Gobernación de CUNDINAMARCA	POLÍTICA	CÓDIGO: E-PID-POL-002
		VERSIÓN: 6
Política Administración de Riesgos		FECHA: 22/Abr/2021

INTRODUCCIÓN

Como parte de las actividades de fortalecimiento institucional y de mejora continua que adelanta la Gobernación de Cundinamarca, se genera una nueva versión de la Política de Administración de Riesgos, con la cual se reafirma el compromiso de la alta dirección con la generación de nuevas herramientas metodológicas para contribuir a una óptima gestión de los riesgos. Lo que permite, no solamente fortalecer el Sistema Integral de Gestión y Control -(SIGC), sino que a la vez, contribuye a facilitar la implementación del Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Control Interno (SCI).

La nueva Política de Administración de Riesgos establece los lineamientos para darle tratamiento, manejo y seguimiento a los riesgos de la Entidad. Alineada con el modelo integrado de planeación y gestión, las líneas de defensa para la efectiva administración de riesgos para su cumplimiento y se articula con los riesgos de gestión, corrupción y seguridad digital.

La Política de Administración de Riesgos, es extensible y aplicable a todos los procesos de la Gobernación de Cundinamarca; y en conjunto con la Guía para la Administración para la Gestión de Riesgos Código: E-PID-GUI-013, establecen los lineamientos para definir los niveles de aceptación del riesgo, clasificación del impacto y posibilidad de materialización, producto del análisis de la dinámica y complejidad organizacional, de los riesgos de operación, los recursos humanos y físicos con los que cuenta la Entidad, la capacidad financiera y los grupos de interés.

Para la Gobernación de Cundinamarca es de fundamental importancia continuar con la adecuada implementación del Modelo Integrado de Planeación y Gestión - MIPG y su ejercicio continuo de generación de valor por medio del Sistema Integral de Gestión y Control – SIGC y el Sistema de Control Interno, con la seguridad que estos sistemas articulados y sincronizados, permitirán una efectiva y oportuna prestación de servicios a la ciudadanía.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

El objetivo del presente documento es el de establecer los lineamientos metodológicos para la administración, gestión, control y monitoreo de riesgos, su adecuado tratamiento, manejo, seguimiento y evaluación del riesgo en la Gobernación de Cundinamarca, en el marco del Modelo Integrado de Planeación y Gestión (MIPG), el Sistema Integral de Gestión y Control (SIGC) y el Sistema de

Control Interno (SCI), aportando al cumplimiento del Plan Departamental de Desarrollo.

El objetivo de la Política de Administración de Riesgos de la Entidad es identificar, valorar y reducir los riesgos que puedan afectar la operación de la Gobernación de Cundinamarca y el cumplimiento de sus objetivos estratégicos, enmarcados en el Plan Departamental de Desarrollo, mediante el diseño y ejecución de controles que prevengan, detecten o mitiguen la probabilidad e impacto de situaciones adversas.

1.2 OBJETIVOS ESPECÍFICOS

- Definir mecanismos de prevención frente a posibles riesgos materializados, protegiendo los recursos e imagen de la Entidad y minimizando las causas que afecten la gestión de los procesos.
- Fortalecer el compromiso de todos los colaboradores, servidores públicos y contratistas de la Gobernación de Cundinamarca, en el oportuno tratamiento de los riesgos mediante controles y acciones encaminadas a prevenir los efectos adversos y la materialización.
- Establecer la administración de riesgos como una herramienta confiable para la planeación institucional y soportar la toma de decisiones.
- Asegurar la continua prestación de los trámites y servicios a cargo de la Gobernación.
- Utilizar en forma correcta los bienes y recursos de la entidad.
- Salvaguardar los bienes del Departamento.
- Evitar o mitigar cualquier pérdida económica que pueda originarse en el desarrollo de las actividades.
- Propiciar la confiabilidad y oportunidad de la información
- Evitar la desviación de la gestión hacia beneficios particulares

2. ALCANCE

Esta política define los lineamientos para la gestión y administración, control y monitoreo de los riesgos de gestión, corrupción y seguridad de la información de la Gobernación de Cundinamarca en el marco del Modelo Integrado de Planeación y Gestión, el Sistema Integral de Gestión y Control y el Sistema de Control Interno. Contemplando la construcción del mapa de riesgos, comunicación, priorización, seguimiento, monitoreo, revisión y actualización para la gestión integral de los riesgos. Garantizando un manejo sistemático, articulado y transversal; aplica a todos los niveles organizacionales y a la totalidad de los procesos del nivel central, que conforman el SIGC.

3. 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.

Ley 489 de 1998. Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional.

Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Función Pública.

Guía para la Gestión del Riesgo de Corrupción. Secretaría de Transparencia. 2015

Decreto Nacional 648 de 2017. Por medio del cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector Función Pública.

Decreto Nacional 338 de 2019. Por medio del cual se modifica el Decreto 1083 de 2015, Reglamentario Único del Sector Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción.

Guía de Roles de las Unidades u Oficinas de Control Interno, Auditoría Interna o quien haga sus veces. Diciembre de 2018.

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP, versión 5, 2020. El Departamento Administrativo de la Función Pública en este documento pone a disposición de las entidades nacionales y territoriales la metodología para la administración del riesgo.

Decreto Ordenanzal 437 de 2020. "Por medio del cual se establece la estructura de la administración pública departamental, se define la organización interna y las funciones de las dependencias del sector central de la administración pública de Cundinamarca y se dictan otras disposiciones".

NTC ISO 9001:2015. Sistema de Gestión de la Calidad. Requisitos.

NTC ISO 14001:2015. Sistemas de Gestión Ambiental. Requisitos con orientación para su uso.

NTC ISO 27001: 2013. Sistemas de Gestión de Seguridad de la Información.

NTC ISO 31000:2018. Gestión del riesgo. Principios y Directrices.

NTC ISO 45001:2018. Sistemas de Gestión de Seguridad y Salud en el Trabajo.

4. GLOSARIO

Definiciones tomadas de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP 2020, Guía para la Gestión del Riesgos de Corrupción – Secretaría de Transparencia 2015 y NTC ISO 14001: 2015.

Administración del Riesgo: Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.

Actividades De Control: Son las acciones establecidas a través de políticas (establecen las líneas generales del control interno.) y procedimientos (son los que llevan dichas políticas a la práctica.) que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

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.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis de Riesgos: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

Apetito del Riesgo: Nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y el Órgano de Gobierno. Puede ser diferentes para los distintos tipos de riesgos que la entidad desea gestionar.

Capacidad de Riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar 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.

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

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.

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

Consecuencias: 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: Medida que permite reducir o mitigar el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Control Correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Control Preventivo: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

Control Detectivo: Controles que se generan durante la ejecución del proceso. Detectan la situación no deseada o riesgo para que se

corrija y se tomen las acciones correspondientes.

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

Evento: Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Frecuencia: Periodicidad con que ha ocurrido un evento.

Identificación del Riesgo: Descripción de la situación no deseada.

Impacto: Las consecuencias o efectos que pueden ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de riesgos: Herramienta metodológica que permite hacer un inventario de los riesgos por proceso, haciendo la descripción de cada uno de ellos, las posibles consecuencias y su forma de tratamiento.

Monitoreo de los mapas de riesgos: Es el seguimiento permanente a la eficacia de las acciones programadas en los planes de manejo con los que cuentan los mapas de riesgos de los diferentes procesos. El mapa de riesgos debe ser revisado de manera periódica ya que el panorama de riesgos cambia constantemente, y se debe revisar si se debe actualizar o modificar el mapa.

Nivel de Riesgo: Valor que se determina a partir de la combinación de 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.

Políticas de Riesgo: Son los criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad, en función de su evaluación.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo, estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. Esta puede ser medida con criterios de Frecuencia (Número de eventos en un periodo determinado) o Factibilidad (Se analiza la presencia de factores internos y externos que pueden propiciar el riesgo).

Probabilidad Inherente: será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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 Ambiental: Eventos que pueden ocasionar incumplimientos en el tratamiento de los aspectos ambientales, objetivos ambientales y demás directrices para prevenir impactos adversos al medio ambiente por las actividades que adelantan las dependencias y entidades de la Gobernación de Cundinamarca.

Riesgo de Gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

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

Riesgo de Fraude: (externo): Pérdida derivada de actos de fraude por personas ajenas a la Entidad.

Riesgo de 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.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

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 la combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para para modificar su probabilidad o impacto, es el nivel de riesgo propio de la actividad. La combinación de la probabilidad con el impacto, nos permite determinar el nivel de riesgo inherente dentro de unas escalas de severidad.

Riesgo Residual: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento, es decir, 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.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. ADMINISTRACIÓN DE RIESGOS

La Gobernación de Cundinamarca tiene un firme compromiso con la adecuada administración de los riesgos en cuanto a su identificación, análisis, valoración y el establecimiento de las acciones de contingencia de aquellos eventos que puedan afectar los objetivos estratégicos y la adecuada prestación de servicios.

Poniendo al alcance de todos los procesos de la Entidad las herramientas necesarias que con el apoyo y participación de los servidores públicos, contratistas y colaboradores promoverá la integridad que permita controlar y responder a los acontecimientos potenciales o aquellos en los que puedan generar situaciones de riesgo.

La metodología se ajusta a la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública (DAFP) y el trabajo articulado de las Secretarías de la Función Pública, Planeación y la Oficina de Control Interno. Su gestión se realiza por medio de la herramienta tecnológica destinada para tal fin a cargo de la Dirección de Desarrollo Organizacional de la Secretaría de la Función Pública de la Gobernación de Cundinamarca; su operatividad se da por medio de la presente Política de Administración del Riesgo, documentada en la Guía para la Gestión de Riesgos Código: E-PID-GUI-013.

6 ELEMENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.

En la administración de los Riesgos de la Gobernación de Cundinamarca, se consideran los siguientes elementos que permiten su eficiente gestión:

6.1 Política de Administración de Riesgos (Lineamientos de la Política)
6.2 Identificación de Riesgos:
6.2.1 Establecimiento del Contexto (Interno, Externo, Identificación de activos).
6.2.2 Identificación de Riesgos (Tipología de Riesgos)
6.2.3 Análisis de Causas
6.3 Valoración de Riesgos
6.3.1 Análisis de Riesgos (Análisis de Impacto)
6.3.2 Evaluación de Riesgos (Riesgo Inherente, valoración de los controles, Riesgo Residual)
6.3.3 Monitoreo y Revisión (Responsabilidades-Líneas de Defensa)
6.3.4 Seguimiento (Reportes Periódicos).
6.4. Comunicación y Consulta

7. NIVELES DE ACEPTACIÓN AL RIESGO

Son los niveles que la Entidad está dispuesta a aceptar relacionada con los objetivos, el marco legal y las disposiciones de la alta dirección que debe o desea gestionar. Los niveles de aceptación al riesgo son:

Tabla 1. Niveles de Aceptación

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
	Baja	**ACEPTAR EL RIESGO:** no se adoptará ninguna medida que afecte la probabilidad o el impacto del riesgo, haciendo un monitoreo periódico al riesgo. (Esta Zona de Riesgo sólo aplica para Gestión y Seguridad Digital **NINGÚN Riesgo de Corrupción es aceptable**).
	Moderada	Se adoptan medidas para **REDUCIR** la probabilidad o el impacto del riesgo o ambos, generalmente conlleva a la implementación de

	[illegible]	[illegible] controles, realizando un monitoreo periódico al riesgo y sus controles.
Riesgos de Gestión por Procesos y Riesgos de Seguridad Digital	**Alta y Extrema**	Se adoptan medidas para **REDUCIR** o **EVITAR** el riesgo, mediante el re-diseño del proceso, la cancelación o abandono de las actividades que dan lugar al riesgo es decir, no iniciar o no continuar con la actividad que lo provoca (No hay riesgos después de tomar medidas de tratamiento). Si es muy difícil para la entidad reducir el riesgo a un nivel aceptable: **COMPARTIR** el riesgo, reduciendo la probabilidad o el impacto y se transfiere parte del riesgo. Ejemplo: Seguros o Tercerización (los mecanismos de transferencia del riesgo deben estar formalizados a través de un acuerdo contractual). Al compartir el Riesgo: **No se transfiere la responsabilidad, si el riesgo.**
Riesgos de Corrupción	**Moderada**	**REDUCIR, EVITAR o COMPARTIR** Se adoptan medidas para **REDUCIR** la probabilidad o el impacto del riesgo o ambos, generalmente conlleva a la implementación de controles, realizando un monitoreo periódico al riesgo y sus controles. **EVITAR** el riesgo, mediante el re-diseño del proceso, la cancelación o abandono de las actividades que dan lugar al riesgo es decir, no iniciar o no continuar con la actividad que lo provoca (No hay riesgos después de tomar medidas de tratamiento). Si es muy difícil para la entidad reducir el riesgo a un nivel aceptable: **COMPARTIR** el riesgo, reduciendo la probabilidad o el impacto y se transfiere parte del riesgo. Ejemplo: Seguros o Tercerización (los mecanismos de transferencia del riesgo deben estar formalizados a través de un acuerdo contractual). Al compartir el Riesgo: **No se transfiere la responsabilidad, si el riesgo.**
		REDUCIR, EVITAR o COMPARTIR Se adoptan medidas para **REDUCIR** la probabilidad o el impacto del riesgo o ambos, generalmente conlleva a la implementación de controles, realizando un monitoreo periódico al riesgo y sus controles.

	Alta Extrema	**EVITAR** el riesgo, mediante el re-diseño del proceso, la cancelación o abandono de las actividades que dan lugar al riesgo es decir, no iniciar o no continuar con la actividad que lo provoca (No hay riesgos después de tomar medidas de tratamiento). Si es muy difícil para la entidad reducir el riesgo a un nivel aceptable: **COMPARTIR** el riesgo, reduciendo la probabilidad o el impacto y se transfiere parte del riesgo. Ejemplo: Seguros o Tercerización (los mecanismos de transferencia del riesgo deben estar formalizados a través de un acuerdo contractual). Al compartir el Riesgo: **No se transfiere la responsabilidad, si el riesgo.**

8 NIVELES DE AUTORIDAD Y RESPONSABILIDAD

Los roles y responsabilidades se definen teniendo en cuenta la estructura organizacional, las funciones descritas en el Decreto Ordenanzal 437 de 2020 y lo sugerido en la Guía para la Administración de Riesgos del DAFP. Determinando que los siguientes niveles de estructura en la administración del riesgo son de carácter participativo con los líderes de procesos, en el cual se determinan los siguientes niveles de autoridad y responsabilidad:

LÍNEA DE DEFENSA ESTRATÉGICA	
INTEGRANTES	Gobernador, Secretarios, Gerencia de buen Gobierno, Comité de Coordinación de Control Interno, Comité Institucional de Gestión y Desempeño
DESCRIPCIÓN	Se encarga de definir el marco general para la administración de riesgos, control y supervisión de su cumplimiento, establecer los lineamientos que se aplicarán en todos los procesos para la adopción y apropiación de la Política de Administración de Riesgos; verificar los cambios del entorno, modificaciones en el direccionamiento estratégico y realizar las modificaciones necesarias verificar el cumplimiento de la Política de Administración de Riesgos, de manera periódica y evaluar su impacto

	impacto.
FUNCIONES	Realizar el seguimiento en el comité institucional de coordinación de control interno, a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por control interno y auditoría interna. Emitir lineamientos a los procesos para la identificación y valoración de los riesgos institucionales y de corrupción así como las acciones de contingencia que se requieran. Identificar y mitigar los riesgos frente a los planes estratégicos.

PRIMERA LÍNEA DE DEFENSA	
INTEGRANTES	Líderes de proceso, Equipos de mejoramiento de los procesos colaboradores, funcionarios y contratistas
DESCRIPCIÓN	Será responsabilidad de los líderes de proceso y de sus equipos de trabajo aplicar el conocimiento técnico sobre la misión de cada proceso para generar una debida administración del riesgo por medio de la identificación de riesgos, análisis, valoración, monitoreo y generación de acciones de mejora.
FUNCIONES	Aplicar los lineamientos establecidos por la línea defensa estratégica para la administración del riesgo. Diseñar y ejecutar los controles establecidos para la mitigación de los riesgos. Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño e identificar en caso de que no estén cumpliendo los posibles riesgos que se están materializando en el cumplimiento de los objetivos. Revisar y reportar a la dirección de desarrollo Organizacional los eventos de riesgos que se han materializado en la entidad incluyendo los riesgos de corrupción, así como las causas que den origen a esos eventos de

	riesgos materializados, como aquellas que estén ocasionando que no se logre el cumplimiento de los objetivos y metas a través del análisis de indicadores asociados a dichos objetivos. 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 la repetición del evento y lograr el cumplimiento a los objetivos. Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, con la segunda y la tercera línea de defensa con relación a la gestión de riesgos.

SEGUNDA LÍNEA DEFENSA	
INTEGRANTES	Secretaría de la función pública - Dirección de Desarrollo Organizacional, Gerencia de Buen Gobierno. Los secretarios y directores líderes de los procesos transversales.
DESCRIPCIÓN	Línea de defensa que soportarán y guiarán en la línea estratégica y la primera línea de defensa en la gestión adecuada de los riesgos, que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo a la gestión de riesgos.
FUNCIONES	Verificar de manera constante los cambios en el direccionamiento estratégico, del entorno y cómo éstos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgo. La revisión de la adecuada definición, el desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base, para llevar a cabo la identificación de los riesgos y realizar las recomendaciones a que haya lugar. Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de

	los mismos. Revisar el perfil de riesgo inherente y residual por cada proceso y consolidarlo. Pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la entidad. Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. 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 vuelvan a materializar el riesgo y lograr el cumplimiento de los objetivos. Verificar de manera constante los cambios en el direccionamiento estratégico, en el entorno y cómo éstos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.

TERCERA LÍNEA DE DEFENSA	
INTEGRANTES	Oficina de Control Interno
DESCRIPCIÓN	Realizar evaluación y aseguramiento independiente sobre la gestión del riesgo en la entidad, catalogada como una unidad auditable, más dentro de su universo de auditoría y por lo tanto debe dar a conocer a toda la entidad el Plan Anual de Auditorías, basado en riesgos y los resultados de la evaluación de la gestión del riesgo.
FUNCIONES	Verificar y analizar la idoneidad de los controles establecidos en los procesos, determinados y si son o no adecuadas para prevenir y mitigar los riesgos de procesos. Realizar seguimiento a los riesgos consolidados en los mapas de riesgos. Reportar el seguimiento a los riesgos identificados asesorando en

	metodologías para la identificación y administración de los riesgos en coordinación con la segunda línea de defensa. Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno durante las evaluaciones. Generar a través de su rol de asesoría una orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces.

9. PERIODICIDAD DE REVISIÓN

La segunda línea de defensa realizará el seguimiento de los mapas de riesgos así:

Riesgos de gestión: Dirección de Desarrollo Organizacional, riesgos de seguridad de la información: Secretaría de Tecnologías de la Información Tics, acompañarán la identificación de riesgos, su valoración y el establecimiento de controles además de manera trimestral realizará el seguimiento al cumplimiento de las actividades de control establecidas. Para los riesgos de corrupción la segunda línea de defensa será ejercida por la Gerencia de Buen Gobierno y la Secretaría de Planeación y su seguimiento será ejercido de manera cuatrimestral.

NOTA: Para los riesgos de corrupción que se materialicen, debe informarse de manera inmediata a la Oficina de Control Interno, y Control Interno Disciplinario y a su vez a la alta dirección y los entes de control respectivos, además el seguimiento se realizará de manera permanente, incrementando su valoración a rango catastrófico y replanteando los controles y actividades de control para que no se vuelva a materializar

10.DIVULGACIÓN

La Política de Administración del riesgo se dará a conocer en todos los niveles de la entidad, mediante canales formales y estrategias de comunicación existentes como son: correos institucionales, intranet, carteleras virtuales, así como las generadas por los procesos, como entrenamiento y asistencia técnica, talleres, capacitaciones, inducción y re inducción, entre otros. Adicional estará disponible para consulta en el aplicativo o herramienta tecnológica utilizada por la Entidad.

LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	05/Mar/2014	Creación del documento
2	13/Jun/2014	Modificación de la política por actualización del Modelo Estándar de Control Interno MECI 2014. Política aprobada mediante acta de comité coordinador del sistema de control interno del 13 de Junio de 2014.

3	27/Jul/2015	• Se incluye alcance a la política. • Adecuación de la política general de manera que se estipulen las directrices que guiaran la administración de riesgos, basándose en planes estratégicos y objetivos de la entidad. • Se incluye calificación de los impactos en los procesos. • Se ajusta la periodicidad del monitoreo a los riesgos y sus controles. Se actualiza la Política por la adopción de los lineamientos de la Guía para la Gestión del Riesgo del DAFP 2011 y los resultados de la encuesta MECI 2014.
4	13/Sep/2016	• Se incluye una referencia al tratamiento de los riesgos de corrupción • Se ajusta la periodicidad del monitoreo a los riesgos y sus controles. • Se detalla lineamiento sobre la actualización de los mapas de riesgos Se actualiza la Política por la adopción de los lineamientos de la Guía Para la Gestión del Riesgo de Corrupción emitida por la Secretaría de Transparencia.
5	18/Feb/2020	Modificación de la política,por la adopción de los lineamientos de la Guía para la Gestión del Riesgo del DAFP 2018.
6	21/Abr/2021	Actualización de la política de conformidad con la nueva Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP, versión 5, 2020. y la articulación de MIPG, SIGC y SCI.

ELABORO		REVISO		APROBO	
Nombre:	Nestor Camilo Zamudio Sopo	**Nombre:**	Cristhian Fabian Ruiz Ramos	**Nombre:**	Paula Susana Ospina Franco
Cargo:	Contratista	**Cargo:**	Director Técnico - 009-05	**Cargo:**	Secretario de Despacho - 020-00
Fecha:	21/Abr/2021	**Fecha:**	22/Abr/2021	**Fecha:**	22/Abr/2021