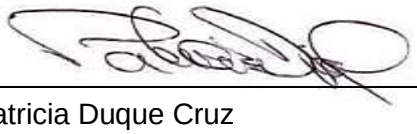
	Responsable del Proceso	Dirección de Planeación
	Aprobación	**Revisión Técnica**
Firma:		
Nombre:	Patricia Duque Cruz	Michael Andrés Ruíz Falach
Cargo:	Contralora Auxiliar	Director Técnico de Planeación
Dependencia:	Despacho Contralor Auxiliar	Dirección de Planeación
R.R. Nº 019 de 2021		**Fecha: Agosto 13 de 2021**

ANDRÉS CASTRO FRANCO
Contralor de Bogotá, D.C.

PATRICIA DUQUE CRUZ
Contralora Auxiliar

MICHAEL ANDRÉS RUÍZ FALACH
Director Técnico de Planeación

Julio de 2021

Tabla de Contenido

INTRODUCCIÓN

Con la entrada en vigencia del nuevo Plan Estratégico Institucional – PEI 2020-2022 "*Control Fiscal Para Una Nueva Agenda Urbana*", la Política de Administración del Riesgo se orientó hacia la "Identificación, análisis y valoración de riesgos para controlar sus efectos", siendo aprobada en el Comité Institucional de Coordinación de Control Interno realizado el 22/02/2021 (Acta No. 1).

En este sentido, el presente documento señala las directrices y lineamientos en la administración de los riesgos, los roles y responsabilidades para generar acciones preventivas, encaminadas a fortalecer los controles de las operaciones y disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones en que se pueda ver expuesta la Contraloría de Bogotá D.C., en cumplimiento de la misión institucional.

Su estructura se ciñe a lo establecido en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*" expedida por el Departamento Administrativo de la Función Pública – DAFP.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Política de Administración de Riesgos fue aprobada en el Comité Institucional de Coordinación del Control Interno en reunión realizada el 22/02/2021 (Acta No. 1), así:

> *"La Contraloría de Bogotá D.C., manifiesta su compromiso con la identificación, análisis y valoración de los riesgos que pueden afectar la gestión de los procesos del Sistema Integrado de Gestión - SIG, con miras a controlar sus efectos sobre el cumplimiento de la misión, a través de las acciones implementadas".*
>
> *"Identificación, análisis y valoración de riesgos para controlar sus efectos"*

1. OBJETIVO

Establecer los principios básicos, directrices, lineamientos y responsabilidades en el marco general de actuación para la gestión y control de los riesgos, encaminadas a disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones en que se pueda ver expuesta la Contraloría de Bogotá, D.C., en cumplimiento de la misión institucional.

2. ESTRATÉGIA ORGANIZACIONAL

La estrategia organizacional de la Contraloría de Bogotá, D.C., se encuentra formalizada en el Plan Estratégico Institucional - PEI, documento que recoge y difunde las principales líneas de acción y estratégicas que se propone adelantar en el corto y medio 6 plazo, orientadas al cumplimiento de su misión y visión institucional, a saber:

Misión[1]. *"Todos somos uno en la vigilancia de los recursos públicos de la ciudad, nuestras acciones son estratégicas para que cada peso invertido se vea reflejado en el bienestar de los bogotanos".*

Visión. *"Seremos una Contraloría confiable y estratégica, que realice un control fiscal para una nueva agenda urbana, a la altura de los retos que hoy tiene la ciudad y las expectativas de los bogotanos".*

En este sentido, la administración de los riesgos es una herramienta de control fundamental para el desempeño de los procesos que integran el Sistema Integrado de Gestión – SIG y contribuye al cumplimiento de los objetivos Institucionales, como son:

[1] Plan Estratégico Institucional – PEI 2020-2022 "Control Fiscal para una nueva agenda urbana".

Imagen No. Objetivo corporativos

FUENTE: Plan Estratégico Institucional – PEI 2020-2022

3. ALCANCE

La Política de Administración de Riesgos (Gestión, corrupción y seguridad de la Información) aplica para todas las dependencias que conforman los diferentes procesos que integran el Sistema Integrado de Gestión - SIG, bajo los lineamientos y directrices expedidas por la Alta Dirección, a través del Comité Directivo y Comité Institucional de Coordinación de Control Interno – CICCI), los cuales deben ser implementados por todos los niveles de la organización, en cumplimiento del ejercicio de sus funciones y en representación de la Entidad, a partir de los siguientes criterios orientadores:

- En la administración de los Riesgos de Gestión y Seguridad de la Información se aplica lo establecido en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5.0*" expedida por el Departamento Administrativo de la Función Pública – DAFP.

- Para los Riesgos de Corrupción se aplica lo establecido en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*, *versión 4.0"* expedida por el Departamento Administrativo de la Función Pública – DAFP.

- Los Riesgos de la Información Digital se gestionan de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información (caja de herramientas).

Los anteriores criterios se complementan con los parámetros establecidos en los siguientes procedimientos: *"Procedimiento para elaborar el contexto de la organización y Plan Estratégico Institucional – PEI – PDE- 03*" y el "*Procedimiento para la Administración Integral de los Riesgos Institucionales – PDE-07*".

4. TÉRMINOS Y DEFINICIONES

- **Alta Dirección:** máxima autoridad, es decir el representante legal como responsable del Sistema de Control Interno según la Ley 87 de 1993 quién deberá disponer de los recursos físicos, económicos, tecnológicos, de infraestructura y de talento humano y la responsabilidad del Proceso en General de la Administración de Riesgos

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

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

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

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

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

- **Control:** Medida que permite reducir o mitigar un riesgo.

- **Factores de Riesgo**: Son las fuentes generadoras de riesgos.

- **Gestión del riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

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

  - ➢ **Riesgo de corrupción**: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

  - ➢ **Riesgo de 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 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):

  - ✓ Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
  - ✓ Integridad: propiedad de exactitud y completitud.
  - ✓ Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas
  - ✓ Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

- **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.

  - ✓ **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.

- **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.

- **Nivel de riesgo**: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo es 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:

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

  - ✓ **Impacto**: consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de

Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

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

- **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.

5. NIVELES PARA CALIFICAR EL IMPACTO

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

- **Riesgos de Gestión y Seguridad de la Información:**

Para los Riesgos de Gestión y Seguridad de la Información se definen impactos económicos y reputacionales como las variables principales, no obstante, cuando se presenten ambos impactos para un riesgo, con diferente nivel de riesgo, se debe tomar el nivel más Alto:

Tabla No. 1 Criterios para definir el nivel de Impacto
Riesgos de Gestión – Seguridad de la Información

Nivel de Riesgo	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.

- ***Riesgos de Corrupción:***

Tabla No. 2 Criterios para calificar el Impacto – Riesgos de Corrupción

Nº	Pregunta Si el riesgo de corrupción se materializa podría...	Riesgo 1		Riesgo 2	
		Si	NO	Si	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 misión de la Entidad?				
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?				
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 o servicios o los 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?				
TOTAL		0		0	
Clasificación del Impacto: Es la cantidad de respuestas afirmativas, revise la tabla de calificación de riesgo de corrupción					

CALIFICACIÓN IMPACTO RIESGO DE CORRUPCIÓN	
RESPUESTAS POSITIVAS	DESCRIPCIÓN
1 - 5	3-Moderada
6-11	4- Mayor
12-19	5- Catastrófico (Extrema)

- **Moderado:** Genera medianas consecuencia sobre la Entidad.
- **Mayor:** Genera alta consecuencias sobre la Entidad.
- **Catastrófico:** Genera consecuencias desastrosas para la Entidad.

NOTA. Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos.

6. NIVELES DE ACEPTACIÓN DEL RIESGO

ZONA DE RIESGO	TRATAMIENTO DEL RIESGO	
	RIESGOS DE GESTIÓN Y RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	RIESGOS DE CORRUPCIÓN
BAJA	Se asume el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado, no se adopta ninguna medida de control que afecta la probabilidad o el impacto del riesgo.	Ningún riesgo de corrupción podrá ser aceptado.
MODERADA	Se establecen acciones de control preventivas que permitan **REDUCIR o COMPARTIR** la probabilidad o el impacto de ocurrencia del riesgo	Se establecen acciones de control preventivas que permitan **REDUCIR o COMPARTIR** la probabilidad o el impacto de ocurrencia del riesgo
ALTA	Se establecen acciones de Control Preventivas que permitan **COMPARTIR, EVITAR o REDUCIR** el riesgo se reduce la probabilidad o el impacto del riesgo transferido o compartiendo una parte de este.	Se adoptan medidas para: **REDUCIR:** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. **EVITAR:** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. **TRANSFERIR O COMPARTIR** una parte del riesgo para reducir la probabilidad o el impacto del mismo. Los riesgos de corrupción se pueden compartir pero no se puede transferir su responsabilidad.
EXTREMA	Se establecen acciones de Control Preventivas y correctivas que permitan **EVITAR, COMPARTIR o REDUCIR** el riesgo con el fin de mitigar la materialización del riesgo.	

Para los riesgos de seguridad de la información Identifica en el Registro de Activos de Información del proceso publicado en la página WEB de la entidad aquellos que se encuentran con criticidad ALTA agrupa los activos de información del mismo tipo y analiza conjuntamente las amenazas y vulnerabilidades que sean comunes y que podrían causar su materialización. Redacta el riesgo orientado a la posibilidad de ocurrencia de un evento teniendo en cuenta la selección anterior:

- ✓ Pérdida de confidencialidad.
- ✓ Pérdida de la integridad.
- ✓ Pérdida de la disponibilidad.

Los procesos que no presentan activos de información con criticidad ALTA deben seleccionar activos de criticidad MEDIA según determinación de la importancia del activo de información para el proceso.

7. TRATAMIENTO DE RIESGO

Reducir	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
Aceptar	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo (Ningún riesgo de corrupción podrá ser aceptado)
Compartir	Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de éste. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.
Evitar	Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o continuar con la actividad que lo provoca.

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas a continuación:

- Para cualquier tipo de Riesgo se debe llevar al Plan de Mejoramiento, efectuar el análisis de causas y determinar acciones preventivas y de mejora.

- Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento y actualizar el mapa de riesgos.

- Para los riesgos de corrupción, la Oficina de Control Interno o responsable del Proceso deberá informar al Proceso de Direccionamiento Estratégico o a las autoridades competentes sobre el hecho encontrado realizar la denuncia ante la instancia de control correspondiente de la ocurrencia de un hecho de corrupción.

- Ante la materialización de los riesgos de gestión y de seguridad de la información en zona extrema, alta y moderada se informará al responsable del proceso o al Proceso de Direccionamiento Estratégico según sea el caso, se procede de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso) y documentarlo en el Plan de mejoramiento.

- Para los riesgos de gestión y de seguridad de la información en zona baja informar al responsable del proceso sobre el hecho, así mismo informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el responsable del proceso para revisar el mapa de riesgos establecer acciones

correctivas al interior de cada proceso, a cargo del responsable respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos y la verificación por parte de la Oficina de Control Interno que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

8. ROLES Y RESPONSABILIDADES

Para la administración integral de los riesgos institucionales se determinan los roles y responsabilidades de las diferentes líneas de defensa, teniendo en cuenta las directrices del Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Modelo Integrado de Planeación y Gestión, entre otras, así:

LÍNEA ESTRATÉGICA	
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.	
Responsables	**Actividades de monitoreo y revisión**
Alta Dirección y Comité Institucional de Coordinación de Control Interno – CICCI	✓ Revisar, aprobar y socializar la Política de administración del riesgo ✓ Aprobar el Mapa de Riesgos de Gestión, Corrupción y Riesgos de Seguridad de la Información en Comité Directivo ✓ Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo) ✓ Analizar los cambios en el contexto de la organización (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles ✓ Realizar seguimiento y análisis periódico a los riesgos institucionales

1ª. LÍNEA DE DEFENSA	
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	
Responsables	**Actividades de monitoreo y revisión**
Responsables de los Procesos	✓ Identificar y valorar los riesgos de Gestión, Corrupción y de la Seguridad de la Información que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera ✓ Diseñar, ejecutar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. ✓ Establecer la(s) acción(es) asociadas al control que mitigan o reducen cada riesgo, determinando el periodo de ejecución, indicador, área responsable y registro que evidencie el cumplimiento de la acción.

1ª. LÍNEA DE DEFENSA	
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	
Responsables	**Actividades de monitoreo y revisión**
	✓ Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo. ✓ Solicitar modificaciones de los diferentes tipos de riesgos de acuerdo con los autoevaluaciones, observaciones o informes de las auditorías internas o externas. ✓ Realizar monitoreo y revisión al Mapa de Riesgos de Gestión, Corrupción y Seguridad de la Información.

2ª. LÍNEA DE DEFENSA	
Tiene a cargo responsabilidades directas frente al monitoreo y evaluación del estado de controles y la Gestión del Riesgo, asegura que la identificación, análisis, valoración, monitoreo y las actividades de control de los riesgos de Gestión, Corrupción y de Seguridad de la Información implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	
Responsables	**Actividades de monitoreo y revisión**
Dirección de Planeación, Supervisores e interventores de contratos o proyectos, comités de contratación, áreas financieras, Tics entre otros	✓ Asesorar a la línea estratégica en el análisis del contexto de la organización (interno y externo), para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo ✓ Consolidar el Mapa de riesgos institucional y presentarlo para aprobación ante el Comité Directivo ✓ Acompañar, orientar y entrenar a los responsables de los procesos en la identificación, análisis y valoración del riesgo ✓ Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de los procesos ✓ Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones. ✓ Evaluar que los riesgos sean consistentes con la actual política de la entidad y que sean monitoreados por la primera línea de defensa ✓ Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno ✓ Acompañar, orientar y entrenar a los responsables y gestores de calidad en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo. ✓ Actualizar la versión del Mapa de Riesgos de Gestión y Corrupción o el Mapa de Riesgos de Seguridad de la Información según sea el

2ª. LÍNEA DE DEFENSA	
Tiene a cargo responsabilidades directas frente al monitoreo y evaluación del estado de controles y la Gestión del Riesgo, asegura que la identificación, análisis, valoración, monitoreo y las actividades de control de los riesgos de Gestión, Corrupción y de Seguridad de la Información implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	
Responsables	**Actividades de monitoreo y revisión**
	✓ caso, con las solicitudes de modificación aprobadas por la Alta Dirección para su respectiva publicación en la página WEB de la Entidad.

3ª. LÍNEA DE DEFENSA	
Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.	
Responsables	**Actividades de monitoreo y revisión**
Oficina de Control Interno	✓ Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos ✓ Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa ✓ Asesorar de forma coordinada con la Dirección de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. ✓ Llevar a cabo el seguimiento a los riesgos consolidados y presentar dicho informe de seguimiento al CICCI según la programación del Plan Anual de Auditoria o reuniones de este comité ✓ Recomendar mejoras a la política de administración del riesgo. ✓ Realizar seguimiento al Mapa de Riesgos, utilizando el Anexo 1 Mapa de Riesgos de Gestión y Corrupción y Anexo 2 Mapa de Riesgos de Seguridad de la Información y determinar el Estado de los Riesgos, así: • **Abierto:** El riesgo continúa para seguimiento. • **Mitigado:** el riesgo se estudia para determinar si este se sigue administrando o se retira del mapa de riesgos. • **Materializado:** el riesgo se lleva al Plan de Mejoramiento para la formulación de acciones correctivas ✓ Verificar la inclusión de los riesgos que se materializan en el plan de mejoramiento.

9. PERIODICIDAD PARA EL SEGUIMIENTO

El seguimiento para todos los riesgos es CUATRIMESTRAL, con fecha de corte abril, agosto y diciembre de cada vigencia, el cual se realizará de acuerdo con lo establecido en el Procedimiento para la Administración Integral de los Riesgos Institucionales – PDE-07 y teniendo en cuenta los roles y responsabilidades definidas en las diferentes líneas de defensa señaladas anteriormente.

10. ACCIONES DE APROPIACIÓN Y COMUNICACIÓN DE LA GESTIÓN DEL RIESGO

La Política de Administración de Riesgos es aprobada en Comité Institucional de Coordinación de Control Interno de la Entidad y comunicada, entre otros medios:

- ✓ Capacitaciones para el fortalecimiento institucional, conceptual y operativo de la gestión integral de riesgos.
- ✓ Asesorías y acompañamiento para el desarrollo del enfoque de administración de riesgos en las actividades diarias.
- ✓ Divulgación de los resultados de la administración y gestión de riesgos en los procesos de la Entidad.

En este sentido, en la Contraloría de Bogotá, D.C. se promueve la transparencia y se fortalece la cultura de autocontrol y prevención, lo cual contribuye a la administración integral de riesgos.

CONTROL DE CAMBIOS

Versión	R.R., Acta y Fecha	Descripción de la Modificación
1.0	R.R. 039 del 25-sep-2019	El documento política de administración de riesgo se ajustó de acuerdo con los nuevos lineamientos establecidos en la Guía para la administración del riesgos y diseño de controles en entidades públicas del DAFP, versión 5.0. Se incorporó al documento la Política de Administración de Riesgos aprobada en el Comité Institucional de Coordinación del Control Interno, realizado el 22/02/2021 (Acta No. 1), así: *"La Contraloría de Bogotá D.C., manifiesta su compromiso con la identificación, análisis y valoración de los riesgos que pueden afectar la gestión de los procesos del Sistema Integrado de Gestión - SIG, con miras a controlar sus efectos sobre el cumplimiento de la misión, a través de las acciones implementadas".* *"Identificación, análisis y valoración de riesgos para controlar sus efectos"* Se modificó la redacción del objetivo, alineación estratégica, alcance, términos y definiciones, calificación del impacto, niveles de aceptación del riesgo y tratamiento del riesgo.
2.0	R.R. 019 del 13 agosto de 2021	