.4 (2018), aclara que “Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento”. Esto significa que el desplazamiento solo podría darse en el eje vertical (probabilidad)

pero no en el horizontal (impacto). Por otra parte, debe recordarse que, en materia de riesgos de corrupción y Lavado de Activos y Financiación de Terrorismo, los impactos no se pueden considerar insignificantes o menores, por lo que el desplazamiento sólo puede darse en una zona de severidad del riesgo moderado, alto o extrema.

Ilustración 27 Desplazamientos en el mapa de calor



Fuente: Elaboración propia a partir de la figura expuesta en la Guía administración del riesgo DAFP V4 (2018), p -67

6. HERRAMIENTAS PARA LA MITIGACION DEL RIESGO

Las etapas de la anterior metodología se llevarán de manera secuencial en el formato DES-FM-12 Mapa y plan de manejo de riesgos y oportunidades de la UAESP.

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 V6, además del mapa de riesgos, las 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)

Así mismo la entidad puede acudir a la herramienta “mapas de aseguramiento”[14]. 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.

7. 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

[14] Circular 103 de 2020 de la Secretaría General de Bogotá.

análisis de contexto, riesgos y controles como resultado de los ejercicios de autocontrol, autoevaluación, evaluación independiente o por decisión del CICCI 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 se recomienda tener en cuenta lo siguiente:

Ilustración 28 Ambiente de control en LA/FT

Fuente: Documento Técnico Lavado de Activos y Financiación del Terrorismo

8. 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 de corrupción se deberá informar a la Alta Dirección sobre el hecho encontrado. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.

- Si el riesgo es de gestión, desastre[15], 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 de Lavado de Activos y Financiación del terrorismo 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.

b. Materialización de riesgos detectada por la Oficina Asesora de Planeación (segunda línea de defensa):

- En los casos de riesgos de corrupción detectado por la segunda Línea de defensa, se debe informar sobre el hecho encontrado a la Oficina de Control 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.
- En los casos de riesgo de Lavado de Activos y Financiación del terrorismo 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, de igual manera deberá denunciarse a través del reporte de operaciones inusuales (interno) y reporte de operaciones

[15] 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

sospechosas que deben ser reportadas a la UIAF (Unidad de Información y Análisis Financiero.

- En los casos de riesgos de gestión desastre[16], 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 de corrupción, 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 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 de Lavado de Activos y Financiación del terrorismo detectado por la tercera 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, de igual manera deberá denunciarse a través del reporte de operaciones inusuales (interno) y reporte de operaciones

[16] Idem

sospechosas que deben ser reportadas a la UIAF (Unidad de Información y Análisis Financiero.

- Si el riesgo es de gestión, desastre[17], 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.

9. 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.

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

[17] Idem

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.

10. 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 documento Técnico la debida diligencia hace parte de los elementos para gestionar la prevención del Lavado de Activos y Financiación del Terrorismo. Así las cosas, en cumplimiento de las acciones orientadas a detectar y control estos riesgos se encuentran las siguientes actividades:

- **Adoptar un lineamiento interno:** La entidad deberá establecer una directriz que oriente sobre cómo se enfoca la prevención y mitigación de los riesgos LA/FT en su interior. Esta directriz podría estar integrada con las directrices anticorrupción o de forma independiente, a través de un documento sencillo.

- **Definir y adoptar un protocolo de consulta a listas:** La consulta a listas restrictivas y vinculantes se constituye en una actividad determinante que

contribuye al despliegue operativo del ejercicio de debida diligencia, y que garantiza certezas en materia de revisión e identificación de la contraparte. Se recomienda como mínimo que la entidad incorpore esquemas de consulta automatizados o con intervención de usuario (manualmente), que garanticen una revisión de las siguientes bases de datos:

- Lista vinculante consolidada del Consejo de Seguridad de las Naciones Unidas.
- Lista restrictiva OFAC que incluye nombres de personas y empresas señaladas de participar en actividades de lavado de activos.
- Listas propias de conocimiento de la entidad.

10.1. REVISION Y DETECCION DE OPERACIONES SOSPECHOSAS DE LA/FT

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/FPADM 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.

10.2. POLITICAS DE MIPG RELACIONADAS DIRECTAMENTE CON LA PREVENCION DE LA/FT

POLITICA MIPG	ARTICULACION LA/FT
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.
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

POLITICA MIPG	ARTICULACION LA/FT
	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, 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 Plan Anticorrupción y de Atención a la Ciudanía (PAAC).
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

POLITICA MIPG	ARTICULACION LA/FT
	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,

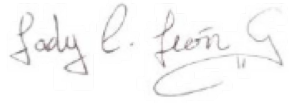
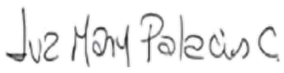
POLITICA MIPG	ARTICULACION LA/FT
	manuales, procedimientos y controles, entre otros, para la implementación del SARLAFT.
Política de Seguimiento y Evaluación del desempeño institucional	Esta política genera lineamientos para que la entidad realice seguimiento y evaluación a su gestión y desempeño, monitoreando 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.
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:

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.
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.

Versión	Fecha	Descripción de la modificación
05	19/09/2023	Se realiza el ajuste de la estructura de la política conforme a lo establecido en la versión 5 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.

AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	Lady Carolina León	Profesional Universitario Oficina Asesora de Planeación	
Revisó	Luz Mary Palacios Castillo	Profesional Universitario Oficina Asesora de Planeación	
Aprobó	Yesly Alexandra Roa Mendoza	Jefe Oficina Asesora de Planeación	Alexandra Roa Mendoza Firmado digitalmente por Alexandra Roa Mendoza Fecha: 2023.09.19 17:48:10 -05'00'
Revisó y Aprobó	Comité Institucional de Coordinación de Control Interno		Acta No 9 del CIGD del 19/09/2023

ALCALDÍA MAYOR
DE BOGOTÁ D.C.

UAESP
Unidad Administrativa Especial
de Servicios Públicos

BOGOTÁ