EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ Transformamos ciudad	**Política de Administración de Riesgos**

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	14/08/2019	Documento original.

ELABORADO POR:	ESTANDARIZADO POR:	REVISADO Y APROBADO POR:
Original firmado	Original firmado	Acta de Comité Institucional de Coordinación de Control Interno No. 5 del 14 de agosto de 2019
Holman Eduardo Barrera Espitia Gestor Junior Sistemas		
Original firmado		
Esperanza Peña Quintero Contratista Subgerencia de Planeación y Administración de Proyectos	**Esperanza Peña Quintero** Contratista Subgerencia de Planeación y Administración de Proyectos	**Comité Institucional de Gestión y Desempeño**

Tabla de contenido

1. PRESENTACIÓN 3
2. DEFINICIONES 3
3. OBJETIVOS 4
4. ALCANCE 4
5. NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO 4
6. NIVELES PARA CALIFICAR EL IMPACTO 6
7. TRATAMIENTO DE RIESGOS 6
8. ESTRUCTURA PARA LA GESTIÓN Y ADMINISTRACIÓN DEL RIESGO 7
8.1 Metodología a utilizar 7
8.2 Herramienta a utilizar 7
8.3 Aspectos relevantes sobre los factores de riesgo estratégicos 7
8.4 Lineamientos o políticas de operación 7
8.5 Periodicidad para el monitoreo, revisión y seguimiento de los riesgos 8
8.6 Tabla de impactos institucional 9
8.7 Niveles de responsabilidad sobre la gestión y administración del riesgo 9
Línea de Defensa Estratégica 9
Primera Línea de Defensa 9
Segunda Línea de Defensa 10
Tercera Línea de Defensa 10

1. PRESENTACIÓN

Esta guía tiene por objetivo establecer los lineamientos que orienten las acciones necesarias para gestionar los riesgos a los cuales está expuesta la Empresa, para prevenir situaciones que afecten el cumplimiento de su misión, objetivos institucionales, objetivos del proceso y la satisfacción de las partes interesadas.

El desarrollo y aplicación de la **Política de Administración del Riesgo** se logra a través de esta guía. Es de anotar que ésta política está incluida en la **Política Integral de Gestión**, que recoge lineamientos de varios modelos de gestión que la requieren, para facilitar y garantizar la implementación de este requerimiento de manera coherente, organizada y articulada.

2. DEFINICIONES[1]

Alta Dirección: se considera Alta Dirección a los directivos con cargo más alto en la empresa, Representante Legal y su equipo Directivo.

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.

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

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

Líder o responsable de proceso: encargado de que el proceso que tenga a cargo, establecido en el mapa de procesos de la Empresa, cumpla sus objetivos. Debe estar involucrado en su fase de diseño, implementación y cambio asegurando en todo momento que se dispone de las métricas necesarias para su correcta monitorización, evaluación y eventual mejora.

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

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

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 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.

1 Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas. DAFP. Octubre de 2018

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.

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.

3. OBJETIVOS

- Gestionar los riesgos atendiendo lo establecido en la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* del Departamento Administrativo de la Función Pública - DAFP, en su última versión o en aquella que la modifique, complemente o sustituya.

- Formalizar al interior de la Empresa una metodología para gestionar y administrar los riesgos.

4. ALCANCE

Los lineamientos definidos en esta guía aplican a todos los procesos de la entidad.

En el caso de los riesgos de seguridad digital, éstos se deben gestionar de acuerdo con los criterios diferenciales descritos en el Modelo de Seguridad y Privacidad de la Información.

5. NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO

De acuerdo con los criterios definidos en la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* del Departamento Administrativo de la Función Pública - DAFP (Evitar, Reducir, Compartir o Transferir y Aceptar o Asumir), los siguientes son los niveles de aceptación de los riesgos en la Empresa:

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación	Acción
Riesgo de corrupción	Bajo	Inaceptable	Para EVITAR a toda costa su materialización, los líderes de proceso deberán realizar un monitoreo mensual de los controles establecidos y reportar cualquier novedad al Comité Institucional de Coordinación de Control Interno y a la Oficina de Control Interno, así como a la Subgerencia de Gestión Corporativa para iniciar los procesos disciplinarios correspondientes. De otra parte, y cuando los escenarios de riesgo identificado se consideran demasiado extremos se pueden abandonar las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.
	Moderado	Inaceptable	
	Alto	Inaceptable	
	Extremo	Inaceptable	

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación	Acción
Riesgo de gestión	Bajo	Aceptable	Los líderes de proceso ASUMIRÁN el riesgo y lo administrarán por medio de las actividades propias del proceso asociado y de los controles establecidos. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.
	Moderado	Aceptable	Los líderes de proceso deben establecer acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.
	Alto	Inaceptable	Los líderes de proceso deben establecer acciones de control preventivas que permitan EVITAR la materialización del riesgo. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.
	Extremo	Inaceptable	Los líderes de proceso deben establecer acciones de control preventivas y correctivas que permitan EVITAR la materialización del riesgo. El monitoreo de estos riesgos será con periodicidad mensual y se debe reportar cualquier novedad al Comité Institucional de Coordinación de Control Interno y a la Oficina de Control Interno. De otra parte, y cuando los escenarios de riesgo identificado se consideran demasiado extremos se pueden abandonar las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.
Riesgo de seguridad digital	Bajo	Aceptable	Los líderes de proceso ASUMIRÁN el riesgo y lo administrarán por medio de las actividades propias del proceso asociado y de los controles establecidos. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.
	Moderado	Aceptable	Los líderes de proceso deben establecer acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.
	Alto	Inaceptable	Los líderes de proceso deben establecer acciones de control preventivas que permitan EVITAR la materialización del riesgo. De otra parte, y cuando los escenarios de riesgo identificado se consideran demasiado extremos se pueden abandonar las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.
	Extremo	Inaceptable	Los líderes de proceso deben establecer acciones de control preventivas y correctivas que permitan EVITAR la materialización del riesgo. El monitoreo de estos riesgos será con periodicidad mensual y se debe reportar cualquier novedad al Comité Institucional de Coordinación de Control Interno y a la Oficina de Control Interno. De otra parte, y cuando los escenarios de riesgo identificado se consideran demasiado extremos se pueden abandonar las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. El registro de seguimiento se realizará cuatrimestralmente por medio del informe de seguimiento de la Oficina de Control Interno.

NOTA: Cuando sea muy difícil para la empresa reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, éste puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberán estar formalizados a través de un acuerdo contractual. Para estos casos se deberá informar al Comité Institucional de Coordinación de Control Interno para la toma de decisiones más adecuada.

Adicionalmente, se deberán documentar Planes de Mejoramiento al interior de los procesos en caso de materialización de riesgos o si es necesario, antes de que ocurra el evento, con criterios de oportunidad, evitando el menor daño en la prestación de los servicios. Estos planes estarán documentados de acuerdo con lo establecido en el proceso Evaluación y Seguimiento.

Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2018, estos también se encuentran en el anexo 4. "Lineamientos para la gestión del riesgo de seguridad digital" de la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* del Departamento Administrativo de la Función Pública – DAFP.

6. 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, teniendo en cuenta las tablas para calificar el impacto para cada tipo de riesgo (riesgos de gestión, riesgos de seguridad digital y riesgos de corrupción) definidas en la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* del Departamento Administrativo de la Función Pública - DAFP, en su última versión o en aquella que la modifique, complemente o sustituya.

7. TRATAMIENTO DE RIESGOS

Las acciones de tratamiento de riesgos se agrupan en:

- *Disminuir la probabilidad*: acciones encaminadas a gestionar las causas del riesgo.
- *Disminuir el impacto*: acciones encaminadas a disminuir las consecuencias del riesgo.

La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo, y en todos los casos, para los riesgos de corrupción la respuesta preferiblemente evitar o reducir el riesgo.

El tratamiento se dará a los riesgos de acuerdo con las opciones entregadas en la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* del Departamento Administrativo de la Función Pública - DAFP, en su última versión o en aquella que la modifique, complemente o sustituya.

Sin embargo, y con el objetivo de asegurar una adecuada gestión de los riesgos mientras se consolida una cultura del autocontrol tangible alrededor de la Administración de Riesgos en la Empresa, se determina que a pesar de que el nivel de riesgo cumpla con los criterios de aceptación de riesgo siempre se deberán formular acciones de tratamiento.

Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2018 o los que se encuentran en el anexo 4 "*Lineamientos para la*

gestión del riesgo de seguridad digital" de la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* del Departamento Administrativo de la Función Pública - DAFP.

Finalmente, y en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables definidos en el presente documento, se deberá volver a analizar y revisar dicho tratamiento.

8. ESTRUCTURA PARA LA GESTIÓN Y ADMINISTRACIÓN DEL RIESGO

8.1 Metodología a utilizar

La metodología definida será la contemplada en la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* del Departamento Administrativo de la Función Pública - DAFP, en su última versión o en aquella que la modifique, complemente o sustituya.

8.2 Herramienta a utilizar

La herramienta dispuesta para la gestión y administración de riesgos es Excel.

8.3 Aspectos relevantes sobre los factores de riesgo estratégicos

Para identificar los riesgos para cada uno de los procesos, se debe tener en cuenta el contexto interno, externo de la Empresa, así como el contexto del proceso y sus activos de seguridad digitales, de acuerdo con lo establecido en la Guía antes citada. De igual manera, se debe tener en cuenta lo establecido en el Plan Estratégico de la Empresa, para garantizar una alineación con el marco estratégico institucional.

8.4 Lineamientos o políticas de operación

- Los responsables de proceso deberán revisar el mapa de riesgos por lo menos una vez en el año y actualizarlo si se requiere, previa aprobación en el Comité Institucional de Coordinación de Control Interno.

- Como resultado del seguimiento realizado por el responsable del proceso al mapa de riesgos, éste podrá solicitar a la Subgerencia de Planeación y Administración de Proyectos eliminar, incluir o modificar riesgos, ajustar su análisis, valoración, acciones, indicadores, responsables, tiempos, entre otros. Los ajustes solicitados deberán ser remitidos a través de correo institucional para su validación y posterior aprobación por parte del Comité Institucional de Coordinación de Control Interno.

- La Subgerencia de Planeación y Administración de Proyectos deberá publicar el Mapa de riesgos de la Empresa en la ERUNET y solicitar a la Oficina Asesora de Comunicaciones su publicación en la página web de la Empresa a más tardar el 31 de enero de cada vigencia, para dar cumplimiento a lo establecido en el literal g del artículo 9 de la Ley 1712 de 2014 y el artículo 73 de la Ley 1474 de 2011.

- Los riesgos de corrupción se identifican de acuerdo con los lineamientos dados en la presente guía, los cuales son objeto de gestión y seguimiento en el marco del Plan Anticorrupción y de Atención al Ciudadano de la Empresa.

- La Oficina de Control Interno evaluará cada 4 meses (30 de abril, 31 de agosto y 31 de diciembre) de cada vigencia en forma independiente el proceso de administración de los riesgos de la Entidad y presentará al Comité Institucional de Coordinación de Control Interno el informe correspondiente. Lo anterior en armonía con el seguimiento a los riesgos de corrupción y el Plan Anticorrupción y de Atención al Ciudadano.

- Los indicadores incorporados en el mapa de riesgos, no necesitan el diligenciamiento de la hoja de vida del indicador.

- En caso de materialización de riesgos se debe elaborar un Plan de mejoramiento y, en todo caso, debe ser informado a las instancias de control interno correspondientes.

- Los responsables de proceso podrán solicitar asesoría a la Subgerencia de Planeación y Administración de Proyectos, la Subgerencia de Gestión Corporativa o la Oficina de Control Interno para la formulación de los Mapas de riesgos.

- Al identificar riesgos para cada uno de los procesos, es importante establecer la relación de cada uno de los riesgos con el cumplimiento de la estrategia organizacional, para garantizar una alineación con el marco estratégico institucional.

8.5 Periodicidad para el monitoreo, revisión y seguimiento de los riesgos

El cumplimiento de esta política, así como la aplicación de la metodología de administración de riesgos de la Empresa se realizará de la siguiente manera:

- Anualmente se revisará completamente el mapa de riesgos de la Empresa, y para ello se tomarán como insumo:
  a. Los resultados de las auditorías realizadas por la Oficina de Control Interno y Organismos de Control.
  b. Lo reportado por los líderes de proceso en los Comités de Autoevaluación y Seguimiento.
  c. Las novedades reportadas al Comité Institucional de Coordinación de Control Interno, según lo establecido en la sección 5. Niveles de aceptación del riesgo o tolerancia al riesgo, de este documento.

  Esta revisión será realizada por el responsable del proceso con el acompañamiento de la Subgerencia de Planeación y Administración de Proyectos, la Subgerencia de Gestión Corporativa y/o la Oficina de Control Interno. El control de cambios estará bajo la responsabilidad de la Subgerencia de Planeación y Administración de Proyectos, una vez sean aprobados por el Comité Institucional de Coordinación de Control Interno.

- Trimestralmente y dentro de los 10 primeros días hábiles posteriores al cierre, los líderes de proceso realizarán la revisión y seguimiento correspondiente y entregará a la Subgerencia de Planeación y Administración de Proyectos el informe de con los resultados obtenidos, el cual incluirá el análisis de los riesgos y los controles para determinar si requiere de algún ajuste.

- Trimestralmente la Subgerencia de Planeación y Administración de Proyecto presentará informes de monitoreo (segunda línea de defensa) al Comité de Coordinación de Control Interno, con el fin de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos.

- Cuatrimestralmente la Oficina de Control Interno presentará informes de seguimiento al Comité de Coordinación de Control Interno, con el fin de evidenciar si se materializó algún riesgo, si es necesario crear alguno nuevo o si se requiere eliminar alguno que con el tiempo no aplique a la Empresa.

8.6 Tabla de impactos institucional

Los criterios para calificar el impacto de los riesgos se harán de acuerdo con las opciones entregadas en la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* del Departamento Administrativo de la Función Pública - DAFP, en su última versión o en aquella que la modifique, complemente o sustituya.

Otros aspectos que la entidad considere necesarios deberán ser incluidos, con el fin de generar orientaciones claras y precisas para todos los funcionarios, de modo tal que la gestión del riesgo sea efectiva y esté articulada con la estrategia de la entidad.

8.7 Niveles de responsabilidad sobre la gestión y administración del riesgo

Además de las responsabilidades establecidas en la sección *8.5 Periodicidad para el monitoreo, revisión y seguimiento de los riesgos*, a continuación, se definen las siguientes por Línea de Defensa:

Línea de Defensa Estratégica

Responsables: Alta Dirección y Comité Institucional de Coordinación de Control Interno.

Responsabilidad frente al riesgo:

- Establecer y aprobar la política de administración del riesgo, la cual puede adoptar la forma de manual o guía de riesgos.
- Aprobar el Mapa de riesgos de la Empresa.
- Realizar seguimiento y análisis periódico a los riesgos.
- En caso de materializarse un riesgo de corrupción debe informarse a las instancias de control interno de la Empresa e iniciar la investigación disciplinaria correspondiente, si a ello hubiese lugar.
- Determinar los ajustes necesarios que se deban hacer frente a la gestión del riesgo.

Primera Línea de Defensa

Responsables: Líderes o responsables de los procesos.

Responsabilidad frente al riesgo:

- Revisar el mapa de riesgos por lo menos una vez en el año y actualizarlo si se requiere, previa aprobación en el Comité Institucional de Coordinación de Control Interno.
- Diseñar, implementar y monitorear los controles y gestionar de manera directa los riesgos, y proponer las mejoras a la gestión del riesgo a que haya lugar.
- Socializar al interior del equipo de trabajo el mapa de riesgos y sus controles.
- Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.

- Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
- Reportar cualquier novedad sobre los riesgos a la Oficina de Control Interno y al Comité Institucional de Coordinación de Control Interno.
- Entregar a la Subgerencia de Planeación y Administración de Proyectos (Segunda Línea de Defensa) y la Oficina de Control Interno (Tercera Línea de Defensa) el informe con los resultados del seguimiento.
- Dar a conocer a la Subgerencia de Planeación y Administración de Proyectos las apreciaciones y propuestas sobre los Riesgos de Corrupción que funcionarios y contratistas formulen, para su análisis e incorporación en caso de ser procedentes.

Segunda Línea de Defensa

Responsables: Subgerencia de Planeación y Administración de Proyectos – Líderes de la implementación de las Políticas establecidas en el Modelo Integrado de Planeación y Gestión -MIPG – Líderes o Coordinadores de otros sistemas de gestión de la Empresa.

Responsabilidad frente al riesgo:

- Asesorar a la línea estratégica en la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo y definición de controles en los temas a su cargo.
- Consolidar el Mapa de riesgos y presentarlo para análisis y aprobación del Comité Institucional de Coordinación de Control Interno.
- Monitorear los riesgos identificados y los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos y con la estructura de los temas a su cargo.
- Presentar los informes de monitoreo al Comité Institucional de Coordinación de Control Interno para monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos.
- Evaluar la coherencia de los riesgos con la presente política y verificar que sean monitoreados por la primera línea de defensa.
- Proponer las acciones de mejora a que haya lugar.

Tercera Línea de Defensa

Responsables: Oficina de Control Interno.

Responsabilidad frente al riesgo:

- Proporcionar un aseguramiento objetivo sobre la efectividad de la gestión del riesgo.
- Asesorar de forma coordinada con la Subgerencia de Planeación y Administración de Proyectos, y la Subgerencia de Gestión Corporativa, a la primera línea de defensa en la identificación de los riesgos y diseño de controles.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

- Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno.
- Recomendar mejoras a la política de administración del riesgo.