POLITICA DE ADMINISTRACIÓN DEL RIESGO

Unidad Administrativa

Especial de Servicios Públicos

Diciembre 29 de 2021

ALCALDÍA MAYOR DE BOGOTÁ D.C.

UAESP Unidad Administrativa Especial de Servicios Públicos

BOGOTÁ

TABLA DE CONTENIDO

INTRODUCCIÓN 5

1. MARCO NORMATIVO 6
2. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO. 7
3. OBJETIVO 8
3.1 OBJETIVOS ESPECÍFICOS 8
4. ALCANCE 9
5. TÉRMINOS Y DEFINICIONES 9
6. ROLES Y NIVELES DE RESPONSABILIDAD FRENTE AL RIESGO. 12
6.1 LÍNEA ESTRATÉGICA. 13
6.2 PRIMERA LÍNEA DE DEFENSA. 13
6.3 SEGUNDA LÍNEA DE DEFENSA. 14
6.4 TERCERA LÍNEA DE DEFENSA. 16
7. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO 17
7.1 METODOLOGÍA A UTILIZAR. 17
7.2. IDENTIFICACIÓN DEL RIESGO. 17
7.2.1 Análisis de Objetivos Estratégicos y de los Procesos, para identificación de los riesgos 17
7.2.2 Establecimiento del Contexto - Factores Internos y Externos. 17
7.2.3 Identificación de los Puntos de Riesgo 18
7.2.4 Identificación de áreas de factores de riesgo. 19
7.2.5 Identificación Áreas de Impacto 20
7.2.6 Descripción de Riesgos. 20
7.2.7 Clasificación del Riesgo 21
7.3 VALORACIÓN DEL RIESGO 23
7.3.1 Análisis de Riesgos 23
7.3.2 Evaluación del riesgo. 27
7.3.2.1 Formulación de controles. 27
7.3.2.2 Análisis y evaluación de los controles: 30
7.3.2.3 Nivel de riesgo residual: 32
7.3.2.4 Nivel de aceptación del riesgo y estrategias para afrontar el riesgo 35
7.3.2.4.1 Marco conceptual para determinar los niveles de Aceptación del riesgo en la UAESP. 35
7.3.2.4.2 ESTRATEGIA PARA COMBATIR EL RIESGO (tratamiento del riesgo) 37
7.3.2.4.3 Niveles de aceptación del riesgo en la UAESP. 40
7.3.3 Mapa de riesgos. 40
7.4 OTRAS HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO. 41
7.5 PERIODICIDAD PARA EL SEGUIMIENTO. 41
8. RIESGOS MATERIALIZADOS 42
9. DIVULGACIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS 43
10. LINEAMIENTOS PARA RIESGOS DE SEGURIDAD DE LA INFORMACION 44

10.1. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN 41
10. 2 IDENTIFICACIÓN DEL RIESGO. 45
10.3 VALORACIÓN DEL RIESGO 47
10.3.1 Análisis del riesgo: probabilidad e impacto. 47
10.3.2 Evaluación del riesgo y Controles asociados a la seguridad de la información. 47
10.3.3. Mapa de riesgos de seguridad de la información. 49
11. LINEAMIENTOS RIESGOS DE CORRUPCIÓN 50
11.1 GENERALIDADES ACERCA DE LOS RIESGOS DE CORRUPCIÓN 50
11.2 IDENTIFICACIÓN DEL RIESGO. TÉCNICAS PARA SU IDENTIFICACIÓN. 51
11.3 VALORACIÓN DE LOS RIESGOS 52
11.3.1 Cálculo de la probabilidad e impacto 52
11.4 VALORACIÓN DEL RIESGO DE CORRUPCIÓN. 54
11.4.1. Establecimiento de controles para el riesgo inherente 55
11.4.2 Determinación del riesgo de corrupción residual. 59
11.5 TRATAMIENTO DE RIESGOS DE CORRUPCIÓN 63
11.6 Matriz (mapa) de riesgos de corrupción 63
11.7 MONITOREO Y REVISIÓN. 64
11.8 ACCIONES EN CASO DE MATERIALIZACIÓN DEL RIESGO 65

INDICE DE TABLAS

Tabla 1. Factores por Categoría del Contexto 18
Tabla 2. Factores de riesgo 19
Tabla 3. Clasificación de riesgos 22
Tabla 4. Criterios para Definir el Nivel de Probabilidad 23
Tabla 5. Criterios para Definir el Nivel de Impacto 24
Tabla 6. Atributos para el diseño del control 31
Tabla 7. Aplicación de controles para establecer el riesgo residual 33
Tabla 8. Niveles de Aceptación del Riesgo 40
Tabla 9. Amenazas y vulnerabilidades de acuerdo con el tipo de activo. 46
Tabla 10. Controles para riesgos de seguridad de la información 48
Tabla 11. Criterios para Definir el Nivel de Impacto – Riesgos de Corrupción 53
Tabla 12. Valoración – Riesgos de Corrupción 54
Tabla 13. Análisis y evaluación de los controles para la mitigación de los riesgos 56
Tabla 14. Peso o participación de cada variable en el diseño del control para la mitigación del riesgo 57
Tabla 15. Resultados de los posibles desplazamientos de la probabilidad del impacto de los riesgos 60

INDICE DE FIGURAS

Figura 1. Mapa de Calor de Riesgo de Gestión y Riesgos de Seguridad de la Información…25
Figura 2. Mapa de calor, ejemplo ……26
Figura 3. Mapa de calor, ejemplo ……27
Figura 4. Controles en los riesgos de gestión……..29
Figura 5. Redacción de controles en riesgos de gestión……29
Figura 6. Redacción de controles en riesgos de gestión……....30
Figura 7. Controles en riesgos de gestión……32
Figura 8. Valoración de controles de riesgos de gestión……34
Figura 9. Valoración de controles de riesgos de gestión 2……34
Figura 10. Ejemplo, riesgo residual……..……35
Figura 11. Definiciones de apetito, tolerancia y capacidad de riesgo ……..…..36
Figura 12. Estrategia para combatir el riesgo……...……38
Figura 13. Ejemplo matriz plan de manejo……39
Figura 14. Pasos para la identificación de activos……..…45
Figura 15. Formato de descripción del riesgo de seguridad de la información……..…47
Figura 16. Formato mapa riesgos seguridad de la información……....49
Figura 17. Ejemplo, información anonimizada……51
Figura 18. Conceptualización activos de información……52
Figura 19. Evaluación de los riesgos de corrupción……..…58
Figura 20. Solidez del conjunto de controles……59
Figura 21. Mapa de riesgo inherente, antes de controles……..……62
Figura 22. Mapa de riesgo inherente, después de controles……..…62
Figura 23. Formato mapa y plan de tratamiento de riesgos……..…63

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 5, en diciembre de 2020[1], Igualmente busca el cumplimiento del requisito de la norma ISO 9001:2015, numeral 6.1, abordaje de riesgos y oportunidades[2].

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, corrupción y seguridad de la información en la estructura de procesos de la UAESP. Se debe tener en cuenta que, frente a los riesgos de seguridad de la información, la guía tiene algunas líneas específicas, que son reseñados en el acápite 10 de este documento. Respecto a los riesgos de corrupción, se siguen teniendo en cuenta los lineamientos de la guía DAFP Versión 4, según lo indica la misma entidad en su guía V.5, y también son reseñados en el acápite 11 de este documento.

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 de riesgos, 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 4, Marzo de 2021), así como a su concreción dentro de la UAESP, a través de la Resolución 313 de 2020 (modificada por loa Resolución 571 de 2021), buscando reglamentar el alcance del Sistema de Gestión y su articulación con el Sistema de Control Interno, de tal

[1] https://www.funcionpublica.gov.co/documents/28587410/34298398/2020-12-16_Guia_administracion_riesgos_dise%C3%B1o_controles_final.pdf/fa179c5e-45bb-dffd-027c-043d4733c834?t=1609857497641.

[2] La UAESP aborda la planeación de Oportunidades a través del documento Política para la Gestión de las Oportunidades.

CO16/7252

manera que permita el aseguramiento de los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades del Estado.

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 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.

- **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 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 5 (diciembre de 2020).

- **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.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO.

La Unidad Administrativa Especial de Servicios Públicos - UAESP, se compromete a identificar, gestionar y evaluar los riesgos de Gestión, Corrupción y Seguridad de la información 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, la identificación, análisis, evaluación, monitoreo, revisión y seguimiento de los riesgos e implementación de acciones de control para su mitigación y planes de contingencia ante la 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 y tratamiento de estos.
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 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.

OBJETIVO

Definir los parámetros de la administración del riesgo de la Unidad a través del establecimiento de mecanismos y herramientas que permitan la identificación, tratamiento, manejo y seguimiento de los riesgos, con el fin de evitar su materialización, con el propósito de controlar los eventos que afecten los objetivos estratégicos de la entidad gestionándolos en un nivel aceptable.

3.1 OBJETIVOS 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, corrupción y seguridad de la información, 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 conciencia y cultura de los colaboradores de la Entidad alrededor de la gestión de los riesgos, con el fin de prevenir, detectar desviaciones y 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.

ALCANCE

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

Los riesgos de gestión 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, de acuerdo señalados en Guía DAFP v.5, pg. 75.

Los riesgos de corrupción se tratarán de acuerdo con los lineamientos señalados en el acápite 11 (, los cuales responden a los señalados en la guía DAFP Versión 4, según lo indica la misma entidad en su guía V.5).

TÉRMINOS Y DEFINICIONES[3]

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.

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.

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

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

CO16/7252

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.

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.

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.

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.

Control de riesgos: La parte de administración de riesgos que involucra la implementación de políticas, estándares, procedimientos para eliminar o minimizar los riesgos adversos.

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

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

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

Integridad: Propiedad de exactitud y completitud.

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.

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.

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: Representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.

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

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

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.

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.

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

6. ROLES Y NIVELES DE RESPONSABILIDAD FRENTE AL RIESGO.

A continuación, se relacionan los niveles de responsabilidad y autoridad establecidos para la administración del riesgo determinados por líneas de defensa, teniendo en cuenta lo establecido en el Manual operativo MIPG V4 y la guía de administración del riesgo de la Función pública V5. 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[4].

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[5].

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

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

6.1 LÍNEA ESTRATÉGICA.

Los responsables de esta línea son la Alta dirección, y las responsabilidades de esta línea son las siguientes:

- Aprobar la Política de Administración del Riesgo como estrategia que apunte al cumplimiento de los planes de la entidad la cual incluye los niveles de responsabilidad y autoridad.
- Definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento.
- Definir y hacer seguimiento a los niveles de aceptabilidad del riesgo.
- 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.
- 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.
- 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.
- Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones para su fortalecimiento.
- Definir los procesos, programas o proyectos susceptibles de posibles actos de corrupción acorde con el análisis del entorno interno y externo.
- 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

6.2 PRIMERA LÍNEA DE DEFENSA.

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

- Monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos incluyendo los indicadores de desempeño, a fin de establecer los posibles riesgos que se están materializando y propiciar una adecuada gestión de riesgos.
- Identificar, analizar. valorar y monitorear los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo, alineados con las metas y objetivos de la entidad, incluyendo los riesgos de corrupción, y actualizarlos cuando se requiera, así como la matriz de riesgos de su proceso
- Identificar los riesgos de servicios o actividades tercerizados, cuando aplique.
- Revisar como parte de los procedimientos de supervisión, el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos
- Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados, acciones de mejora, 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 de riesgos y el plan de manejo de riesgos, 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 informarlos 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.

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 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 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, incluyendo los riesgos de corrupción, 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 de riesgos y presentarlo para evaluación ante el Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno CICCI, para su posterior socialización y publicación en la página web.
- Monitorear trimestralmente los riesgos identificados 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 del proceso realizado por la primera línea de defensa

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 y definición de controles, relacionados con los temas a su cargo.
- Monitorear los riesgos identificados y los controles establecidos por la primera línea de defensa relacionados con los temas a su cargo

6.4 TERCERA LÍNEA DE DEFENSA.

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

- Asesorar a la UAESP acerca de las metodologías, herramientas y técnicas para la identificación y administración de los riesgos 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 en los trabajos de auditoría interna.
- Revisar 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 que se evalúen y actualicen la política de administración del riesgo, la identificación de los riesgos 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 realizar las recomendaciones a que haya lugar.
- Llevar a cabo la evaluación independiente de la gestión de los riesgos 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 a 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.

7. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

7.1 METODOLOGÍA A UTILIZAR.

La metodología corresponde a la establecida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 de diciembre de 2020 del DAFP, concretada en las etapas señaladas en el presente documento.

Se plantean algunos lineamientos específicos para los riesgos de seguridad de la información, reseñados en el acápite 10 de este documento (acogiendo lo establecido en la anterior guía en el capítulo 5, págs. 75 y ss.).

Los riesgos de corrupción se tratarán de acuerdo con los lineamientos señalados en el acápite 11 (los cuales responden a los señalados en la guía DAFP Versión 4, según lo indica la misma entidad en su guía V.5).

Las etapas de esta metodología se llevarán de manera secuencial en el formato DES-FM-12 V10 Mapa y plan de manejo de riesgos de la UAESP, el cual acoge el modelo propuesto por el DAFP en la Guía para la gestión del riesgo Versión 5 (pág. 52 a 56). y aplicando el procedimiento: “DES-FM-16 V4, Administración del riesgo”

7.2. IDENTIFICACIÓN DEL RIESGO.

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 ISO 31000, Numeral 2.15).

7.2.1 Análisis de Objetivos Estratégicos y de los Procesos, para identificación de los riesgos.

Los riesgos identificados 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 concretarse en los objetivos de los procesos (ver lineamientos en la Guía de Administración del Riesgo DAFP, v5, pág. 28).

7.2.2 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:

Tabla 1. Factores por Categoría del Contexto.

,x	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.
	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.
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.

Fuente: Tomado de la Guía de Administración del Riesgo del DAFP, 2018.

7.2.3 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, corrupción 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 pública, desde insumos, procesos, productos, resultados, efectos e impactos y el cumplimiento de los objetivos (eficacia y eficiencia).

7.2.4 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 V.5, señala a manera de ejemplo, las siguientes:

Tabla 2, 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
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5 - diciembre de 2020.

7.2.5 Identificación Áreas de Impacto

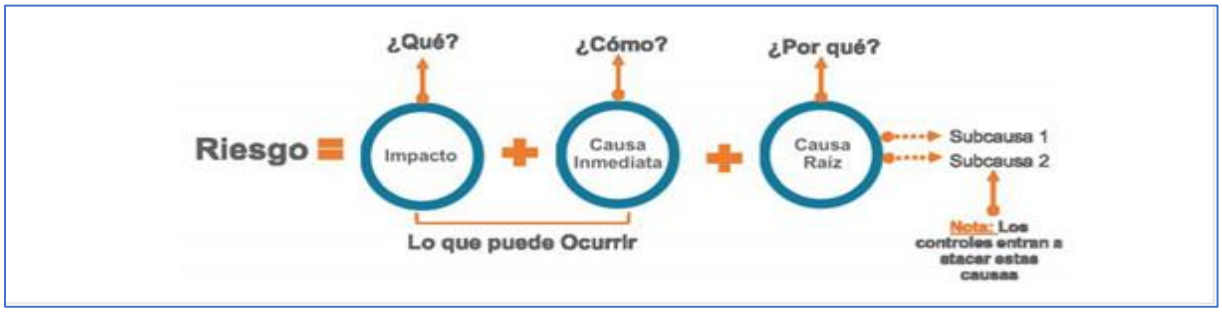
El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la Entidad en caso de materializarse un riesgo (estos conceptos se desarrollan en el numeral 7.3.1, literal b).

7.2.6 Descripción de Riesgos

La identificación del riesgo de gestión 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.

Premisas para una adecuada redacción del riesgo.

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



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020, p. 32 (Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020).

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.

(Ver ejemplos de aplicación en la Guía para la Administración del Riesgo DAFP, v5, pág. 34)

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: Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

7.2.7 Clasificación del Riesgo

La Unidad adaptó los tipos de riesgos definidos en el numeral 2.6 de la Guía de administración de riesgos V5 - DAFP, ubicados en las páginas 34 y 35 de la citada guía:

Tabla 3. 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.3 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).

7.3.1 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-V10 Mapa y plan de manejo de riesgos de la UAESP, en el cual se tienen formulados y especificados estos criterios.

a. **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.

Tabla 4. Criterios para Definir el Nivel de Probabilidad.

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020

b. 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.

Tabla 5. Criterios para Definir el Nivel de Impacto.

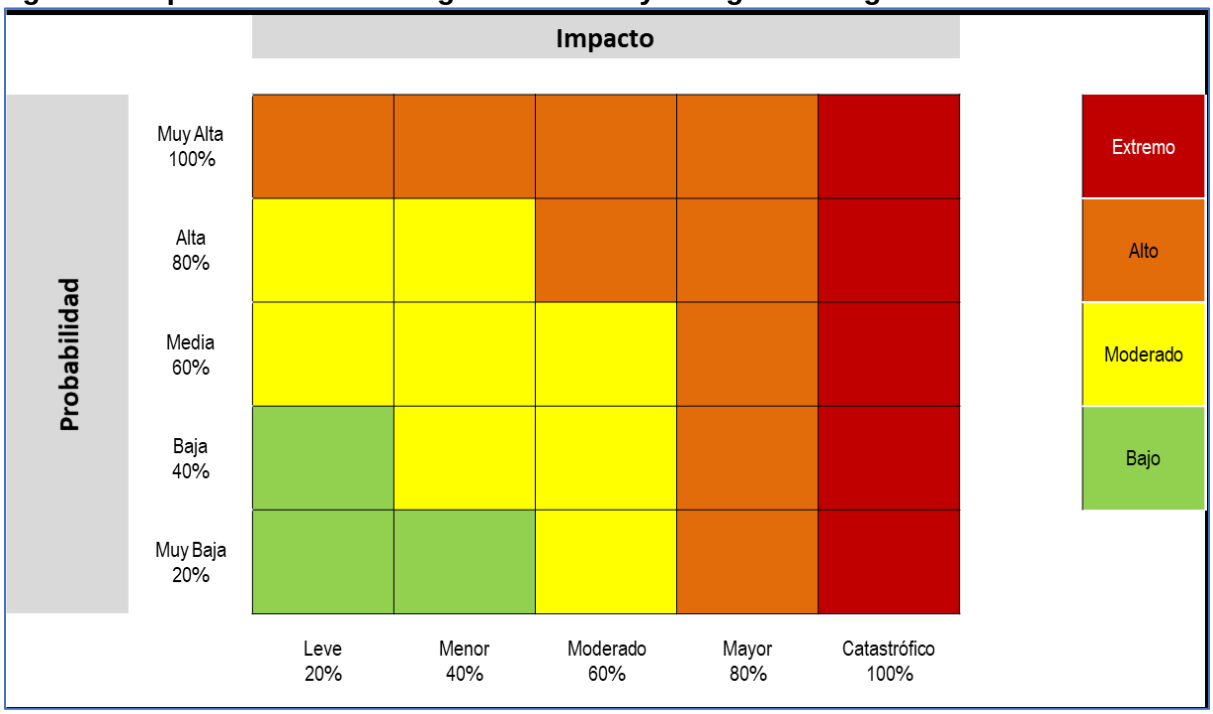
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020.

c. Definición de Nivel del Riesgo (riesgo inherente)

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:

Figura 1. 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 5 - diciembre de 2020

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.

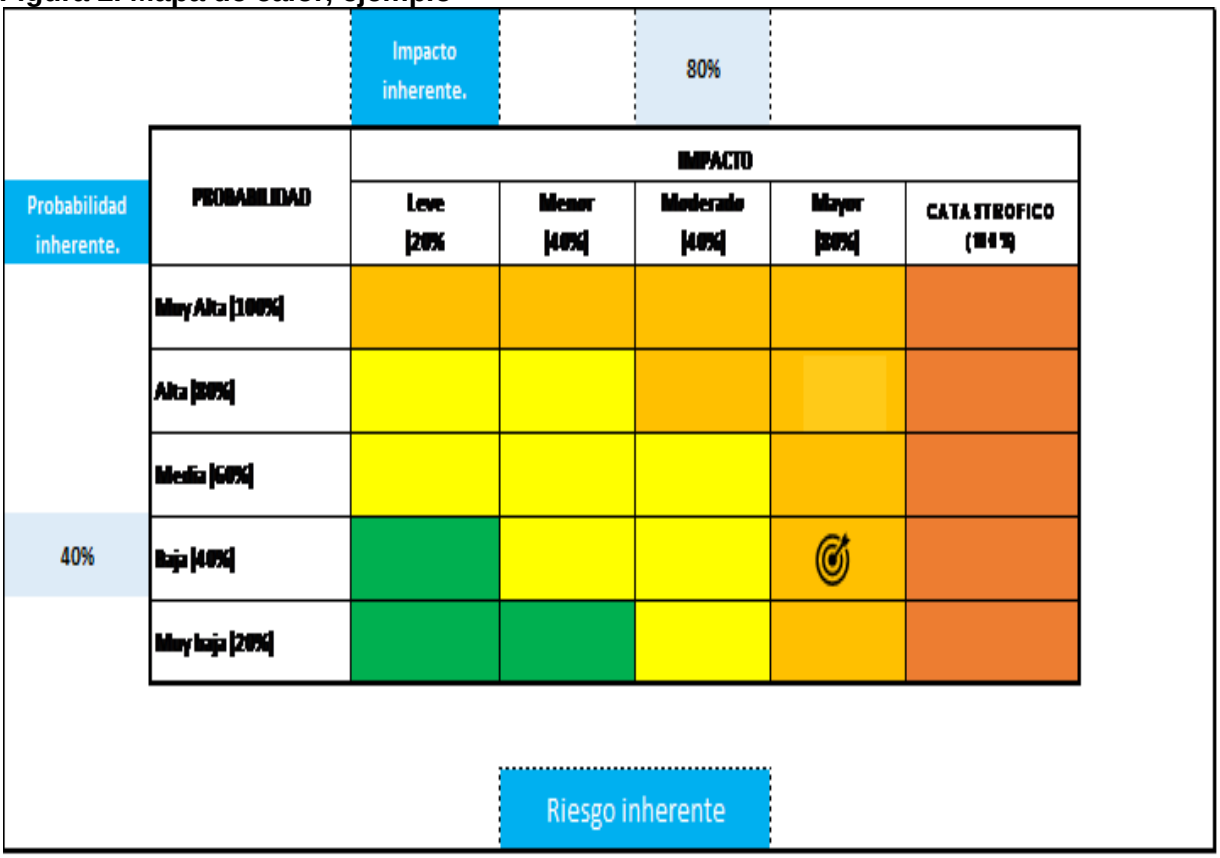
Esta matriz de 5 x 5, traza en su eje X el impacto y en su eje Y la probabilidad de ocurrencia.

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

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

Para un riesgo con una probabilidad del 40% y un impacto del 80%, su ubicación en el mapa de calor sería así:

Figura 2. Mapa de calor, ejemplo

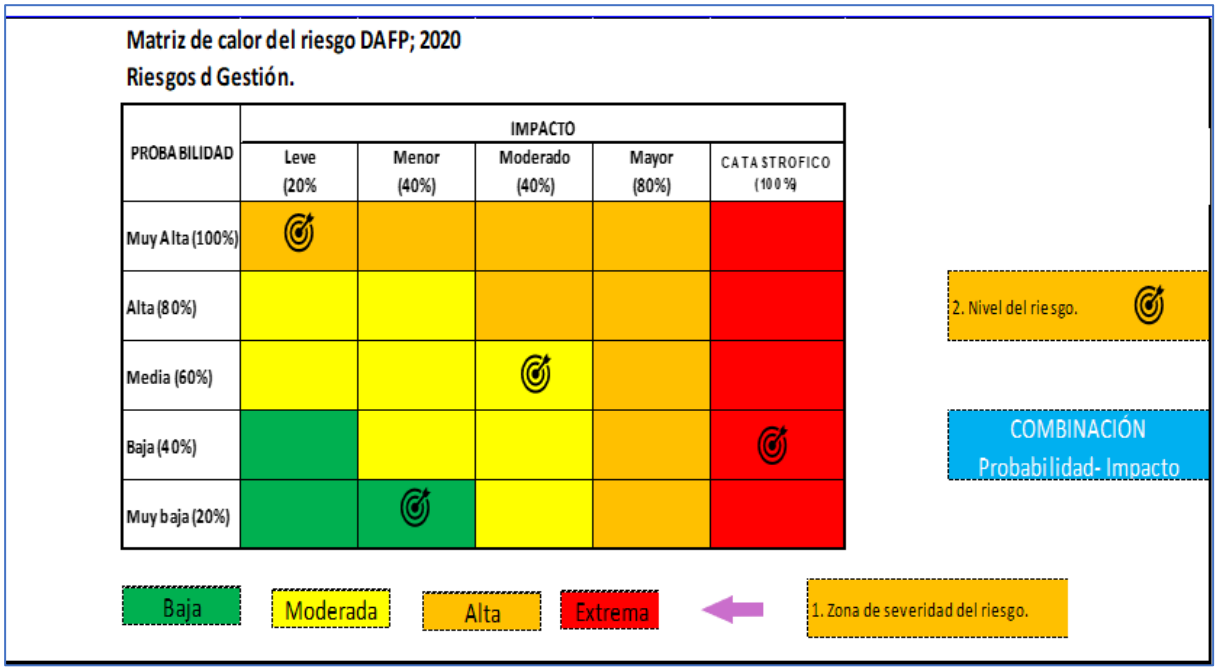


Fuente: elaboración propia a partir de la gráfica expuesta en la Capacitación: Gestión del Riesgo: análisis y evaluación, Secretaría General de Bogotá, julio 16 de 2021.

Los distintos riegos de una entidad pueden tener diferente ubicación en el mapa de calor (ubicación que se denomina nivel de severidad del riesgo), según la combinación de probabilidad e impacto (lo que se denomina nivel del riesgo):

Figura 3. Mapa de calor, ejemplo.

.



Fuente: elaboración propia a partir de la gráfica expuesta en la Capacitación: Gestión del Riesgo: análisis y evaluación, Secretaría General de Bogotá, julio 16 de 2021.

7.3.2 Evaluación del riesgo.

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

7.3.2.1 Formulación 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.

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 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.

(Ver ejemplo: Guía de la Administración de Riesgos y el diseño de controles en entidades públicas, DAFP, v5, pág. 43 y 44)

d. Integración de controles: El diseño de un control puede atacar causas asociadas a riesgos de gestión, corrupción y seguridad de la información.

e. 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:

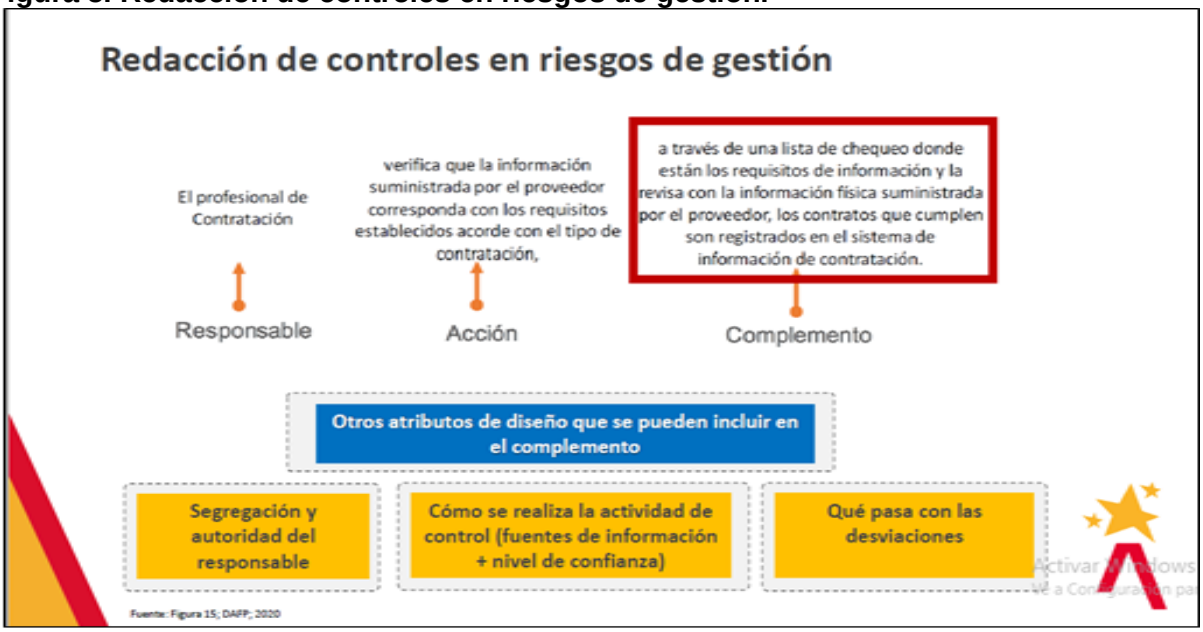
- Manual: controles que son ejecutados por personas.
- Automático: son ejecutados por un sistema.

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.

Figura 4. Controles en los riesgos de gestión.

Fuente: Capacitación Secretaría Genera, 16 de julio de 2021

Figura 5. Redacción de controles en riesgos de gestión.



Fuente: Capacitación Secretaría Genera, 16 de julio de 2021

CO16/7252

Figura 6. Redacción de controles en riesgos de gestión.

Fuente: Capacitación: Gestión del Riesgo: análisis y evaluación, Secretaría General de Bogotá, julio 16 de 2021.

7.3.2.2 Análisis y evaluación de los controles:

De acuerdo con la Guía DAFP v5, el diseño del control tiene unos atributos teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 6 de la Guía se puede observar la descripción y peso asociados a cada uno así:

Tabla 6 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.	25%
*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.	-

Tabla 6 Atributos para el diseño del control

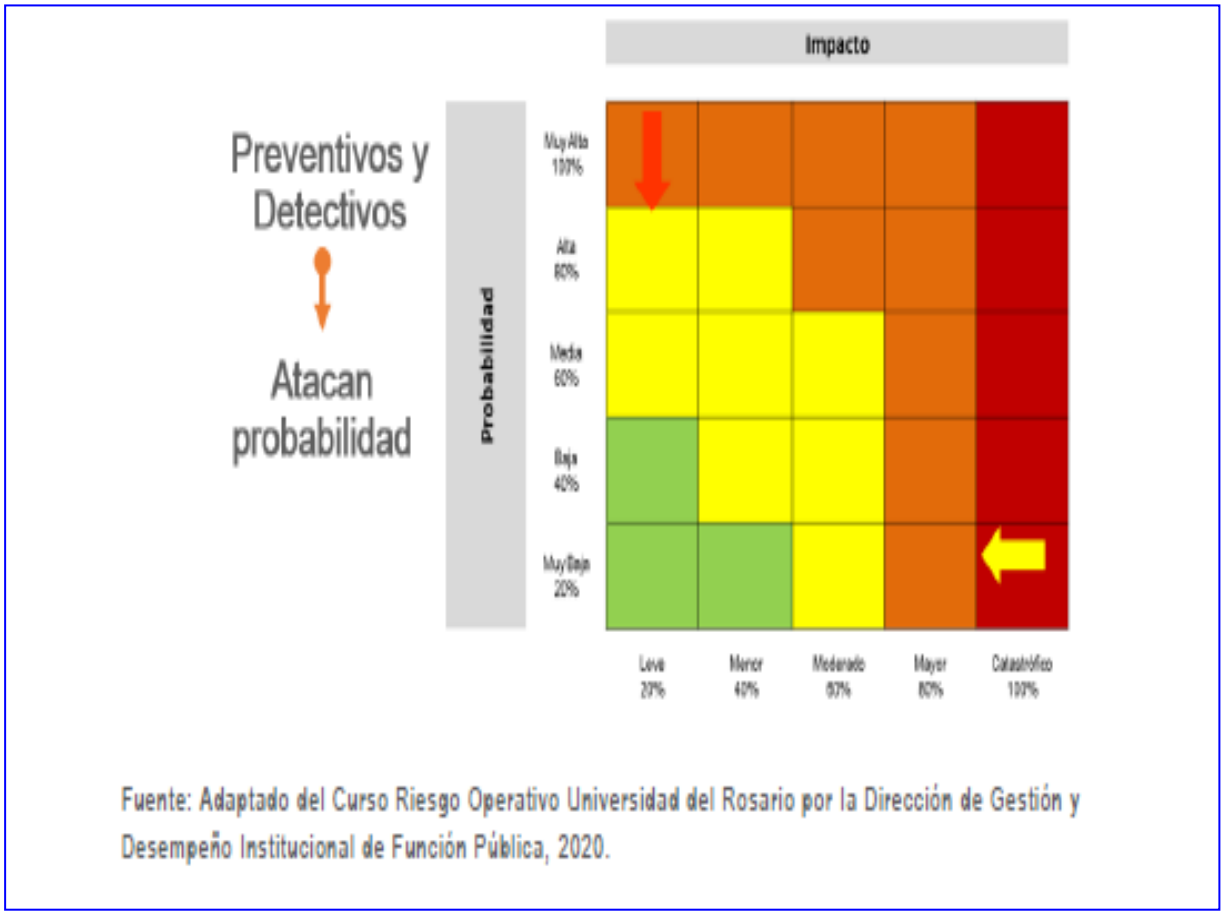
Sobre un mismo riesgo puede haber diversos controles, y estos operan de manera acumulativa sobre el riesgo. La sumatoria de los controles no podría dar 100%, ya que eso significaría que se ha eliminado el riesgo, lo cual no ocurre en realidad.

7.3.2.3 Nivel de riesgo residual:

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

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.

Figura 7. Controles en riesgos de gestión.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP - diciembre de 2020

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.

Para mayor claridad, ver ejemplo guía DAFP, p49.

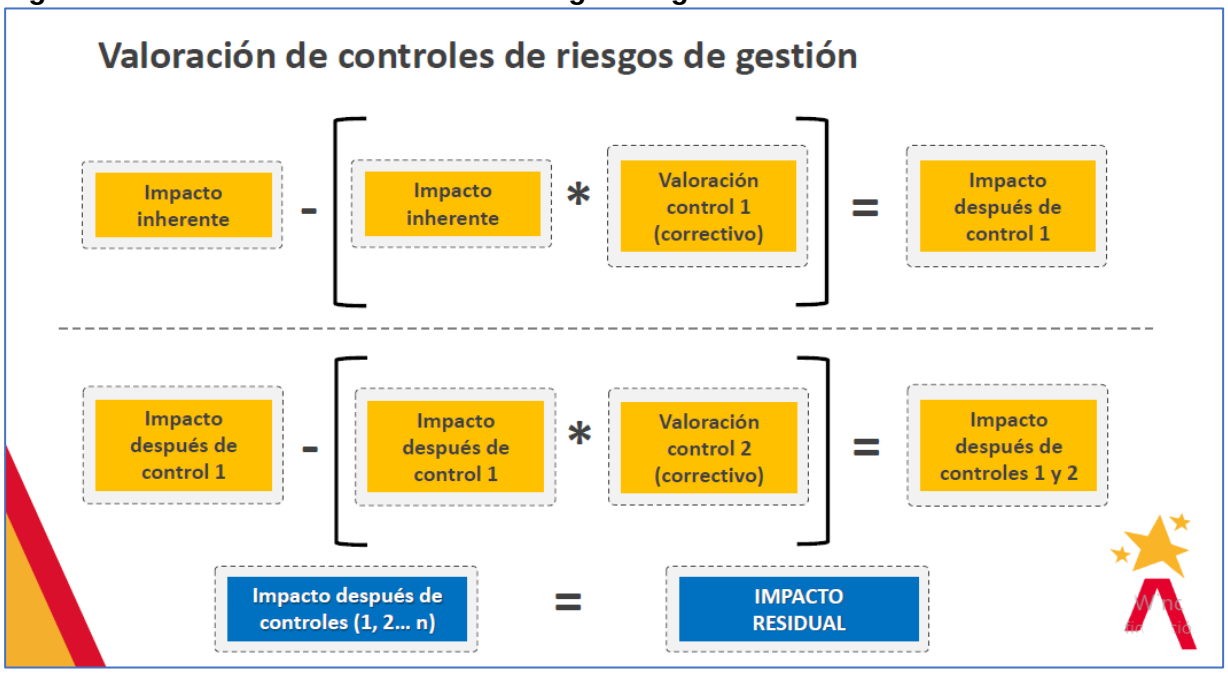
Tabla 7. Aplicación de controles para establecer el riesgo residual.

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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

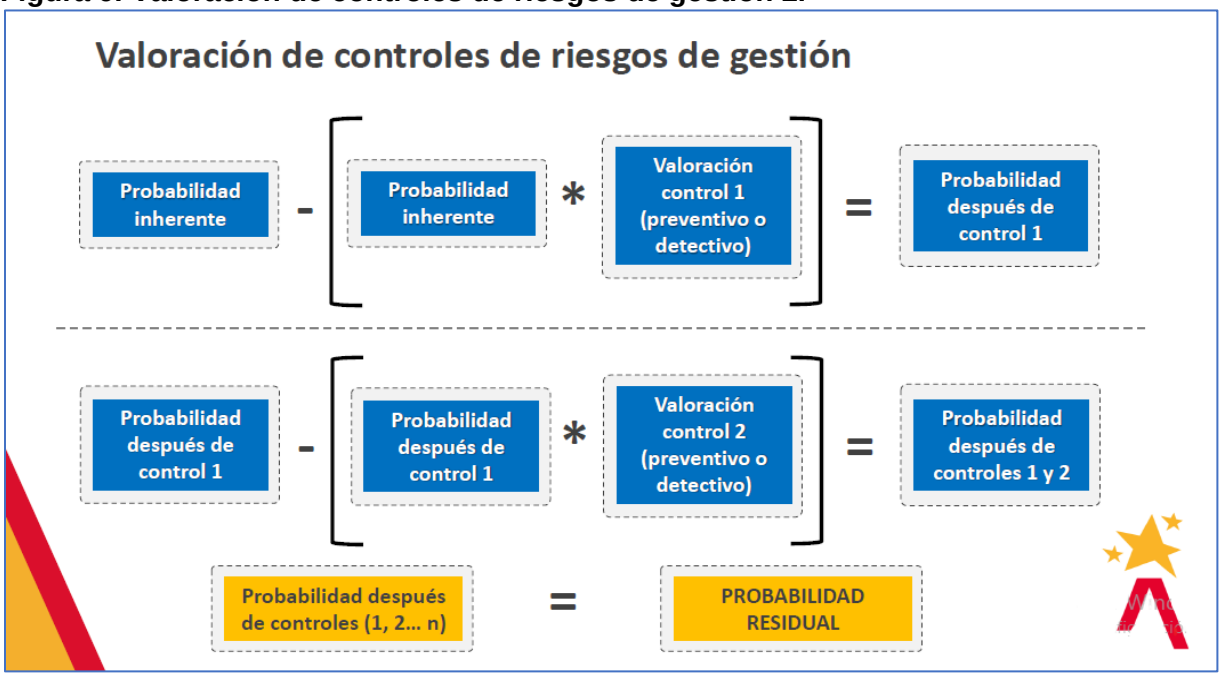
CO16/7252

Figura 8. Valoración de controles de riesgos de gestión.



Fuente: Capacitación: Gestión del Riesgo: análisis y evaluación, Secretaría General de Bogotá, julio 16 de 2021.

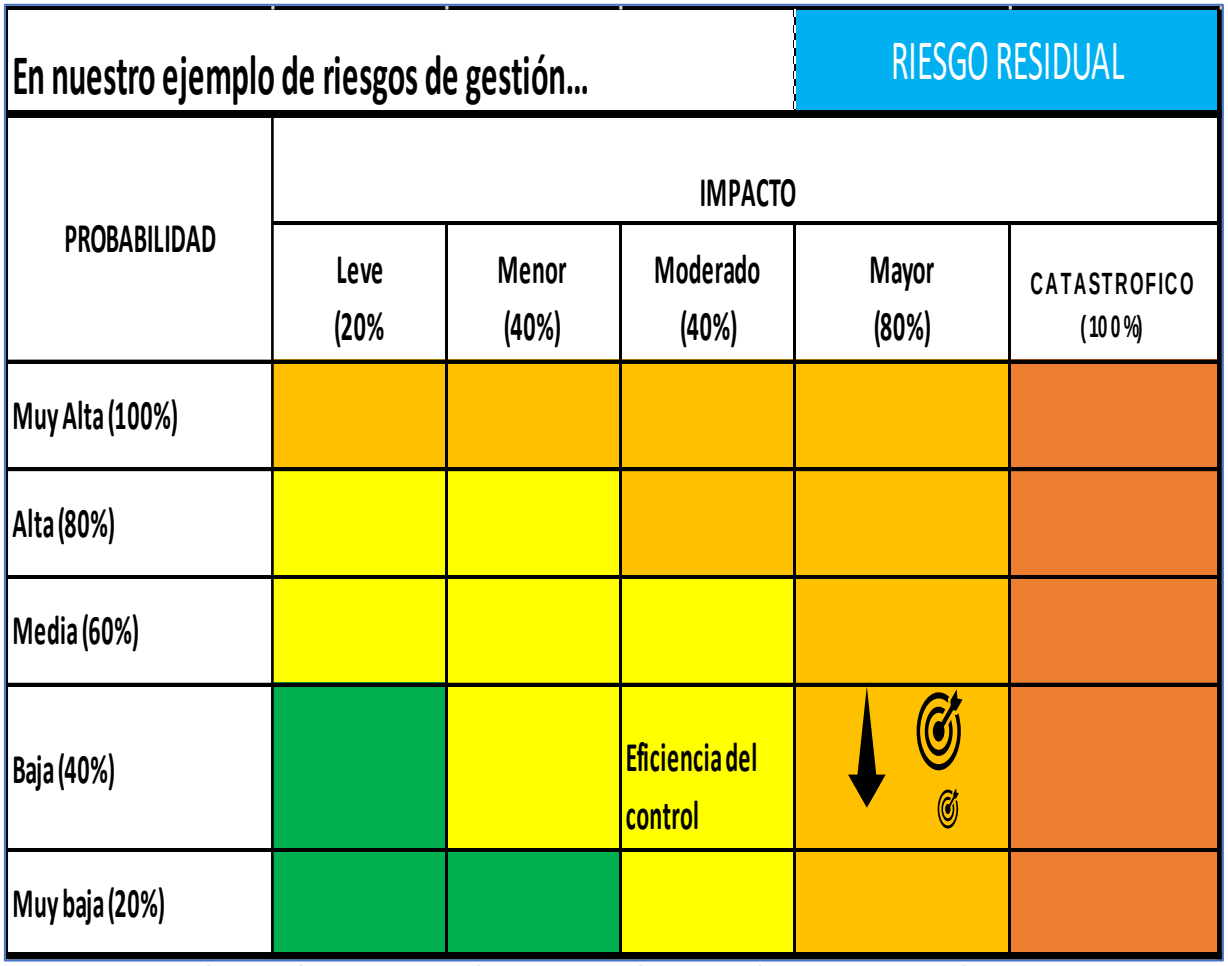
Figura 9. Valoración de controles de riesgos de gestión 2.



Fuente: Capacitación: Gestión del Riesgo: análisis y evaluación, Secretaría General de Bogotá, julio 16 de 2021.

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.

Figura 10. Ejemplo, riesgo residual.



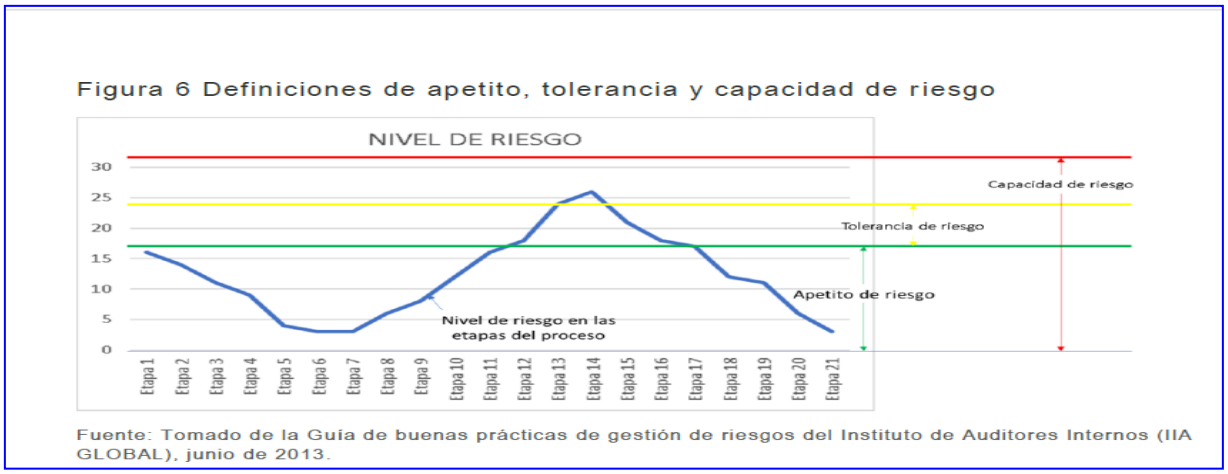
Fuente: Capacitación: Gestión del Riesgo: análisis y evaluación, Secretaría General de Bogotá, julio 16 de 2021.

7.3.2.4 Nivel de aceptación del riesgo y estrategias para afrontar el riesgo

7.3.2.4.1 Marco conceptual para determinar los niveles de Aceptación del riesgo en la UAESP.

Acogiendo los lineamientos del DAFP en la Guía de administración del riesgo V.5, se establecen las siguientes categorías conceptuales para determinar los niveles de Aceptación del riesgo en la UAESP:

Figura 11. Definiciones de apetito, tolerancia y capacidad de riesgo.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP - diciembre de 2020

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. Es el ejercicio que ya se ha adelantado en relación con la aplicación de los mapas de calor, tanto para el riesgo inherente como para el riesgo residual.

En la gráfica el nivel de riesgo corresponde a la línea azul, que señala que los procesos son dinámicos (tienen etapas), y que un riesgo determinado puede ser leve en una determinada etapa, pero muy relevante en otra. Este análisis corresponde a la identificación de los “puntos de riesgo”, dentro de la identificación del riesgo.

Las siguientes categorías (apetito, tolerancia y capacidad de riesgo) se aplican para el nivel de riesgo “residual”, toda vez que **la UAESP dentro de esta política de riesgos, define que todo riesgo, por el sólo hecho de ser identificado, debe ser objeto de tratamiento a través de la aplicación de controles para evitar su materialización.** Lo anterior en cumplimiento de los principios que rigen de la administración pública (art 209 de la Constitución Política).

DETERMINACIÓN DEL APETITO DEL RIESGO. El apetito del riesgo se entiende como el nivel de riesgo residual que la Unidad define como aceptable, en condiciones normales de operación, para el logro de sus metas y objetivos, en el marco de las disposiciones de la alta dirección. 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 son inaceptables.

DETERMINACIÓN DE TOLERANCIA AL RIESGO: En la Guía DAFP v5, se define como el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Este valor debe ser igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo. Es necesario establecer un nivel de tolerancia al riesgo ya que la UAESP por la naturaleza de sus funciones debe acometer tareas en donde, aun siendo sujetas de control, persisten riesgos en su ejecución, caso en el cual la entidad debe adelantar acciones para MITIGAR la posibilidad de materialización del riesgo. 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).

DETERMINACIÓN DE LA CAPACIDAD DE RIESGO: es el máximo valor del nivel de riesgo que una entidad puede soportar, antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. A partir de este punto la alta dirección considera que no sería posible el logro de los objetivos de la entidad. Para cada uno de estos eventos, la alta dirección de la UAESP, en el marco del Comité Institucional de Coordinación de Control Interno, debe realizar el análisis de riesgos críticos que tienen un nivel de severidad muy alto frente a los cuales se deben tomar decisiones. Frente a estos eventos, la UAESP puede tomar la decisión de evitar el riesgo no emprendiendo la acción. Sin embargo, la UAESP, por la naturaleza de sus funciones, puede verse en la necesidad de emprender tareas incluso en estas circunstancias, caso en el cual la entidad debe adelantar acciones para MITIGAR la posibilidad de materialización del riesgo, o TRASLADAR (tercerizar) el mismo en aquella parte que sea susceptible de esta medida. 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).

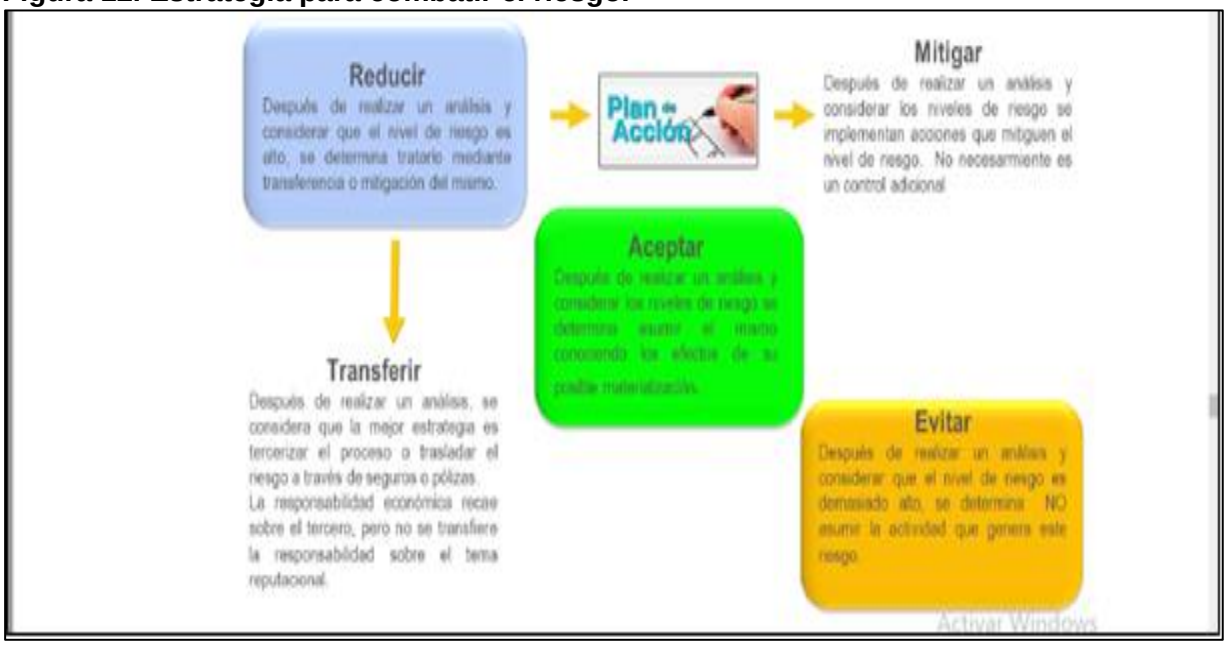
Una relación sencilla entre los anteriores conceptos es la siguiente: “El apetito es el nivel de riesgo que la empresa quiere aceptar y su tolerancia es la desviación respecto a este nivel. La capacidad es el máximo de riesgo que una organización puede soportar en la persecución de sus objetivos.”[6]

7.3.2.4.2 ESTRATEGIA PARA COMBATIR EL RIESGO (tratamiento del riesgo)

Decisión que se toma frente a un determinado nivel de riesgo. En la UAESP, siempre que se identifique un riesgo (riesgo inherente) se deben establecer controles para evitar su materialización. Respecto al riesgo residual la UAESP puede decidir aceptarlo, reducirlo o evitarlo, conforme lo señala el DAFP:

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

Figura 12. Estrategia para combatir el riesgo.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP - diciembre de 2020

Las diferentes opciones para combatir los riesgos se materializan en el siguiente acápite.

Para todos los casos en que subsista un riesgo residual, se debe definir un plan de manejo del riesgo. Así, mientras 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. Ejemplo:

Figura 13. Ejemplo matriz plan de manejo.

Riesgo	zonR. Inh	Control	Zon R. Resid	**Plan Acción**	Respon-sable	Fecha imple-menta-ción	Fecha Seguimiento	Seguimiento	Estado
Posibilidad de afectación económica por multa y sanciones del organismo de control debido la adquisición de bienes y servicios fuera de los requerimientos normativos.	Zona alta	Control 1 El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación. Control 2 El jefe de del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	Zona alta	**Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso.**	Oficina de TIC	30/11/2020	30/06/2020	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo.	En curso

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP - diciembre de 2020, construido con base al ejemplo págs. 52 a 56

Los planes de contingencia son aquellos que se establecen cuando se ha materializado el riesgo.

En el caso de riesgos en zona de severidad extrema, con una probabilidad media o superior, se deben establecer previamente planes de contingencia para hipótesis de riesgos materializados.

7.3.2.4.3 Niveles de aceptación del riesgo en la UAESP.

De acuerdo con el anterior marco conceptual, la UAESP define los siguientes niveles de aceptación del riesgo:

Tabla 8. Niveles de Aceptación del Riesgo.

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVELES DE ACEPTACIÓN	ACCIÓN A TOMAR
Riesgos de Gestión y Riesgos 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 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 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 mensual o una vez terminada la gestión del riesgo. y por último EVITAR el riesgo por medio de la definición acciones de plan de manejo, 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.

7.3.3 Mapa de riesgos

Las etapas de la anterior metodología se llevarán de manera secuencial en el formato DES-FM-12 V10, Mapa y plan de manejo de riesgos de la UAESP (hoja “Riegos de gestión”), el cual acoge el modelo propuesto por el DAFP en la anterior Guía (pág. 52 a 56).

Igualmente se debe aplicar el procedimiento: “Administración del riesgo” documento DES-PC-07 V7,del SIG de la UAESP, que tiene por objeto: “Definir las actividades para la administración del riesgo y oportunidades, mediante la aplicación de la Política de administración del riesgo de la UAESP, a partir de su identificación y valoración (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 de la Unidad Administrativa Especial de Servicios Públicos – UAESP”.

7.4 OTRAS HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO.

De acuerdo con la guía DAFP v. 5, además del mapa de riesgos, las UAESP puede acudir a otras herramientas para la administración del riesgo a saber:

- Revisión histórica de eventos materializados (…) [ver Guía pág. 58]
- Indicadores claves de Riesgo (Key Risk Indicators- KRI) (…) [ver Guía pág. 58]

Así mismo la entidad puede acudir a la herramienta “mapas de aseguramiento”[7]. 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.

7.5 PERIODICIDAD PARA EL SEGUIMIENTO.

Los riesgos se actualizan y validan de manera permanente y en cualquier momento, considerando las condiciones de operación internas o externas y no están sometidos a una determinada vigencia. Cada líder de proceso actualiza el análisis de contexto, riesgos y controles como resultado de los ejercicios de autocontrol, autoevaluación, evaluación independiente o por decisión del CICCI según estime conveniente para asegurar el cumplimiento de los objetivos del proceso; en todo caso la revisión y actualización se realizará mínimo una vez al año con el acompañamiento de la Oficina Asesora de Planeación y la asesoría de la Oficina de Control Interno.

Los riesgos de corrupción actualizados se publican a más tardar el 31 de enero de cada año.

De acuerdo con el nivel del riesgo residual, la periodicidad para el seguimiento del riesgo se determina de acuerdo con los niveles de aceptación del riesgo (ver tabla 8, págs. 38 y 39 de este documento).

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

El proceso reporta trimestralmente a la segunda línea de defensa a través del mapa y plan de manejo de riesgos, 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 de contingencia para su tratamiento, previa realización del análisis de causas correspondiente (ver acápite 8 de este documento).

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 hábiles del mes de enero.

8. RIESGOS MATERIALIZADOS

Cuando se detecte la materialización de los riesgos, se establecen 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 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.

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 riesgos de Gestión 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.

- Si el riesgo es de gestión y/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.

10. LINEAMIENTOS PARA RIESGOS DE SEGURIDAD DE LA INFORMACION

Siguiendo el orden temático de la Guía de la Administración de Riesgos y el diseño de controles en entidades públicas, DAFP, v5 (diciembre, 2020), se establecen unos lineamientos particulares para los riesgos de seguridad de la información, si bien en algunos aspectos es aplicable la metodología general explicada en los anteriores acápites.

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 políticas seguridad de la información, que hace parte del Sistema integrado de gestión (SIG) de la entidad.

Para este tipo de riesgos se establecen los siguientes lineamientos específicos, en la Guía de Riesgos DAFP v.5 (diciembre, 2020), capítulo 5.

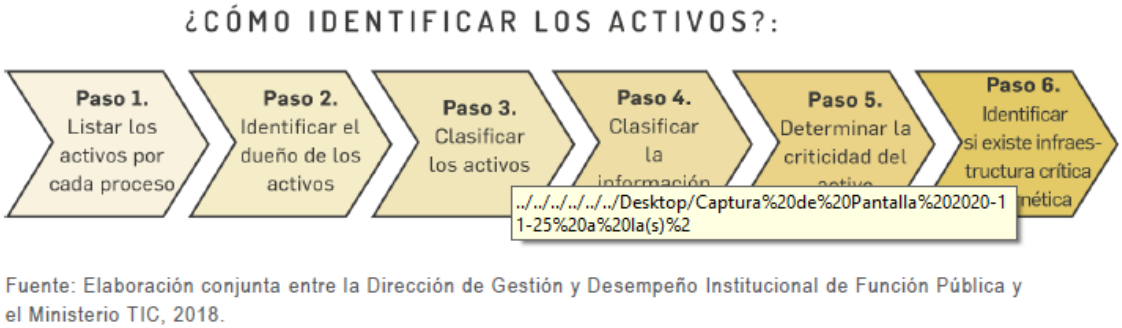
10.1. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

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

¿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 administración del riesgo DAFP V5./ Figura 20 Conceptualización activos de información

Figura 14. Pasos para la identificación de activos.



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

10. 2 IDENTIFICACIÓN DEL RIESGO.

Se siguen los pasos de la metodología del DAF. Sin embargo, 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[8].

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 seguridad de la información para entidades públicas”[9] 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

[8] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
[9]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

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 del a información de la estrategia de Gobierno Digital (GD) del Ministerio de la Tecnologías de Información y las Comunicaciones"

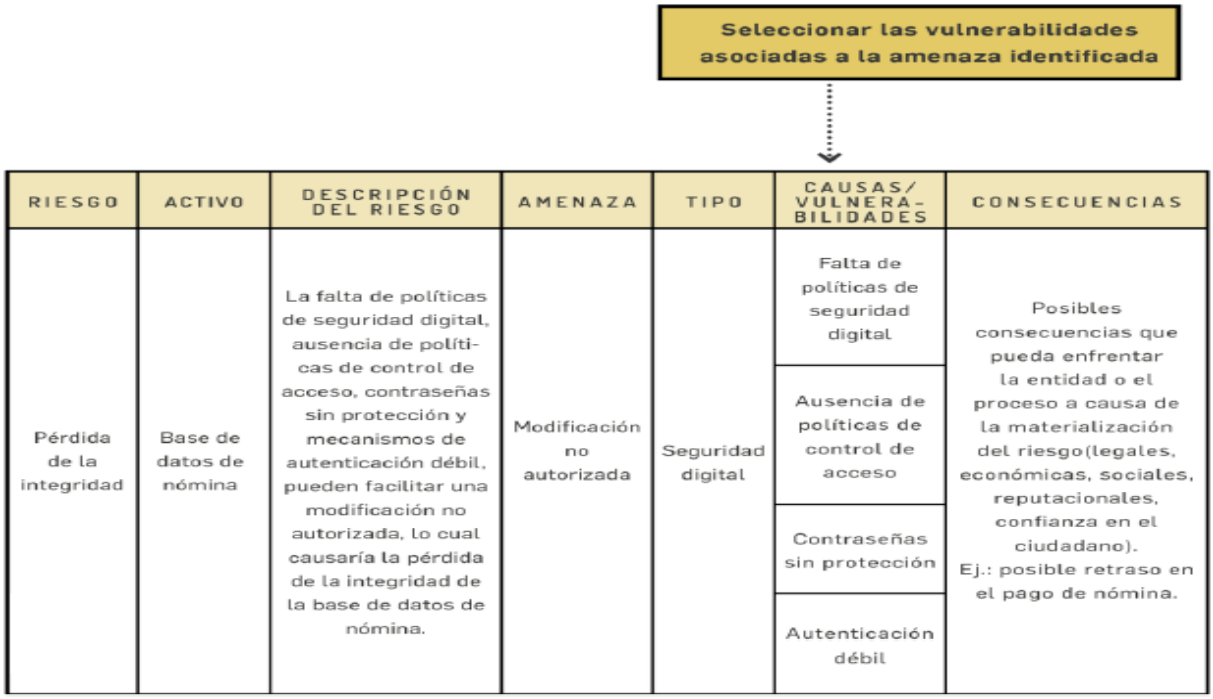
Tabla 9. Amenazas y vulnerabilidades de acuerdo con el tipo de activo.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
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: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC. 2018.

En el siguiente ejemplo de la Guía de Riesgos del DAFP v.5, sobre un activo como es la base de datos de nómina.

Figura 15. Formato de descripción del riesgo de seguridad de la información.



RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Pérdida de la integridad	Base de datos de nómina	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Fuente: Guía administración del riesgo DAFP V5./ Figura 22 Conceptualización activos de información, pág. 79.

10.3 VALORACIÓN DEL RIESGO

10.3.1 Análisis del riesgo: probabilidad e impacto.

De acuerdo con la Guía de Riesgos DAFP v.5, en este aspecto, los riesgos de seguridad de la información se someten a la metodología general. Por lo tanto, para esta etapa se asociarán las tablas de probabilidad e impacto definidas en las páginas 18 a 23 de esta política.

10.3.2 Evaluación del riesgo y Controles asociados a la seguridad de la información.

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):

Tabla 10. 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: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

10.3.3. Mapa de riesgos de seguridad de la información.

Debe tener la siguiente estructura básica:

Figura 16. Formato mapa riesgos seguridad de la información.

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Pérdida de la integridad**	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	**Probable**	**Menor**	**Moderado**	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Fuente: Guía administración del riesgo DAFP V5, pág. 85

Las etapas de la anterior metodología se llevarán de manera secuencial en el formato DES-FM-12 Mapa y plan de manejo de riesgos de la UAESP (hoja "Riegos de Seguridad Información"), el cual acoge el modelo propuesto por el DAFP en la anterior Guía (pág. 52 a 56).

11. LINEAMIENTOS RIESGOS DE CORRUPCIÓN

Siguiendo el orden temático de la Guía de la Administración de Riesgos y el diseño de controles en entidades públicas, DAFP, v5, en la misma se señala que se siguen teniendo en cuenta los lineamientos de la guía DAFP Versión 4 (2018). Igualmente, la Guía V.5 tiene un acápite específico, el número 4, destinado a la gestión de riesgos de corrupción donde se resumen los lineamientos de la Guía V. 4

11. 1 GENERALIDADES ACERCA DE LOS RIESGOS DE CORRUPCIÓN

Dentro de las reseñadas en el capítulo 4, de la Guía de Riesgos DAFP v.5, se destacan los siguientes:

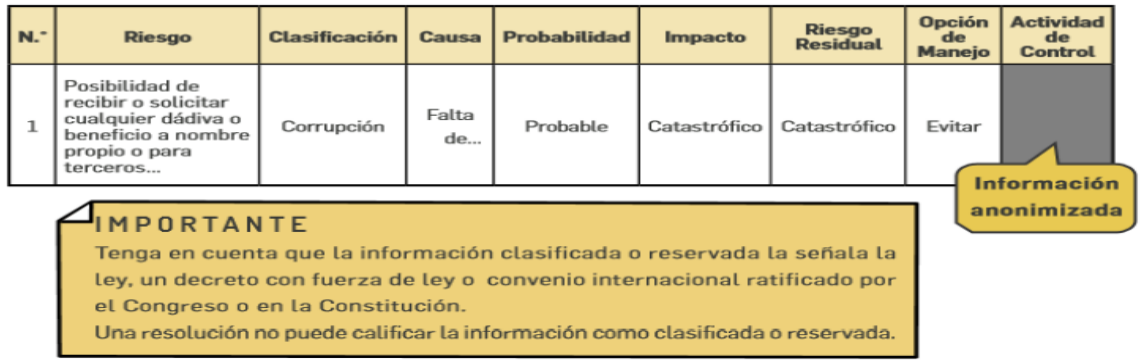
- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de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

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

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

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

Figura 17. Ejemplo, información anonimizada.



Fuente: Guía administración del riesgo DAFP V5./, pág. 66.

- **Ajustes y modificaciones**: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

- **Monitoreo:** en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

- **Seguimiento:** el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

11.2 IDENTIFICACIÓN DEL RIESGO. TÉCNICAS PARA SU IDENTIFICACIÓN.

Definición de riesgo de corrupción: 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 y/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.

Las restantes temáticas asociadas a la identificación del riesgo se aplican de acuerdo con la metodología general

11.3 VALORACIÓN DE LOS RIESGOS

11.3.1 Cálculo de la probabilidad e impacto

Análisis de la probabilidad

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:

Figura 18. Conceptualización activos de información

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 administración del riesgo DAFP V5.

Análisis del impacto

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:

Tabla 11. Criterios para Definir el Nivel de Impacto – Riesgos de Corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	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.		Nivel de impacto MAYOR 10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

Fuente: Secretaría de Transparencia de la Presidencia de la República.

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

Por lo anterior, y teniendo en cuenta las respuestas a las preguntas referentes a la valoración de los riesgos de corrupción se establece la siguiente valoración:

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

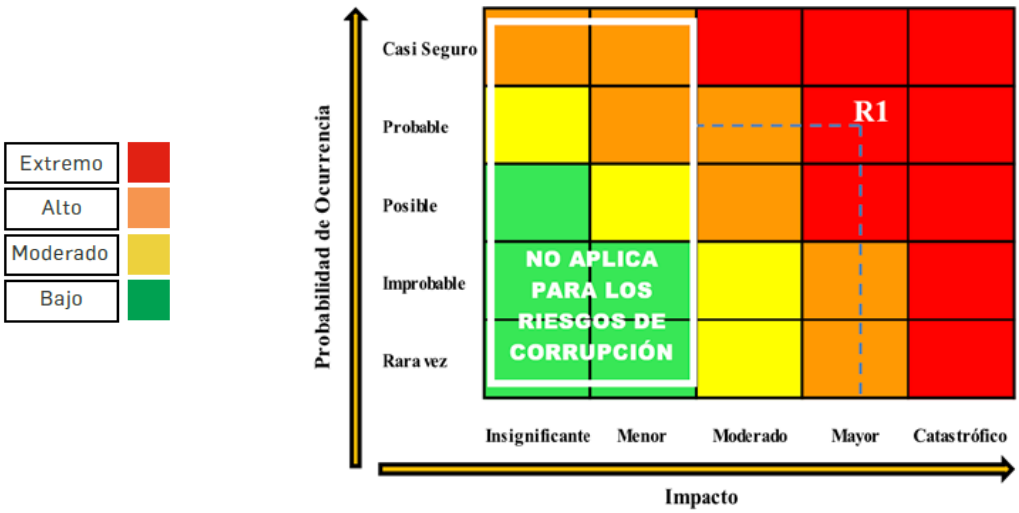
11.4 VALORACIÓN DEL RIESGO DE CORRUPCIÓN.

Tabla 12. Valoración – Riesgos de Corrupción.

Nivel	Impacto	Descripción	Riesgos de Corrupción
3	MODERADO	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de UNO a CINCO preguntas(s) genera un impacto MODERADO
4	MAYOR	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de SEIS a ONCE preguntas genera un impacto MAYOR
5	CATASTRÓFICO	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto CATASTRÓFICO

Fuente: DAFP.2020

Figura 1. Mapa de Calor de Riesgo de Corrupción



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020

Para los riesgos de corrupción, 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 los riesgos de corrupción no admiten aceptación, es decir, el impacto de ningún riesgo de corrupción, 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, 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 riesgos de corrupción. En esa medida los riesgos de corrupción siempre deben tener un tratamiento.

11.4.1. Establecimiento de controles para el riesgo inherente.

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, por lo tanto, se debe hacer remisión a dicho documento (Pag 48 a 67). 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 están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados, según los pautas que se señalan a c**ontinuación.**
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 (ver Pag 50).
Paso 2: Debe tener una periodicidad definida para su ejecución. (ver Pag 51-52)
Paso 3: Debe indicar cuál es el propósito del control. (ver Pag 53-54)
Paso 4: Debe establecer el cómo se realiza la actividad de control. (ver Pag 54-55)
Paso 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control (ver Pag 55-56)
Paso 6: Debe dejar evidencia de la ejecución del control. (ver Pag 57-58)

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, pág.74), solo establece dos tipos de controles preventivos y detectivos (no alude a los correctivos, que sí están admitidos en la Guía V.5). En consecuencia, para riesgos de corrupción sólo se permiten riesgos preventivos y detectivos.

Tabla 13. 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), p 60

Tabla 14. 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), p 60

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

Figura 19. Evaluación de los riesgos de corrupción.

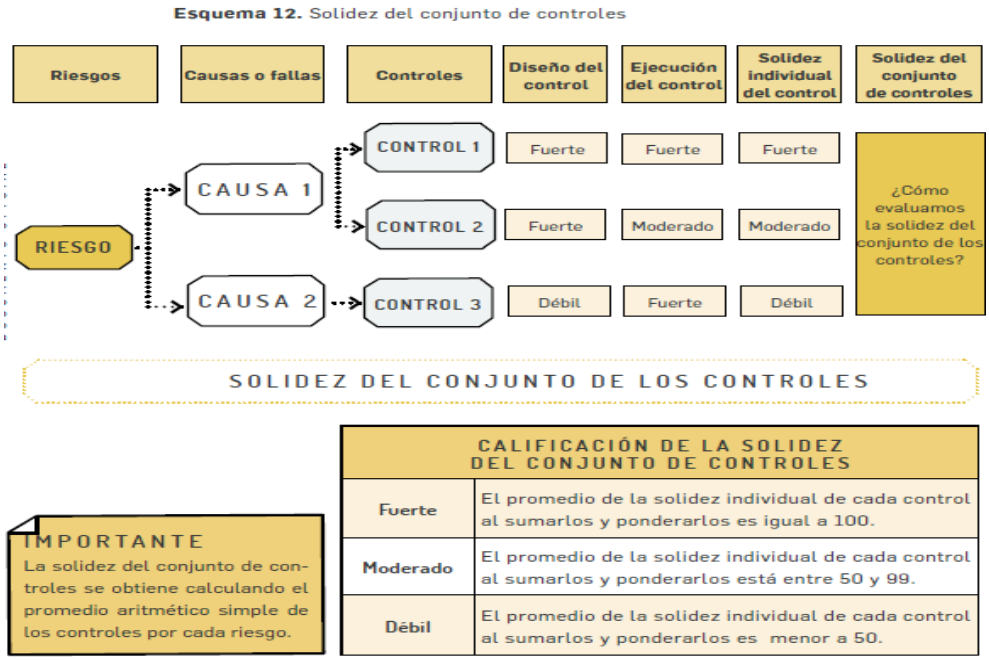
RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO - PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

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), p 62

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.

Figura 20. Solidez del conjunto de controles.



Fuente: Guía administración del riesgo DAFP V4 (2018), p 64

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), págs. 48-65

11.4.2 Determinación del riesgo de corrupción residual.

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:

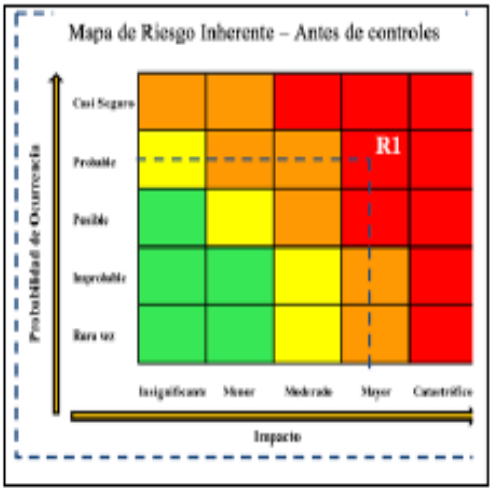
Tabla 15. Resultados de los posibles desplazamientos de la probabilidad del impacto de los riesgos.

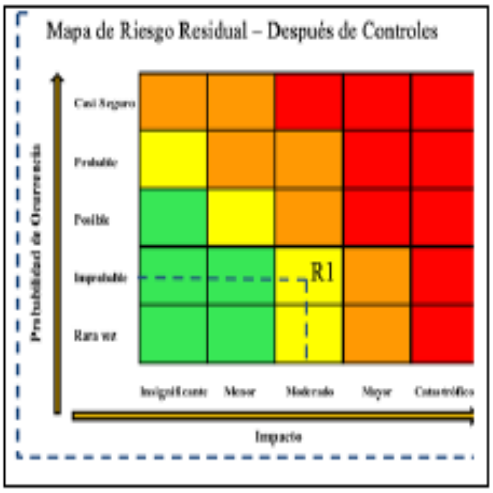
SOLIDEZ DEL CONJUNTO DE LOS CONTROLES.	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
fuerte	directamente	directamente	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

Tenemos el riesgo 1 con una calificación de riesgo inherente de probabilidad e impacto como se muestra en la siguiente gráfica:

Como podemos observar, es probable que el riesgo suceda y, en caso de materializarse, tiene un impacto mayor para la entidad. Ahora, supongamos que existen controles bien diseñados, que siempre se ejecutan, y que estos controles disminuyen de manera directa la probabilidad.

En nuestro ejemplo disminuiría dos cuadrantes de probabilidad, pasa de probable a improbable y un cuadrante de impacto, pasa de mayor a moderado.





Fuente: Guía administración del riesgo DAFP V4 (2018), p 66-67

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, 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.

Figura 21. Mapa de riesgo inherente, antes de controles.

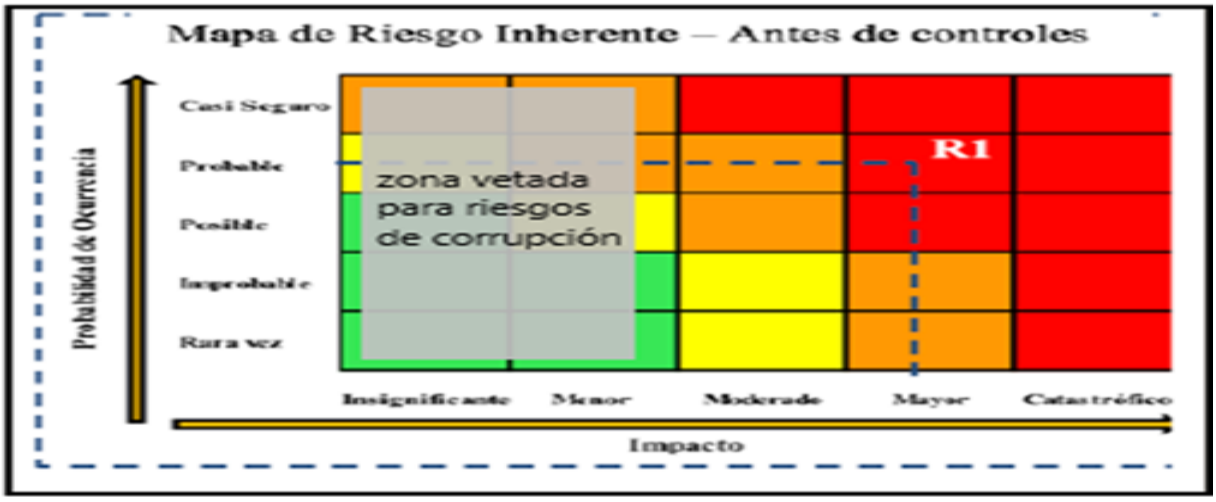


Figura 22. Mapa de riesgo inherente, después de controles.

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

11.5 TRATAMIENTO DE RIESGOS DE CORRUPCIÓN

La Guía de riesgos DAFP v4 (2018), señala las mismas posibilidades de tratamiento de riesgo de la Versión 5 (2020), por lo tanto, se debe acudir a la parte general de este documento para esos efectos. Sin embargo, la Guía V.4 aclara que “En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo”, lo anterior dado que se parte de la premisa de que “los riesgos de corrupción son inaceptables” (pág. 68).

Para el caso de riesgo residual se debe definir un plan de manejo del riesgo. el cual consiste tomar acciones o controles adicionales para evitar la materialización de los riesgos, el cual requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

En caso de materialización del riesgo, se definen las acciones señaladas en el acápite 11.7

11.6 Matriz (mapa) de riesgos de corrupción.

Figura 23. Formato mapa y plan de tratamiento de riesgos.

Formato mapa y plan de tratamiento de riesgos

- DOCUMENTO OFICIAL -

N.	RIESGO	CLASIFICACIÓN	CAUSAS	PROBABILIDAD	IMPACTO	RESPUESTA RESIDUAL	OPCIÓN MANEJO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
N	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para celebrar un contrato	Corrupción	Debilidades en la etapa de planeación	Probable	Catastrófico	Extremo	Reducir	Manual de contratación implementado con parámetros técnicos y financieros para cada tipo de contratación, formalizado en procedimiento.	Manual de contratación	Jefe de contratos	Primer trimestre de...	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= ((# de casos de favorecimiento a proponentes presentados periodo actual - # de casos de favorecimiento a proponentes presentados periodo anterior) / # de casos de favorecimiento a proponentes presentados periodo anterior) x 100
			Presiones indebidas				Reducir	Comité de contratación	Acta administrativo conformando comité	Jefe de contratos	Trimestralmente	
			Carencia de controles en el procedimiento de contratación				Reducir	Difusión y capacitación a todos los funcionarios del proceso.	Actas de capacitación	Director talento humano	Del (día /mes/año) al (día / mes/año)	
			Excesiva discrecionalidad				Acción de Contingencia	Iniciar la investigación disciplinaria, fiscal o remitir a las instancias correspondientes para el proceso penal.	Comunicación iniciando o remitiendo investigación	Jefe control disciplinario interno	1 semana una vez el riesgo de liquidez se materialice	

Fuente: Guía administración del riesgo DAFP V5, pág. 84

Las etapas de la anterior metodología se llevarán de manera secuencial en el formato DES-FM-12 V10, Mapa y plan de manejo de riesgos de la UAESP (hoja “Riegos de corrupción”), el cual acoge el modelo propuesto por el DAFP en la Guía de riesgos V. 4 (pág. 52 a 56).

CO16/7252

11.7 MONITOREO Y REVISIÓN.

Le corresponde a la primera línea de defensa el establecimiento de actividades de control, como medio para propiciar el logro de los objetivos. Las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo.

Le corresponde a la segunda línea de defensa (oficina de planeación) adelantar el monitoreo constante la gestión de riesgos de corrupción, y a la efectividad de los controles establecidos, a través de la matriz o mapa de riesgos de la entidad, con la misma periodicidad que se realiza para los restantes riesgos de la entidad. Lo anterior teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

A la tercera línea de defensa le corresponde el seguimiento de riesgos de corrupción. En consecuencia, al jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles, con la misma periodicidad con que se hace seguimiento a los riesgos generales de la entidad, a saber:

- 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.

11.8 ACCIONES EN CASO DE MATERIALIZACIÓN DEL RIESGO

- En los casos de riesgos de corrupción detectado por la primera Línea de defensa, se debe informar sobre el hecho encontrado a la Oficina de Planeación y a la Oficina de Control Interno, para lo de su competencia, de considerarlo necesario, realizar la denuncia ante los entes respectivos y a la Alta Dirección sobre el hallazgo y las acciones tomadas.

- 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 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.

- 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 riesgos de corrupción detectado por la tercera Línea de defensa, se deben tomar las siguientes acciones

  1). Informar a las autoridades de la ocurrencia del hecho de corrupción.
  2). Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
  3). Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
  4). Llevar a cabo un monitoreo permanente.

El resto de las temáticas asociadas a la identificación y valoración del riesgo se aplican de acuerdo con la metodología general

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.

AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	LADY CAROLINA LEON GUTIERREZ	Profesional Universitario Oficina Asesora de Planeación	
	LUZ MARY PALACIOS CASTILLO	Profesional Universitario Oficina Asesora de Planeación	
	AIDA YOLIMA ZARATE AGUILLON	Técnico Operativo Oficina Asesora de Planeación	
	BLAIR ALEJANDRO TORREZ RODRIGUEZ	Contratista Oficina Asesora de Planeación.	
	JUAN CARLOS PULIDO FONSECA	Contratista Oficina Asesora de Planeación.	
	RUTH YAILENA RICAURTE PEÑA	Contratista Oficina Asesora de Planeación.	
Revisó	GERMAN GUILLERMO SANDOVAL PINZON	Contratista Oficina Asesora de Planeación.	
Aprobó	FRANCISCO JOSE AYALA SANMIGUEL	Jefe Oficina Asesora de Planeación	
Revisó y Aprobó	Comité Institucional de Coordinación de Control Interno		

ALCALDÍA MAYOR
DE BOGOTÁ D.C.

UAESP
Unidad Administrativa Especial
de Servicios Públicos

BOGOTÁ