8. APROBACION Y ACTUALIZACIÓN

Las políticas de seguridad de la información, serán aprobadas en sesión del Comité SIGEL o quien haga sus veces y las actualizaciones a que haya lugar, serán aprobadas por la misma instancia y se realizaran cuando se requiera.

9. CONTROL DE CAMBIOS

Versión	R.R. No.	Descripción de la Modificación
1.0	R.R. No.022 14-jul-2016	Se adoptan las Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá, D.C., para efectos de obligatoriedad en su cumplimiento, la cual forma parte de la documentación que soporta el Sistema Integrado de Gestión, en el marco del Subsistema de Seguridad de la Información y de la estrategia del Gobierno en Línea.
2.0	R.R. No. 022 19-abr-2018	Se actualizan las Políticas, conforme a lo aprobado en el Comité SIGEL No.3 realizado el día 11 de junio de 2019, a la normatividad legal vigente y a lo establecido en la Norma Técnica Colombiana ISO/IEC 27001:2013, con las directrices para la proteger la información, asegurando que en ella se cumplan las características de integridad, disponibilidad y confidencialidad, mediante la ejecución de acciones en concordancia con disposiciones legales, operativas, tecnológicas y de acuerdo al objetivo estratégico, debiéndose modificar el nombre a Políticas de Seguridad de la Información
3.0	R.R. No.038 24-sep-2019	

CONTRALORÍA DE BOGOTÁ, D.C.

Resolución Reglamentaria Número 039

(Septiembre 25 de 2019)

"Por la cual se adopta la Política de Administración del Riesgo para la Contraloría de Bogotá D.C."

EL CONTRALOR DE BOGOTÁ D.C.
En ejercicio de las atribuciones constitucionales y legales, especialmente las conferidas en el Decreto Ley 1421 de 1993, el Acuerdo 658 de 2016 modificado por el Acuerdo 664 de 2017 y,

CONSIDERANDO:

Que la Constitución Política establece en su artículo 209, que "*La Administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley*" y en el artículo 269 la obligación de las autoridades correspondientes en las entidades públicas, de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley.

Que la 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*", establece que son objetivos del control interno, entre otros, la protección de los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten y definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

Que el Decreto 1083 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"* que compiló el Decreto 1537 de 2001. Establece en su artículo 2.2.21.5.4 la Administración de riesgos**.** "*Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspecto tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos."*

Que el Departamento Administrativo de la Función Pública expidió la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, según la cual la Alta Dirección debe establecer la Política de Administración de Riesgos, es decir determinar lineamientos precisos acerca del tratamiento, manejo de los riesgos.

Que se hace necesario adoptar la Política de Administración del Riesgo para la Contraloría de Bogotá. D.C.

Que la Política de Administración del Riesgo para la Contraloría de Bogotá, D.C., fue aprobada en Comité Institucional de Coordinación de Control Interno como consta en el Acta No. 01 en sesión del 14 de agosto de 2019

En mérito de lo expuesto, el Contralor de Bogotá D.C.

RESUELVE:

ARTÍCULO PRIMERO. Adoptar la Política de Administración del Riesgo para la Contraloría de Bogotá, D.C. que se anexa a la presente Resolución y hace parte integral de esta.

ARTÍCULO SEGUNDO. El seguimiento y actualización de los Riesgos en la Entidad será responsabilidad de los responsables de los Procesos del Sistema Integrado de Gestión SIG.

ARTÍCULO TERCERO. La Oficina de Control Interno, realizará la evaluación de los controles establecidos para evitar que los riesgos se materialicen, así como las acciones preventivas y correctivas establecidas por los Responsables de los Procesos.

ARTÍCULO CUARTO. La Dirección de Planeación brindará apoyo y asesoría en las actividades correspondientes a la Política de Administración del Riesgo en la Contraloría de Bogotá, D.C.

ARTÍCULO QUINTO. Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina y Gerentes velar por la divulgación de la Política de Administración del Riesgo.

ARTÍCULO SEXTO. La presente Resolución rige a partir de la fecha de su publicación y deroga las normas que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los veinticinco (25) días del mes de septiembre de dos mil diecinueve (2019).

JUAN CARLOS GRANADOS BECERRA
Contralor de Bogotá D.C.

Aprobación	**Revisión Técnica**
Firma:	Firma:
Nombre: María Anayme Barón Durán	Mercedes Yunda Monroy
Cargo: Contralora Auxiliar	Directora Técnica
Dependencia: Despacho Contralora Auxiliar	Dirección de Planeación
R.R. No. 039 DE SEPTIEMBRE 25 DE 2019	

JUAN CARLOS GRANADOS BECERRA
Contralor de Bogotá, D.C.

MARÍA ANAYME BARÓN DURÁN
Contralora Auxiliar

MERCEDES YUNDA MONROY
Directora Técnica de Planeación

MARÍA ANAYME BARÓN DURÁN
Responsable Proceso Direccionamiento Estratégico
Contralora Auxiliar

Septiembre de 2019

INTRODUCCIÓN

Toda actividad está expuesta a situaciones de riesgo que pueden afectar en forma negativa el cumplimiento de la misión, objetivos institucionales, objetivos del proceso o la satisfacción del cliente como consecuencia de la diversidad de riesgos de corrupción, de Gestión y de Seguridad de la información, por lo que se requiere un acercamiento más profundo, metodológico y sistemático a la administración de riesgos para la Contraloría de Bogotá, D.C.

El presente documento técnico toma como referencia 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; por tanto, establece los lineamientos para la identificación, análisis, valoración, evaluación y tratamiento de los riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos, y planes institucionales, los cuales deben ser acatados por todos los servidores públicos de la entidad en el desarrollo de sus funciones y son complemento a la Política identificada en el Plan Estratégico Institucional PEI 2016 – 2020 *"Una Contraloría aliada con Bogotá"* , que establece: "*La Contraloría de Bogotá D.C., asume la Administración del Riesgo como parte integral del Direccionamiento Estratégico, lo que implica un compromiso institucional 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*"[1].

1. OBJETIVO:

Establecer los principios básicos, lineamientos, responsabilidades y directrices que permitan 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 función del desarrollo de un pensamiento basado en riesgos aplicando las normas en materia de riesgos y la metodología expedida por el Departamento Administrativo de la Función Pública DAFP "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*" versión 4.0, con el fin de alcanzar de manera eficaz y efectiva la misión y el cumplimiento de los objetivos institucionales.

[1] Política de Administración del Riesgo. Plan Estratégico Institucional PEI 2016 – 2020.

Alineación con el Plan Estratégico

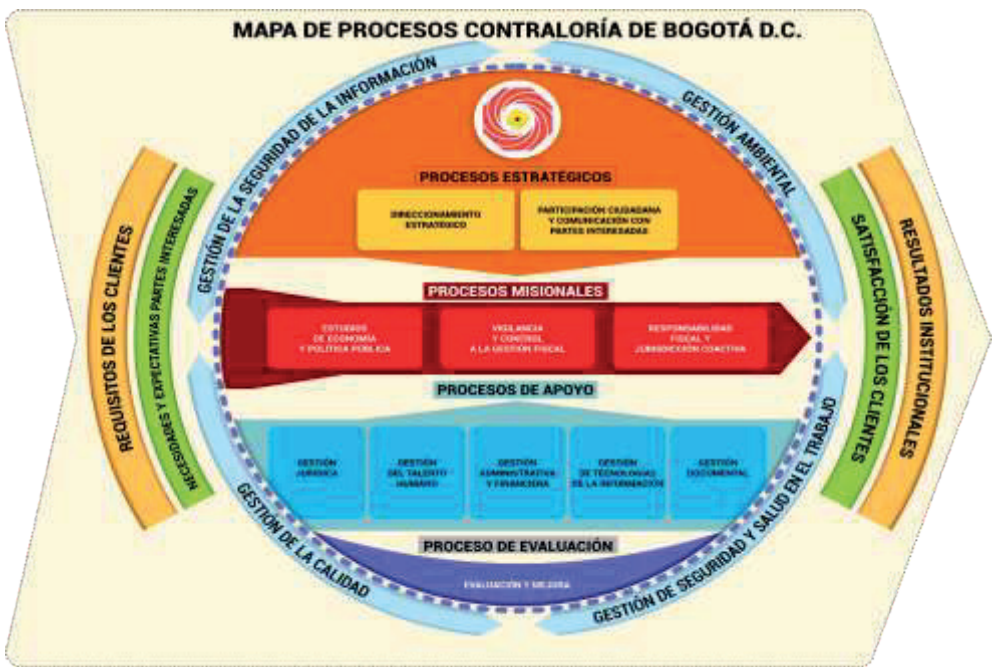
La estrategia organizacional de la Contraloría de Bogotá, D.C., se encuentra formalizada en el Plan Estratégico Institucional - PEI, documento que recoge y difunde las principales líneas de acción y estratégicas que se propone adelantar en el corto y medio plazo, orientadas al cumplimiento de su misión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

Misión. La Contraloría de Bogotá, D.C., es la entidad que vigila la gestión fiscal de la Administración Distrital y de los particulares que manejan fondos o bienes públicos, en aras del mejoramiento de la calidad de vida de los ciudadanos del Distrito Capital.

Visión. En el año 2020, la Contraloría de Bogotá, D.C., será reconocida por los ciudadanos como una entidad confiable por su efectividad en la vigilancia y control del uso adecuado de los recursos públicos, fundada en la participación ciudadana, la sostenibilidad y el uso de la tecnología.

Para la Entidad, la administración de los riesgos es una herramienta de control fundamental para el cumplimiento de los objetivos estratégicos y de los procesos internos. Es por esto que la presente política se encuentra armonizada con la misión y visión organizacional, así como con el Sistema Integrado de Gestión - SIG.

Mapa de procesos:



2. ALCANCE.

La política debe ser aplicada por toda la entidad desde el Direccionamiento Estratégico como línea estratégica (Alta Dirección y el Comité Institucional de Coordinación de Control Interno – CICCI) hasta el nivel operativo en cumplimiento de las tareas diarias del que hacer de la institución. Aplica a todos los procesos y proyectos de la Entidad y a todas las actividades realizadas por los funcionarios durante el ejercicio de sus funciones y en representación de la Entidad.

Se complementa con los parámetros establecidos en los siguientes procedimientos: "Procedimiento para elaborar el contexto de la organización y Plan Estratégico Institucional – PEI" y "Procedimiento para la Administración Integral de los Riesgos Institucionales".

3. 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

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

- **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 inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- **Riesgo residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

- **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.

- **Probabilidad:** posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

- **Impacto**: consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un 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.

- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.

- **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.

- **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.

- **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizado.

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

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

- **Integridad:** propiedad de exactitud y completitud.

- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.

- **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

- **Apetito al riesgo:** Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

4. RESPONSABILIDADES Y ROLES

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. ✓ 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,	✓ Asesorar a la línea estratégica en el análisis del contexto de

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**
Supervisores e interventores de contratos o proyectos, comités de contratación, áreas financieras, Tics entre otros	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 caso, con las solicitudes de

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**
	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.

5. ETAPAS PARA LA GESTIÓN DEL RIESGO

La gestión de riesgos institucionales comprende las actividades de análisis del contexto interno y externo, identificación y análisis del riesgo, valoración, evaluación, definición de controles para el tratamiento y seguimiento. Las diferentes etapas con sus actividades específicas y responsables se describen en el "*Procedimiento para la Administración Integral de los Riesgos Institucionales"*.

6. NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO.

La siguiente tabla presenta el mapa de calor (Riesgo Inherente- sin controles) que contiene los niveles de aceptación y la medida de tratamiento para los riesgos de Gestión, Corrupción y Seguridad de la información. Los riesgos de corrupción son inaceptables.

TABLA No.7 Mapa de Calor

ZONA DE RIESGO - NO APLICA RIESGOS DE CORRUPCIÓN

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Rara vez (1)	B	B	M	A	E
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

ZONA DE RIESGO

MEDIDA DE TRATAMIENTO DEL RIESGO

B: Zona de riesgo baja: ACEPTAR EL RIESGO
M: Zona de riesgo moderada: REDUCIR EL RIESGO
A: Zona de riesgo Alta: COMPARTIR EL RIESGO
E: Zona de riesgo extrema: EVITAR EL RIESGO

ZONA DE RIESGO - RIESGO DE CORRUPCIÓN

PROBABILIDAD	IMPACTO		
	Moderado	Mayor	Catastrófico
Casi Seguro (5)	E	E	E
Probable (4)	A	E	E
Posible (3)	A	E	E
Improbable (2)	M	A	E
Rara vez (1)	M	A	E

ZONA DE RIESGO

MEDIDA DE TRATAMIENTO DEL RIESGO DE CORRUPCIÓN

M: Zona de riesgo moderada: REDUCIR EL RIESGO
A: Zona de riesgo Alta: COMPARTIR EL RIESGO
E: Zona de riesgo extrema: EVITAR EL RIESGO

7. NIVELES PARA CALIFICAR EL IMPACTO

⇒ Riesgos de gestión:

TABLA 4. .Criterios para Calificar el Impacto - NO APLICA CORRUPCIÓN		
NIVEL DEL IMPACTO	**CRITERIOS PARA CALIFICAR EL IMPACTO**	**VALOR DEL IMPACTO**
CATASTRÓFICO	Interrupción de las operaciones de la Entidad por más de cinco (5) días.	5
	Intervención por parte de un ente de control u otro ente regulador.	
	Pérdida de Información crítica para la entidad que no se puede recuperar	
	Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.	
	Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados	
MAYOR	Interrupción de las operaciones de la Entidad por más de dos (2) días.	4
	Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.	
	Sanción por parte del ente de control u otro ente regulador	
	Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno	
	Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.	
MODERADO	Interrupción de las operaciones de la Entidad por un (1) día.	3
	Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad	
	Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.	
	Reproceso de actividades y aumento de carga operativa	
	Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos	
	Investigaciones penales, fiscales o disciplinarias	
MENOR	Interrupción de las operaciones de la Entidad por algunas horas.	2
	Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.	
	Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.	
INSIGNIFICANTE	No hay interrupción de las operaciones de la entidad.	1
	No se generan sanciones económicas o administrativas.	
	No se afecta la imagen institucional de forma significativa.	

⇒ Riesgos de Corrupción:

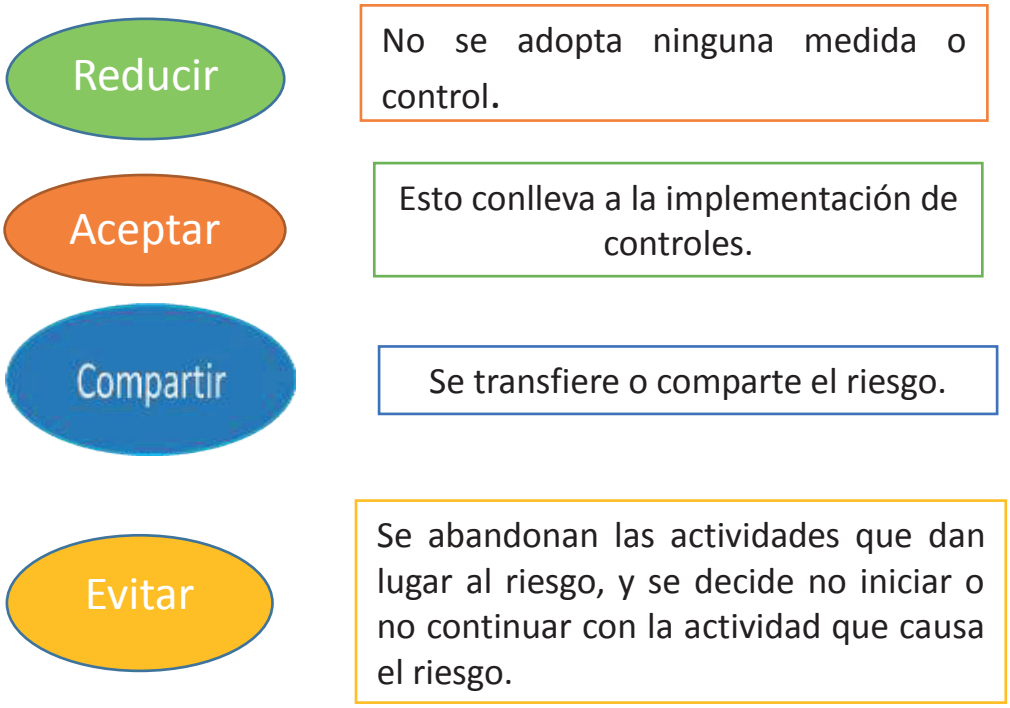
TABLA No.5. CRITERIOS PARA CALIFICAR EL IMPACTO - RIESGOS DE CORRUPCIÓN					
Nº	Pregunta Si el riesgo de corrupción se materializa podría...	Riesgo 1		Riesgo 2	
		Si	NO	Si	NO
1	¿Afectar al grupo de funcionarios del proceso?				
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?				
3	¿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)

⇒ Riesgos de Seguridad de la Información:

TABLA 6. Criterios para Calificar el Impacto - Riesgos de Seguridad Digital		
Descriptor	**Descripción**	**calificación riesgos estratégicos**
Insignificante	Sin afectación de la integridad de la información Sin afectación de la disponibilidad de la información Sin afectación de la confidencialidad de la información	1
Menor	Afectación leve de la integridad de la información Afectación leve de la disponibilidad de la información Afectación leve de la confidencialidad de la información	2
Moderado	Afectación moderada de la integridad de la información Afectación moderada de la disponibilidad de la información Afectación moderada de la confidencialidad de la información	3
Mayor	Afectación grave de la integridad de la información Afectación grave de la disponibilidad de la información Afectación grave de la confidencialidad de la información	4
Catastrófico	Afectación muy grave de la integridad de la información Afectación muy grave de la disponibilidad de la información Afectación muy grave de la confidencialidad de la información	5

8. TRATAMIENTO DE RIESGOS



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.

9. PERIODICIDAD PARA EL SEGUIMIENTO

El seguimiento para todos los riesgos será CUATRIMESTRAL y su adecuado control se registra en el ANEXO 1. Mapa de Riesgos de Gestión y Corrupción y ANEXO 2 Mapa de Riesgos de Seguridad de la Información.

10. ACCIONES PARA LA APROPIACIÓN DE LA GESTIÓN DEL RIESGO

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, a través de:

- ✓ 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.

- ✓ Seguimiento cuatrimestral a todos los riesgos ubicados en las diferentes zonas de riesgo Baja, Moderada, Alta y Extrema de los anexos de la matriz de riesgos, identificada para cada uno de los procesos de la Entidad.

- ✓ Divulgación de los resultados de la administración y gestión de riesgos en los procesos de la Entidad

11. ACCIONES ANTE LA MATERIALIZACIÓN DEL RIESGO

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.

CONTROL DE CAMBIOS

Versión	R.R., Acta[2] o modificación[3] Día mes año	Descripción de la modificación
1.0	Acta No 01 del 14 de agosto de 2019 Comité Institucional de Coordinación de Control Interno	

[2] Acta de Comité que aprueba la versión 1.0 del documento.
[3] Fecha en la cual el responsable del proceso aprueba la modificación del documento.