Política de Administración del Riesgo Alcaldía de Fusagasugá

Proceso de Direccionamiento Estratégico

Dirección de Desarrollo Organizacional

Versión 4

Febrero 14 de 2025

Índice

Contenido

1. MARCO NORMATIVO Y TÉCNICO 3
2. CONTEXTO ESTRATEGICO DE LA ENTIDAD 3
3. COMPROMISO CON LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 4
4. DECLARACIÓN DE LA ENTIDAD 5
5. OBJETIVOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 5
5.1 Objetivo principal 5
5.2 Objetivos específicos 5
6. ALCANCE DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 5
7. GLOSARIO 5
8. RESPONSABILIDADES 8
9. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO 11
10. IDENTIFICACIÓN DEL RIESGO 11
11. DESCRIPCIÓN DEL RIESGO 13
12. VALORACIÓN DEL RIESGO 15
13. NIVEL DE APETITO AL RIESGO 17
14. VALORACIÓN DE CONTROLES 18
14.1 Estructura para la descripción del control 18
14.2 Análisis y evaluación de controles 18
15. TRATAMIENTO DE RIESGOS 19
16. HERRAMIENTAS PARA LA GESTIÓN DE RIESGOS 19
17. ACCIONES ANTE LA MATERIALIZACIÓN DE RIESGOS 20
18. ESTRATEGIAS PARA LA ACEPTACIÓN DEL RIESGO RESIDUAL 21
19. MONITOREO Y REVISIÓN 21
20. SEGUIMIENTO Y EVALUACIÓN 22
21. REVISIÓN DE RIESGOS INSTITUCIONALES 23
22. COMUNICACIÓN Y CONSULTA 23
23. CONTROL DE CAMBIOS 23

Índice de tablas

Tabla 1 Contexto estratégico de la Entidad 3
Tabla 2 Responsabilidades de las líneas de defensa 8
Tabla 3 Áreas factores de riesgo 12
Tabla 4 Clasificación de riesgos 14
Tabla 6 Probabilidad de riesgo de Gestión, Seguridad de la información y fiscales 15
Tabla 7 Probabilidad de Riesgos de corrupción 15
Tabla 8 Calificación del impacto riesgos de gestión, seguridad de la información y riesgos fiscales 16
Tabla 9 Calificación del Impacto de riesgos de corrupción 16
Tabla 10 preguntas orientadoras en la definición de riesgos de corrupción 17
Tabla 11 Determinación del riesgo inherente 17
Tabla 5 nivel de aceptación de riesgos de SGSST 18
Tabla 12 Atributos para el diseño de los controles 20
Tabla 13 Acciones de respuesta a riesgos 21

Índice de ilustraciones

Ilustración 1 Formulación del riesgo de gestión 13
Ilustración 2 Formulación de riesgo fiscal 14

1. MARCO NORMATIVO Y TÉCNICO

- Ley 1474 de julio 12 de 2011 Artículo 73, modificado por el Artículo 31 de la Ley 2195 de 2022, el Gobierno Nacional reglamenta que: "Cada Entidad del orden Nacional, Departamental y Municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano".
- Ley 1562 de julio 11 de 2012, define la obligación de implementar Sistemas de Control de Riesgos Laborales y las Medidas Especiales de Promoción y Prevención.
- Decreto 124 del 26 de enero de 2016 "Por el cual se sustituye el Título IV de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano", se estableció en su Artículo 2.1.4.1. como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022
- Decreto 1072 de mayo 26 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo".
- Decreto 648 de abril 19 2017, "Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública".
- Decreto 1499 de septiembre 11 de 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015", se realiza la articulación entre el Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Control Interno.
- Decreto 016 del 03 de febrero de 2023, "Por medio del cual se adopta la Estructura de la Alcaldía del Municipio de Fusagasugá-Cundinamarca, se señalan las funciones generales de sus Dependencias y se dictan otras disposiciones".
- Decreto 058 del 13 de junio de 2023, "Por medio del cual se compila y se actualiza la implementación del Modelo Integrado de planeación y gestión – MIPG, en el Municipio de Fusagasugá y se dictan otras disposiciones.
- Resolución 0312 de febrero 13 de 2019, "Por la cual se definen los Estándares Mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST)."
- Norma Técnica Colombiana ISO 9001 Sistema de Gestión de la Calidad.
- Norma Técnica Colombiana ISO 31000:2018 Gestión del Riesgo.
- Norma Técnica Colombiana ISO/IEC 27001:2022 "Sistema de Gestión de la Seguridad de la Información".
- Norma Técnica Colombiana ISO 27005:2020 "Tecnología de la información. Técnicas de seguridad. Gestión de riesgos para la seguridad de la información.
- Norma Técnica de Colombiana ISO 45001:2018 "Sistema de Gestión de Seguridad y Salud en el Trabajo".
- Guía Técnica Colombiana GTC 45:2012 "Guía para la identificación de los peligros y la valoración de los riesgos de Seguridad y Salud en el Trabajo".
- Guía para administración de riesgos y el diseño de controles en entidades públicas, versión 6 de noviembre de 2022, del Departamento Administrativo de la Función Pública.
- Modelo Nacional de Gestión de Riesgos de Seguridad de la Información para entidades públicas de 2018, anexo 4.
- Lineamientos establecidos por la Agencia Nacional de Defensa Jurídica del Estado y los manuales, guías y demás documentos emitidos por Colombia Compra Eficiente, relacionados con los riesgos de Defensa Judicial y contratación.

2. CONTEXTO ESTRATEGICO DE LA ENTIDAD

Tabla 1 Contexto estratégico de la Entidad

Contexto Estratégico Alcaldía de Fusagasugá		
	Económicos y financieros	Recursos de inversión, presupuesto.
		Modernización del Estado

Contexto Externo	**Gobernanza pública**	Formalización Laboral
		Cambio de administración
		Objetivos del desarrollo sostenible
		Líneas estratégicas del PND
		Compromisos contra la gestión de riesgos de corrupción y fiscales.
	Sociales y culturales	Objetivos del desarrollo sostenible
		Seguridad Ciudadana, prevención de la corrupción
	Tecnológicos	Estrategias de seguridad de la información
		Plataformas tecnológicas
		Conpes 3975 Política Nacional para la transformación digital
		Política de seguridad digital
		Plan Nacional de Desarrollo
	Ambiental	Contaminación, Desastres naturales
	Legales y reglamentarios	Plan de Desarrollo y normatividad aplicable a las Entidades de orden territorial, Política de transformación Digital (Directiva presidencial SIMPLIFICACIÓN DE INTERACCIÓN DIGITAL LOS CIUDADANOS Y EL ESTADO "2.5. La adopción del modelo de riesgos de seguridad digital de MINTIC es una oportunidad para integrar a todos los procesos a través de la implementación de oportunidades de mejoramiento en materia de continuidad de negocio.
	Comunicaciones	Herramientas virtuales, canales de información, acceso a la tecnología en el territorio.
Contexto Interno	**Financieros**	Presupuesto, Plan Anual de Adquisiciones.
	Talento Humano	Planta de personal, capacitada, formalizada, ejecución de los planes Institucionales
		Manual de funciones adoptado, y socializado.
		Modelo de operación por procesos actualizado
	Modelo de operación por procesos	Apropiación del Modelo Integrado de Planeación y Gestión
		Administración del sistema de gestión de calidad con enfoque basado en riesgos
	Tecnología	Herramientas y aplicativos internos, servidores internos de la Entidad (Intranet, LGPI, ControlDoc Página Web). Adopción de estrategias para fortalecer la seguridad de la información y prevenir los nuevos tipos de riesgos informáticos relacionados con la suplantación de identidad institucional
	Estratégicos	Planeación institucional, funciones y competencias de las dependencias determinadas por el Decreto 016 de 2023.
	Comunicación Interna	Herramientas y aplicativos internos, servidores internos de la Entidad (Intranet, LGPI, ControlDoc Página Web). Canales internos, Redes Sociales.
	Infraestructura	Instalaciones de la Administración Municipal, Centro administrativo Municipal.

Elaboración Propia.

3. COMPROMISO CON LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Alcaldía de Fusagasugá está comprometida con el fortalecimiento de la cultura del autocontrol y la prevención, razón por la cual, acogiendo los lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP), a través del Modelo Integrado de Planeación y Gestión y su articulación con el Sistema de Control Interno, así como lo establecido en la Guía para la Administración de Riesgos y el diseño de controles en entidades públicas, versión 6 de Noviembre de 2022, emitida por el Departamento Administrativo de la Función Pública, la cual incluye un capítulo específico relacionado con el riesgo fiscal, bajo los lineamientos anteriormente mencionados la entidad acoge la presente política de administración de riesgos, como una decisión de la alta dirección y su equipo de servidores públicos, de realizar la administración y gestión de los riesgos inherentes a las actividades propias de la misma.

En consecuencia, la Administración municipal de Fusagasugá, se compromete a gestionar los riesgos identificados de gestión, fiscales, corrupción, seguridad de la información, seguridad y salud en el trabajo, mediante la aplicación de controles y acciones que permitan el desarrollo de una gestión pública efectiva y el cumplimiento de los objetivos estratégicos, respondiendo a las necesidades y expectativas de sus partes interesadas.

La presente Política para la Administración de Riesgos, deberá revisarse y ajustarse con una periodicidad de mínimo un (1) año, cuando se presenten cambios en la normatividad o se indiquen nuevos lineamientos del orden nacional.

4. DECLARACIÓN DE LA ENTIDAD

"La Alcaldía de Fusagasugá se compromete a administrar adecuadamente los Riesgos de Gestión, Corrupción, Seguridad de la Información, Seguridad y Salud en el Trabajo y Fiscales, asociados a los objetivos estratégicos, planes, proyectos y procesos institucionales, acatando la metodología propia para su gestión, implementando las acciones de control oportunas para evitar la materialización y la actuación correctiva inmediata ante las eventualidades, para mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables".

5. OBJETIVOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

5.1 Objetivo principal

Gestionar en la entidad la identificación, valoración, tratamiento, manejo y seguimiento a los Riesgos de Gestión, Corrupción, Seguridad y privacidad de la Información, Seguridad y Salud en el Trabajo y riesgos fiscales, con el fin de mitigar o eliminar sus efectos en el logro de los objetivos estratégicos, para una gestión pública efectiva de la Administración Municipal de Fusagasugá.

5.2 Objetivos específicos

- Definir los roles y responsabilidades frente a la gestión de los riesgos en la entidad.
- Establecer la herramienta metodológica para definir los diferentes tipos de riesgos en los procesos de la entidad, definiendo las actividades de identificación, documentación, valoración, seguimiento y control que permita fortalecer la gestión Institucional.
- Constituir las directrices y técnicas para identificar, examinar y evaluar los riesgos propios de los diferentes procesos de la alcaldía de Fusagasugá, en procura de disminuir sus efectos negativos.
- Diseñar las actividades de monitoreo y seguimiento, de tal forma que la administración del riesgo se constituya en el instrumento de mejoramiento continuo y admita formular acciones efectivas para la toma de decisiones tendientes a fortalecer la gestión institucional.

6. ALCANCE DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Política de Administración del Riesgo es de obligatoria aplicación a los procesos, planes institucionales, proyectos y productos de la entidad durante el desarrollo de la gestión planificada y a todos los servidores públicos en el ejercicio de sus funciones, así mismo, es aplicable en las etapas de identificación, análisis, valoración, monitoreo, seguimiento y evaluación de los riesgos asociados a la Gestión, Corrupción, Fiscal, Seguridad y Salud en el Trabajo y Seguridad de la información, donde esta última es extensible y aplicable a los procesos de la entidad pública que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información, de acuerdo a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC.

7. GLOSARIO

Para el desarrollo de la presente Política, se toman las definiciones establecidas por el Departamento Administrativo de la Función Pública (DAFP) a través de la Guía para la Administración del Riesgo y

Diseño de Controles en Entidades Públicas (Versión 6 de 2022);

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.

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

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares).

Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.
b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Capacidad de Riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo, En el caso de riesgo fiscal, se usa el término circunstancia inmediata, asociado a la misma causa inmediata

Causa raíz: Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.

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

Control: Medida que permite reducir o mitigar un riesgo.

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

Efecto de riesgo fiscal: Es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento potencial del riesgo fiscal: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Gestión del riesgo fiscal: Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

Gestor Público: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal los llamados a prevenir riesgos fiscales. A título de ejemplo, además de los gestores fiscales, son gestores públicos entre otros (sin perjuicio a las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

Gestor fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión, y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique). A título de ejemplo son gestores fiscales entre otros (sin perjuicio de las

particularidades de cada Entidad): Representante legal, Ordenador del gasto, autorizado para contratar, pagador, tesorero, Almacenista.

Integridad: Propiedad de exactitud y completitud.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

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

Patrimonio público: Se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

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

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales.

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

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

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviarla 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 fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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.

Tolerancia al Riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

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

8. RESPONSABILIDADES

Con la entrada en vigencia del Modelo Integrado de Planeación y Gestión (MIPG), que integra los sistemas de gestión de la calidad y de desarrollo administrativo, se crea un único sistema degestión articulado con el sistema de control interno, el cual se actualiza y alinea con el modelo de las tres líneas de defensa. Este modelo de líneas de defensa, proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados. Este modelo proporciona una mirada nueva a las operaciones, ayudando a asegurar el éxito continuo de las iniciativas de gestión del riesgo. Las responsabilidades de la gestión de riesgos y del control están distribuidas en varias áreas; de allí que deban ser coordinadas cuidadosamente para asegurar que los controles operen.

Se describen las responsabilidades frente a la gestión de los riesgos por línea estratégica y líneas de defensa según la siguiente tabla:

Tabla 2 Responsabilidades de las líneas de defensa

Responsabilidades de las Líneas de Defensa		
Línea de Defensa	Responsable	Responsabilidad frente al Riesgo
Línea Estratégica	Alta Dirección, Comité Institucional de Gestión y Desempeño	Asegurar la implementación y desarrollo de las políticas de gestión y desempeño institucional que permitan el soporte de la gestión del riesgo en diferentes ámbitos institucionales.
		Generar recomendaciones de mejora a la política de administración del riesgo.
	Comité Institucional de Coordinación de Control Interno	Someter a aprobación la política de administración del riesgo, diseñada por la Dirección de Desarrollo Organizacional y realizar seguimiento en prevención y detección de fraude y mala conducta.
		Evaluar la eficacia de la política frente a la gestión del riesgo institucional.
		Realizar el monitoreo de los riesgos críticos identificados.
		Analizar los riesgos, vulnerabilidades, amenazas que representen peligro en el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos y capacidades de la Alcaldía.
		Garantizar el cumplimiento de los planes institucionales, estratégicos y sectoriales de la entidad.
Primera Línea	Líderes de Proceso (Secretarios de Despacho, Directores, Jefes de Oficina y funcionarios de las dependencias en todos los niveles)	Identificar, analizar, valorar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso.
		Definir la opción de tratamiento a los riesgos acorde con la Política de Administración del Riesgo.
		Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
		Desarrollar ejercicios de análisis, autoevaluación, monitoreo y control de riesgos, así como la aplicación de acciones de mejora para el fortalecimiento de la eficiencia, eficacia y efectividad de los controles establecidos para los riesgos identificados.
		Informar a la Dirección de Desarrollo Organizacional (Segunda línea) sobre los riesgos de gestión, fiscales y de corrupción materializados en los procesos a cargo.
		Reportar a la Oficina de las TIC y Transformación Digital (segunda línea) los incidentes que se presenten en materia de seguridad de información digital.

		Notificar a la Dirección de Gestión del Talento Humano (segunda línea) los accidentes de trabajo presentados o condiciones que pueden ocasionarlos.
		Definir, aplicar y hacer seguimiento a los controles para gestionar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso.
Segunda Línea	Líderes de Direccionamiento Estratégico	Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la Política de Administración de Riesgos, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual.
		Consolidar el mapa de riesgos por procesos e institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo ante el CIGD para su análisis y ajuste.
		Actualizar la documentación que soporta la estrategia de tratamiento de riesgos.
		Capacitar, acompañar, orientar y entrenar a los líderes de procesos en la metodología de administración de riesgos y en la mejora de los controles establecidos por la primera línea.
		Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
		Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalúe y gestione los riesgos y controles para que se generen acciones.
		Verificar que la gestión de los riesgos esté acorde con la Política de Administración de Riesgos y que sean monitoreados por la primera línea de defensa.
		Identificar cambios en el apetito del riesgo en la entidad, especialmente para determinar el tratamiento más apropiado de los riesgos ubicados en zona baja y ser sometidos a consideración del CICI.
		Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo.
Segunda Línea	Dirección de Gestión del Talento Humano	Garantizar la afiliación de trabajadores y colaboradores al Sistema de Riesgos Laborales.
		Definir el procedimiento para la identificación de peligros, así como la evaluación y valoración de riesgos laborales de la entidad.
		Conformar y garantizar el funcionamiento del Comité Paritario de Seguridad y Salud en el Trabajo (COPASST).
		Elaborar e implementar el Plan Anual de Salud y Seguridad en el Trabajo.
		Reportar a la Administradora de Riesgos Laborales (ARL) y a la Entidad Promotora de Salud (EPS) todos los accidentes de trabajo y las enfermedades laborales diagnosticadas.
		Ejecutar las actividades de prevención y control de peligros y riesgos, de conformidad al resultado de la identificación de peligros y la evaluación y valoración de riesgos de SST.
		Definir el procedimiento para la Identificación y Valoración de Activos de la Entidad, de acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).
		Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).

Segunda Línea	Oficina de las TIC	Asesorar y acompañar a la primera línea de defensa en la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
		Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.
		Impartir lineamientos en materia de tecnología digital para el intercambio, pertinencia, calidad, oportunidad y seguridad de la información.
		Gestionar la seguridad informática en cada uno de los componentes de tecnología para garantizar la integridad, disponibilidad y confidencialidad de la información.
Segunda Línea	Líderes de procesos transversales como: Gestión de Hacienda Pública, Gestión Documental y Gestión Jurídica y Contractual	Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.
		Implementar las acciones necesarias para el tratamiento de riesgos de los depósitos de archivos, la planeación estratégica de la gestión documental y la administración de archivos para la preservación y el control de la información.
		Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico.
Tercera Línea	Oficina de Control Interno	Realizar seguimiento sobre el diseño y efectividad de las actividades de administración del riesgo en la entidad para ayudar a asegurar que los riesgos claves o estratégicos estén adecuadamente definidos, sean gestionados apropiadamente y que el sistema de control interno opera eficazmente.
		Asesorar a la primera línea de defensa, de forma coordinada con la Dirección de Desarrollo Organizacional, el Proceso de Gestión TIC y el Proceso de Gestión del Talento Humano, en la identificación de los riesgos y diseño de controles.
		Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos por procesos y reportar los resultados al CICCI.
		Recomendar mejoras a la Política de Administración del Riesgo.
		Evaluar la efectividad de la operación de los controles determinando si están operando como fueron diseñados y si la persona que ejecuta el control posee autoridad y competencia para desempeñar el control de manera efectiva.

Fuente: Elaboración propia.

De igual manera, la Dirección de Desarrollo Organizacional, el Proceso de Gestión TIC y el Proceso de Gestión del Talento Humano, llevarán a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Socializar anualmente la metodología para la administración de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, alcance, comunicación de los planes y proyectos del proceso asesorado.
- Capacitar a los líderes de los procesos y los profesionales establecidos como enlaces.
- Liderar las mesas de trabajo a realizarse en temas de gestión de riesgos.
- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología establecida. (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, Departamento Administrativo de la Función Pública, 2022).
- Identificar claramente los líderes, integrantes y el personal idóneo del proceso, responsable del reporte de las acciones de control del plan de acción de la matriz de riesgo, donde se evidencia la fecha de finalización y las evidencias de seguimiento.
- Consolidar el mapa de riesgos de proceso con toda la información respectiva, a partir de la información construida con los líderes e integrantes de cada proceso.

- Consolidar el mapa de riesgos de la Alcaldía de acuerdo con la actualización efectuada a los diferentes mapas de riesgos por procesos.
- Identificar, socializar y publicar el mapa de riesgos por procesos e institucional a partir de los mapas de procesos.

Por su parte, los líderes de proceso tienen la responsabilidad de:

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de "administración del riesgo", la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.
- Delegar, por parte del líder del proceso, el o los profesionales idóneos que se encargarán del análisis, identificación, monitoreo, reporte y socialización de los riesgos asociados al proceso.

9. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

En el diseño de la presente política, la metodología acogida por la Alcaldía de Fusagasugá para la administración de los riesgos de Gestión, Corrupción, Seguridad de la información, Seguridad y Salud en el Trabajo y riesgos fiscales corresponde a la contenida en el documento "Guía para la Administración del Riesgo y del Diseño de Controles en Entidades Públicas", Versión 6, establecida por el Departamento Administrativo de la Función Pública, publicada en el mes de noviembre de 2022; además del Anexo No.4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del Ministerio TIC, publicada el mes de octubre de 2021; y la Ley 1562 de 2012 "por la cual se modifica el Sistema de Riesgos Laborales". Es importante subrayar que dicha metodología, se desarrolla a través de las siguientes actividades:

1. Identificación del riesgo.
2. Análisis del riesgo.
3. Valoración del riesgo.
4. Monitoreo del riesgo.
5. Lineamientos sobre los riesgos relacionados con posibles actos de corrupción.
6. Lineamientos sobre riesgos de Seguridad de la Información.
7. Lineamientos sobre riesgos fiscales.

10. IDENTIFICACIÓN DEL RIESGO

Durante esta etapa se identificarán los riesgos que estén o no bajo el control de la organización para tal propósito se analizará el contexto estratégico de la Entidad y de igual manera el contexto interno y externo, determinando los factores que puedan generar riesgos que afecten el cumplimiento de la misionalidad de la Entidad y el cumplimiento de los objetivos.

La Entidad desarrollará las siguientes fases:

Análisis de Objetivos Estratégicos: Analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento. Deben estar alineados con la misión y visión institucional y se deben formular con metodología SMART (específico, medible, alcanzable, relevante y proyectado en el tiempo).

Análisis Objetivos de Procesos: Los objetivos de proceso deben ser analizados con base en características mínimas y deben contribuir a los objetivos estratégicos.

Identificación de puntos de Riesgo: Se identificarán aquellas actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo y deban mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Identificación de Áreas de Impacto: Entendida como la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que se definen son de orden económico y/o reputacional.

Identificación de Áreas de Factores de Riesgo: Consideradas como aquellas fuentes generadoras de riesgos. La Administración adoptará los factores de riesgo propuestos en la guía metodológica Versión No. 6 del DAFP, presentados en la siguiente tabla:

Tabla 3 Áreas factores de riesgo

Factor	Definición	Ícono	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.		Hurtos a activos
			Posibles comportamientos no éticos de los servidores públicos
			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 de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de la identidad
			Asalto a la oficina
			Atentados, vandalismo y orden público.

Fuente. Guía para la administración del riesgo versión 6 2022

En el caso de riesgos de la seguridad de la información se identificarán los siguientes tres (3) riesgos inherentes de seguridad de la información: Pérdida de la confidencialidad, pérdida de la integridad y pérdida de la disponibilidad, los cuales deberán ser asociados al grupo de activos específicos del proceso, analizando las posibles amenazas y vulnerabilidades que puedan originar su materialización. Para tal fin se adoptarán las herramientas metodológicas contenidas en el Anexo 4 del Modelo Nacional de Gestión de Riesgos de Seguridad de la Información para Entidades Públicas.

En el caso de riesgos fiscales se adoptará lo establecido en el capítulo 4 del documento Lineamientos para el Análisis de Riesgo Fiscal de la Guía para la Administración del Riesgo Versión 6 año 2022, donde se identificarán los puntos de riesgo fiscal y las circunstancias inmediatas, entendiendo los primeros como aquellas situaciones donde de acuerdo al Artículo 3 de la Ley 2010 de 2000, potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

Las circunstancias inmediatas se configuran como toda aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica (causa raíz) para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.
Es pertinente establecer las áreas de impacto que siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo, esto sin desconocer que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

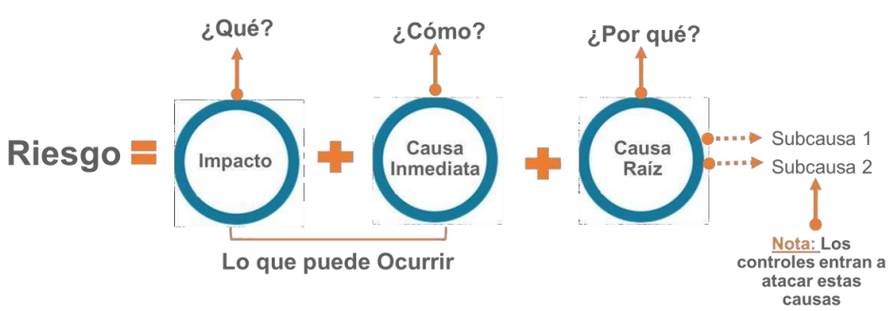
De igual manera dentro de la identificación de la causa raíz o potencial hecho generador se tendrá en cuenta lo que establece la guía. "Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntar a contrarrestar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales. Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador."

11. DESCRIPCIÓN DEL RIESGO

La descripción de los riesgos de gestión, de seguridad de la información y de seguridad y salud en el trabajo debe contener todos los detalles que sean necesario, asegurando que sean de fácil comprensión tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicie con la frase **POSIBILIDAD DE** y se analizan los siguientes aspectos:

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, corresponde a la razón por la cual se puede presentar el riesgo, es la base para la definición de controles. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa que pueden ser analizadas, pero explicará mejor el riesgo.

Ilustración 1 Formulación del riesgo de gestión



Fuente: Guía para la administración del riesgo Versión 6 2022

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

Los riesgos en la Alcaldía de Fusagasugá, se construirán de acuerdo a los procesos establecidos en el mapa de procesos, dando cumplimiento a los objetivos de la entidad y contemplando las siguientes premisas:

- No describir como riesgos omisiones ni desviaciones del control.
- No describir causas como riesgos.

- No describir riesgos como la negación de un control.

Tabla 4 Clasificación de riesgos

Clasificación de Riesgos		
Categoría		**Factores de Riesgo**
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.	Procesos
Fraude externo	Pérdidas derivadas de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	Evento externo
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos un participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.	Talento humano
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	Tecnología
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad	Factores varios
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.	Factores varios
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.	Infraestructura Evento externo

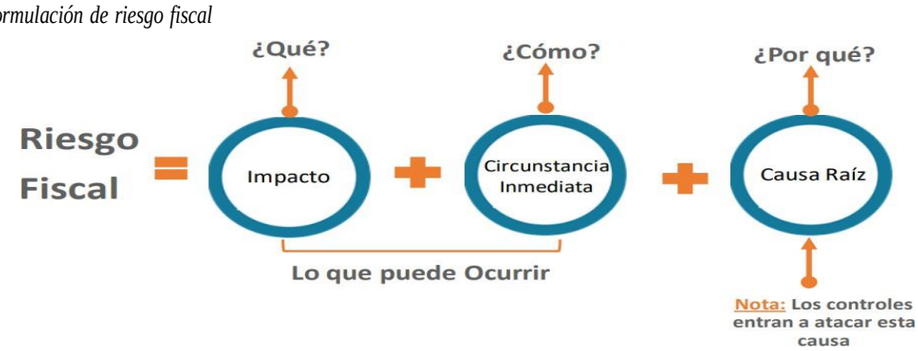
Fuente. Guía para la administración del riesgo versión 6 2022

En el caso de los riesgos fiscales se adoptarán los siguientes parámetros:

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

Por su parte, la estructura a utilizar para la redacción de riesgos fiscales será tal y como se presenta en la siguiente imagen:

Ilustración 2 Formulación de riesgo fiscal



Fuente. Guía para la administración del riesgo Versión 6 año 2022

Los riesgos de corrupción se formularán estableciendo los siguientes componentes:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

Es preciso indicar que en el caso de los riesgos de corrupción se deben cumplir las fases de identificación del contexto (Interno y Externo), determinar los factores generadores de riesgos de corrupción y construcción del riesgo, esta última requerirá realizar la identificación del proceso, el objetivo del proceso, establecer las causas, identificar los eventos de riesgo y sus consecuencias.

12. VALORACIÓN DEL RIESGO

Análisis del Riesgo

En la Entidad se adopta una metodología de expertos para realizar la etapa de análisis de los riesgos, en la cual los líderes de los procesos y demás personal de las dependencias, con base en su conocimiento y experiencia, realizan la revisión del contexto, la caracterización del proceso, su objetivo, alcance, puntos de riesgo y áreas de impacto. Con toda esta información definida se procede a determinar los valores más apropiados para las variables de probabilidad e impacto, con las cuáles se determinará el nivel de riesgo inherente para cada uno de los riesgos.

Determinación de la Probabilidad: La estimación de la probabilidad estará asociada a la posibilidad de ocurrencia del riesgo, debido a la cantidad de veces que se ve expuesto el proceso en el transcurso de un (1) año al pasar por el punto de riesgo. De tal forma que a mayor cantidad de veces se ejecuta una actividad susceptible de riesgo, mayor será la probabilidad de ocurrencia.

La Administración municipal establecerá la posibilidad de ocurrencia de los riesgos de gestión y seguridad de la información, corrupción y riesgos fiscales de acuerdo a los criterios establecidos en la guía de administración del riesgo de la función pública versión No. 6 como se observa en las siguientes tablas.

Tabla 5 Probabilidad de riesgo de Gestión, Seguridad de la información y fiscales

Probabilidad de riesgo de Gestión, seguridad de la información y Fiscales		
	Frecuencia de la Actividad	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de24 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 Versión 6 año 2022

Tabla 6 Probabilidad de Riesgos de corrupción

Probabilidad de riesgo de Corrupción			
Nivel	**Probabilidad**	**Frecuencia de la Actividad**	**Frecuencia**
1	Rara vez	El evento ocurre solo en circunstancias excepcionales.	No se ha presentado en los últimos cinco años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos cinco años.
3	Posible	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos dos años.
4	Probable	El evento puede ocurrir en la mayoría de las circunstancias.	Al menos una vez en el último año.
5	Casi seguro	El evento ocurre en la mayoría de las circunstancias.	Más de una vez en el año.

Fuente. Guía para la administración del riesgo. Versión 6 año 2022

Determinación del Impacto: Los impactos podrán ser de tipo económico y/o reputacional. Para definir el impacto de cada uno de los riesgos de gestión, de seguridad de la información y riesgos

fiscales, se tendrá en cuenta la tabla establecida en la Guía de Administración del Riesgo Versión 6 que se presenta a continuación:

Tabla 7 Calificación del impacto riesgos de gestión, seguridad de la información y riesgos fiscales

	Afectación Económica	Afectación 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. Versión 6, 2022.

En los riesgos de seguridad de la información, se tendrá en cuenta que la política de seguridad de la información se encuentra vinculada al Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: Seguridad de la Información, arquitectura, servicios ciudadanos digitales.

Para los riesgos de corrupción, se seguirán los lineamientos definidos por la Secretaría de Transparencia de la Presidencia de la República aplicando la siguiente tabla de valoración:

Tabla 8 Calificación del Impacto de riesgos de corrupción

Nivel	Impacto	Descripción	Respuestas afirmativas
1	Moderado	Genera medianas consecuencias sobre la Entidad	1 a 5
2	Mayor	Genera altas consecuencias sobre la Entidad	6 a 11
3	Catastrófico	Genera desastrosas consecuencias sobre la Entidad	12 a 19

Fuente. Guía para la Administración del Riesgo. Versión 6, 2022.

Cada riesgo de corrupción identificado es valorado de acuerdo con las preguntas de la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 9 preguntas orientadoras en la definición de riesgos de corrupción

No.	Pregunta	Respuesta	
	Si el riesgo de corrupción se materializa podría:	SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la Entidad?		
4	¿Afectar el cumplimiento de la misión del sector?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad, por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		

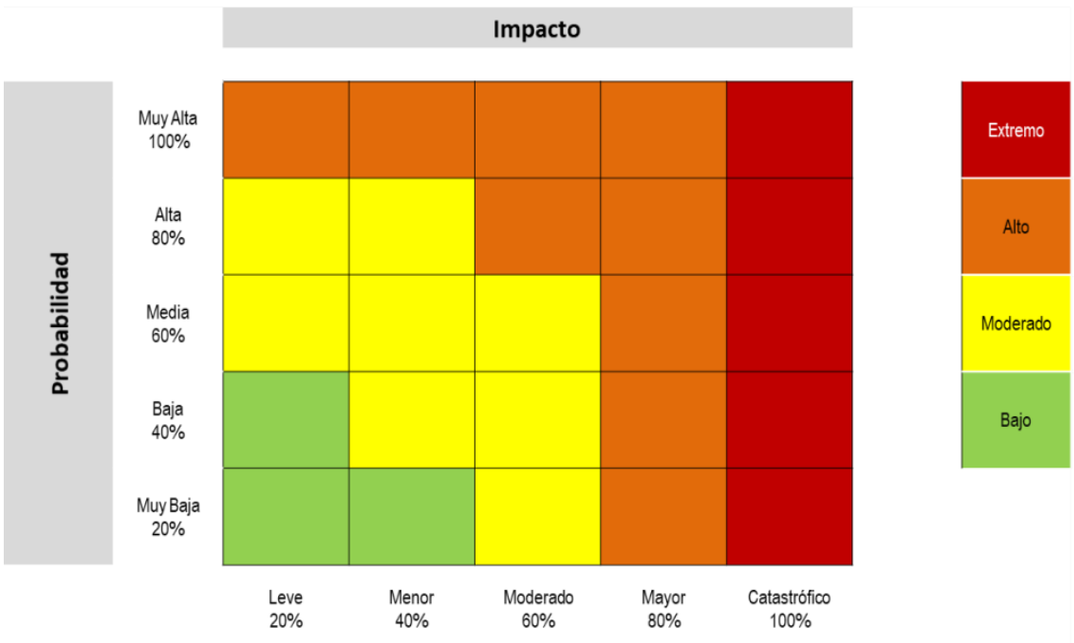
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Fuente. Guía para la Administración del Riesgo. Versión 6, 2022.

Determinación del Riesgo Inherente

Posterior a la definición de la probabilidad y el impacto, se debe determinar el valor resultante del riesgo inherente haciendo uso de los valores establecidos para cada una de estas variables, ubicándolos dentro de una matriz de calor, la cual contendrá cuatro niveles de riesgo cualitativo a saber: Bajo, Moderado, Alto y Extremo.

Tabla 10 Determinación del riesgo inherente



Fuente. Guía para la Administración del Riesgo. Versión 6, 2022.

13. NIVEL DE APETITO AL RIESGO

Para los riesgos de corrupción, la Entidad no es flexible en la aceptación de conductas o hechos de corrupción, por lo tanto, no hay aceptación del riesgo, su tratamiento se realizará de acuerdo con los lineamientos de esta política.

Para los riesgos fiscales, no hay un nivel de riesgo aceptable, toda vez que el objeto sobre el cual recae el efecto dañoso potencial, son los recursos, bienes y/o intereses públicos, siendo inaceptable cualquier nivel de aceptación sobre los mismos. Por lo tanto, la Entidad no es flexible en la aceptación de conductas o hechos que generen este tipo de riesgo, y su tratamiento debe orientarse a la prevención y mitigación de acuerdo con los lineamientos de esta política.

Para los riesgos de gestión y de seguridad de la información, la Entidad aceptará un nivel de riesgo residual en zona moderada. Por su parte, para los riesgos relacionados con seguridad y salud en el trabajo, la Entidad se acoge a los lineamientos de la Guía Técnica Colombiana GTC 45:2012 “Guía para la Identificación de los Peligros y la Valoración de los Riesgos en Seguridad y Salud en el Trabajo”, adoptando dentro de la escala el nivel de riesgo III (Aceptable) como se indica en la siguiente

tabla:

Tabla 11 nivel de aceptación de riesgos de SGSST

I	No Aceptable	Situación crítica. Suspender actividades hasta que el riesgo estébajo control. Intervención urgente.
II IIII	No aceptable o aceptable con control específico	Corregir y adoptar medidas de control de inmediato. Sin embargo, se debe suspender actividades si el nivel de riesgo está por encima o igual de 360 puntos.
III	Aceptable	Mejorar si es posible. Sería conveniente justificar la intervención ysu rentabilidad.
IV	Aceptable	Mantener las medidas de control existentes, pero se deberían considerar soluciones o mejoras y se deben hacer comprobacionesperiódicas para asegurar que el riesgo aún es aceptable.

Fuente: Guía para la identificación de los peligros y la valoración de los riesgos en salud ocupacional GTC 45 –

14. VALORACIÓN DE CONTROLES

- Es de recordar que los controles son acciones o medidas tomadas con el fin de dar tratamiento a los riesgos en procura de su prevención o mitigación.
- La identificación de controles se debe realizar a cada riesgo mediante la aplicación de entrevistas a los líderes de procesos y personal experto que interviene en el proceso.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

14.1 Estructura para la descripción del control

Para una adecuada redacción del control se propone una estructura que facilitará entender su tipología y otros atributos para su valoración.

- **Responsable de ejecutar el control:** Se identifica mediante el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará la herramienta, software o aplicativo con el que se realiza la actividad y el servidor que la utiliza.
- **Acción:** Se determina mediante el uso de verbos que indican las acciones que se deben realizar y que constituyen el control.
- **Complemento:** Corresponde a los detalles que contextualizan la situación y permiten identificar claramente el objeto del control.

14.2 Análisis y evaluación de controles

En la siguiente tabla se presentan los atributos de los controles, los atributos informativos permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos atributos no tienen una incidencia directa en su efectividad.

Tabla 12 Atributos para el diseño de los controles

Atributos para el Diseño de Controles				
Características			**Descripción**	**Peso**
Atributos de	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%

Eficiencia	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos Informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pesa a que se ejecutan en el proceso, no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente. Guía para la administración del riesgo Versión 6 año 2022

Una vez se aplican los controles durante la ejecución de los procesos, se debe obtener un resultado de disminución del nivel de riesgo como consecuencia del desplazamiento de los valores en los ejes de probabilidad y/o impacto para cada uno de los riesgos identificados, tras lo cual se obtendría el nivel de riesgo residual a través del cual se prioriza el tratamiento de los riesgos.

En los riesgos asociados a la seguridad de la información, las entidades públicas podrán dar tratamiento a los riesgos de información, empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “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.

15. TRATAMIENTO DE RIESGOS

A continuación, se describen las opciones con las que se puede dar tratamiento a los riesgos.

- **Aceptar el Riesgo:** Consiste en aceptar la probable pérdida, lo cual está enmarcado dentro del rango de apetito al riesgo de la Entidad, es decir, el riesgo se encuentra en un nivel que es aceptado por la misma, sin embargo, el líder del proceso deberá realizar un seguimiento a los controles existentes de su mapa de riesgos, sin que esto genere acciones distintas a las existentes con el fin de fomentar lecciones aprendidas.
- **Reducir el Riesgo:** Implica implementar controles orientados a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas de protección), con el fin de llevar los riesgos ubicados en zona alta y extrema a la zona baja o moderada que son aquellos que asume la Entidad.
  Después de realizar un análisis y considerar que el nivel de riesgo es alto, se establecerá un plan de acción que determinará tratarlo mediante transferencia o mitigación del riesgo.
  La transferencia consiste en tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas, de esta manera la responsabilidad económica podrá recaer también sobre el tercero, sin embargo, con esto no se transfiere el impacto reputacional.
  La mitigación por su parte, consistirá en la implementación de acciones que mitiguen el nivel de riesgo ya sea dirigidas a disminuir la probabilidad de ocurrencia y/o el impacto.
- **Evitar el Riesgo:** Implementar medidas para prevenir la materialización de los riesgos siendo necesario eliminar o dejar de realizar la actividad susceptible de riesgo. Este tipo de determinaciones deben ser soportadas por escrito en donde se evidencie la respectiva aprobación por la instancia idónea.

16. HERRAMIENTAS PARA LA GESTIÓN DE RIESGOS

Para las fases correspondientes al análisis, identificación, valoración y administración de los riesgos

institucionales, los Líderes de los Procesos de Direccionamiento Estratégico, GestiónTIC y Gestión del Talento Humano establecerán las herramientas de gestión de los riesgos de conformidad a su compromiso y responsabilidad en la Segunda Línea de Defensa. Para este fin se tienen establecidas las siguientes herramientas.

Matriz de Riesgos FO-DE-022 aplicable a los riesgos de corrupción.

Mapa de Riesgos FO-DE-044 aplicable a los riesgos de gestión y fiscales.

Formato Reporte de Eventos de Riesgo FO-DE-063 para el registro de los casos de materialización de riesgos.

Procedimiento de reporte de evento de riesgo PR-DE-018

Mapa de Riesgos de Seguridad de la Información FO-GT-014 para la identificación, clasificación y tratamiento de Riesgos de Seguridad de la Información, de conformidad al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Matriz de Identificación de Peligros, Evaluación y Valoración de Riesgos FO-GTH-050, la que se encuentra armonizada con el Plan de Seguridad y Salud en el Trabajo del Proceso Gestión del Talento Humano.

17. ACCIONES ANTE LA MATERIALIZACIÓN DE RIESGOS

Cuando se materializan riesgos identificados en los mapas de riesgos de la Entidad, se aplicarán las acciones descritas en la siguiente tabla:

Tabla 13 Acciones de respuesta a riesgos

Acciones de Respuesta a Riesgos		
Tipo de Riesgo	**Responsable**	**Acción**
Riesgos de Corrupción	Líder de proceso	Informar a la Oficina de Desarrollo Organizacional sobre los riesgos materializados según lo establecido en el componente de Seguimiento y Monitoreo haciendo uso del formato para el reporte de eventos de riesgo.
		Realizar análisis de la situación sobre las causas que generaron la materialización del riesgo.
	Oficina de Control Interno	Identificar, documentar y tomar las acciones correctivas, teniendo en cuenta el impacto del riesgo materializado, en el formato de Plan de Mejoramiento FO-CSG-013.
		Si dentro del seguimiento realizado a los riesgos de corrupción, la Oficina de Control Interno identifica que se han materializado uno o más riesgos, las acciones requeridas son las siguientes: a) Convocar al Comité Institucional de Coordinación de Control Interno para informar sobre los hechos detectados, donde se tomarán las decisiones para iniciar la investigación de los hechos. b) Una vez surtido el conducto regular establecido por la Entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia correspondiente. c) Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. d) Verificar la definición de acciones correctivas en el formato Plan de Mejoramiento FO-CSG-013 y la actualización del mapa de riesgos correspondiente.
		Informar a los líderes de proceso involucrados para que realicen el análisis de la situación y definan las acciones a que haya lugar.
		Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso para que brinden apoyo en la revisión del mapa de riesgos.
		Proceder de manera inmediata aplicando el plan de contingencia o de tratamiento de incidentes de Seguridad de la Información que permita la continuidad del servicio o el restablecimiento del mismo y crear el respectivo plan de mejoramiento en el formato FO-CSG-013.

Riesgos de Gestión, Seguridad de la información, y riesgos fiscales	Líder de proceso	Todo incidente de Ciberseguridad deberá ser reportado, siguiendo el procedimiento PR- GT-006 Versión 1, a través de la plataforma GLPI del Proceso de Gestión TIC.
		Informar a la Dirección de Desarrollo Organizacional sobre los riesgos materializados según lo establecido en el componente de Seguimiento y Monitoreo haciendo uso del formato para el reporte de eventos de riesgo.
		Iniciar el análisis de causas y determinar acciones preventivas y de mejora a documentar mediante Plan de Mejoramiento en el formato FO-CSG-013 y replantear los riesgos del proceso.
		Analizar y actualizar el mapa de riesgos correspondiente.
		Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.
	Oficina de Control Interno	Informar al líder del proceso sobre el hecho encontrado.
		Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso para revisar el mapa de riesgos.
		Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.
		Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.
Riesgos de Seguridad y Salud en el Trabajo	Líder de proceso	Reportar a la Dirección de Gestión del talento humano los accidentes o enfermedades laborales presentados con los colaboradores de la Entidad, de acuerdo al instrumento establecido.
		Realizar análisis de la situación sobre las causas que generaron el accidente o enfermedad laboral.
		Implementar las medidas correctivas necesarias para evitar la materialización de riesgos.
		Revisar y actualizar el mapa de riesgos correspondiente y sus controles asociados.

Elaboración Propia.

18. ESTRATEGIAS PARA LA ACEPTACIÓN DEL RIESGO RESIDUAL

Estrategias de tratamiento de riesgo		
Tipo de riesgo	**Zona de riesgo residual**	**Estrategia de tratamiento controles asociados**
Riesgos de gestión, seguridad digital	Baja	Se ACEPTA el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza reporte mensual de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad o el impacto de ocurrencia del riesgo, se hace seguimiento BIMESTRAL y se registran sus avances en la matriz de riesgos.
	Alta y extrema	Se debe incluir el riesgo en el mapa de riesgos por proceso, y se establecen acciones de control preventivas que permitan EVITAR la materialización del riesgo. Se monitorea MENSUALMENTE y se registra en la matriz de riesgos.
Riesgos de corrupción y fiscales	Ningún riesgo de corrupción ni riesgo fiscal podrá ser aceptado, la periodicidad de seguimiento será MENSUAL, para evitar a toda costa materialización por parte de los procesos a cargo de estos.	

19. MONITOREO Y REVISIÓN

En aplicación del modelo de las líneas de defensa, la gestión de riesgos contará con una etapa de monitoreo en cabeza de los procesos pertenecientes a la primera y segunda línea. Su propósito es desarrollar actividades de supervisión continua en el día a día de las actividades y el mantenimiento

efectivo de controles internos, además de supervisar la eficacia e implementación de las prácticas de gestión de riesgos. Por lo tanto, las actividades de monitoreo no estarán sujetas a una periodicidad específica ya que su ejecución se enmarca en un contexto de ciclo continuo.

En esta etapa, el líder del proceso con el apoyo de las dependencias integrantes de la segunda línea de defensa, en conjunto con su equipo de trabajo y el acompañamiento de la Dirección de Desarrollo Organizacional, analizarán los resultados del monitoreo y revisión con el fin de identificar desviaciones, establecer tendencias, generar alertas y/o emitir recomendaciones con base en información clave que permita la toma de decisiones para la ejecución de acciones que orienten a la Alta Dirección y al personal de la primera línea de defensa.

Los líderes de los procesos son responsables en igual medida desde su rol de realizar, como actividad de autocontrol, el monitoreo permanente al comportamiento de los Riesgos de Gestión, Corrupción, Seguridad de la Información, de Seguridad y Salud en el Trabajo y Riesgos Fiscales, la implementación de los controles y acciones, verificando su efectividad, lo cual deberá quedar registrado mediante actas de reuniones internas en formato FO-DE-027 V3.

Se debe dejar registro del desarrollo de cada actividad puntual de monitoreo que se realice desde cada uno de los procesos, a través de actas, listados de asistencia a reuniones, mesas de trabajo, oficios o envío de correos electrónicos y reportes de eventos de riesgo, entre otros según el caso a tratar. Estos documentos constituyen la evidencia del cumplimiento de las actividades asociadas al rol designado.

Si durante el monitoreo realizado a los Riesgos de Gestión, Corrupción, Seguridad de la Información y riesgos fiscales se genera actualización del Mapa de Riesgos, esta deberá reportarse a la Dirección de Desarrollo Organizacional mediante comunicación efectuada por el Sistema de Gestión Documental ControlDoc, con su respectivo documento soporte en donde se evidencien las causales de las decisiones tomadas.

Para los riesgos de Seguridad y Salud en el Trabajo, la identificación de peligros y evaluación de los riesgos, se realiza en la herramienta desarrollada por la Entidad, la cual deberá ser documentada y actualizada:

- Como mínimo una vez al año.
- Cada vez que ocurra un accidente de trabajo mortal.
- Cada vez que ocurra un evento catastrófico.
- Cuando se presenten cambios relevantes en los procesos, en las instalaciones, en la maquinaria o en los equipos.

El líder del proceso de Gestión de Talento Humano reportará a la Dirección de Desarrollo Organizacional, mediante comunicación escrita por el Sistema de Gestión Documental ControlDoc, la gestión de los riesgos de Seguridad y Salud en el Trabajo realizada durante cada periodo trimestral con corte al 31 de marzo, 30 de junio, 30 de septiembre y 31 de diciembre de cada vigencia. La entrega de la información deberá producirse dentro de los primeros diez (10) días hábiles siguientes a las fechas de corte trimestral.

Para los casos de materialización de riesgos de Seguridad y Salud en el Trabajo y en particular los relacionados con accidentes de trabajo mortales y/o catastróficos, el reporte se realizará dentro de los cinco (5) días hábiles siguientes a la realización del evento.

20. SEGUIMIENTO Y EVALUACIÓN

Corresponderá a la Oficina de Control Interno en su rol de tercera línea de defensa la actuación en

esta etapa con el fin de proporcionar aseguramiento objetivo e independiente sobre la gestión de riesgos, así como pronunciarse sobre la efectividad de los controles para evitar la materialización de los riesgos.

La periodicidad de los seguimientos a los Riesgos de Gestión, Fiscales, de Seguridad de la Información y de Seguridad y Salud en el Trabajo será trimestral con corte en los meses de marzo, junio, septiembre y diciembre de cada año. Por su parte, los seguimientos a los Riesgos de Corrupción serán cuatrimestrales, a efectuarse en los meses de abril, agosto y diciembre, ajustándose a la normativa actual vigente en la materia.

Producto de la realización de los seguimientos periódicos, la Oficina de Control Interno generará informes de seguimiento y evaluación con base en la información de gestión de riesgos y evidencias relacionadas con los planes de acción establecidos en los respectivos mapas de riesgos. La información objeto de seguimiento y evaluación será reportada directamente a la Oficina de Control Interno desde cada una de las dependencias responsables de procesos en la Entidad.

El líder de proceso junto con el delegado de riesgos analiza los resultados del seguimiento y establecen acciones inmediatas ante cualquier desviación. Procederán a comunicar las desviaciones al interior de su dependencia e impartirán las directrices necesarias para la ejecución de las acciones a implementar.

21. REVISIÓN DE RIESGOS INSTITUCIONALES

La revisión de los riesgos será realizada sobre los mapas de riesgos vigentes, validando la pertinencia de la información e ingresando los nuevos riesgos identificados de acuerdo con la metodología provista por el Departamento Administrativo de la Función Pública. Se debe garantizar el cumplimiento de una revisión general a los mapas de riesgos de la Entidad como mínimo una vez cada año, dejando registro de las actividades asociadas al proceso de actualización, teniendo en cuenta los riesgos materializados y los cambios derivados del análisis del contexto en articulación con los objetivos estratégicos.

22. COMUNICACIÓN Y CONSULTA

La Dirección de Desarrollo Organizacional articulará con el Proceso de Comunicación Pública, las estrategias para la difusión de la Política de Administración de Riesgos y se implementará en coordinación con cada Jefe de Oficina, Secretario de Despacho y Director.

Así mismo, La Dirección de Desarrollo Organizacional, coordinara con el Proceso de Comunicación Pública la actualización en la página web de la Alcaldía de Fusagasugá, los Mapas de Riesgos de gestión por procesos, de seguridad de la información, de seguridad y salud en el trabajo, de corrupción y fiscales.

23. CONTROL DE CAMBIOS

Versión	Fecha de Versión	Descripción del cambio
1	31/01/2023	Formulación de política de Administración del Riesgo
2	17/03/2023	Ajuste del Marco Normativo
3	30/01/2024	Ajuste del Marco Normativo, adaptación a la Versión No. 6 de la guía de administración del riesgo 2022, se incluye el componente de riesgos fiscales.
4	14/02/2025	Ajuste del documento en cuanto a responsabilidades, roles y funciones, uso de conceptos, documentos con base en la normativa vigente.