BOGOTÁ EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ D.C.	**Política de Administración de Riesgos**

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	14/08/2019	Documento original.
2	28/10/2020	Incluir el objetivo estratégico con el cual se alinea la política, inclusión de los criterios de riesgos de fraude, así como ajustes en el documento para unificar tiempos y especificar lineamientos de operación y responsabilidades en las líneas de defensa. Dada la emergencia por el Covid-19, este documento se entiende como validado y aprobado con el acta del Comité.

ELABORADO POR:	ESTANDARIZADO POR:	REVISADO Y APROBADO POR:
Holman Eduardo Barrera Espitia Gestor Junior Sistemas		Acta de Comité Institucional de Coordinación de Control Interno No. 4 del 28 de octubre de 2020
Maribel Carolina González Moreno Contratista Subgerencia de Planeación y Administración de Proyectos	**Esperanza Peña Quintero** Contratista Subgerencia de Planeación y Administración de Proyectos	**Comité Institucional de Coordinación de Control Interno**

Tabla de contenido

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 esta 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.

La Política de Administración de Riesgos contribuye al logro del objetivo No. 5 del Plan Estratégico 2020-2024 de la empresa, el cual se refiere a "*Construir una estructura de gobierno corporativo que involucre un modelo integrado de planeación y gestión orientado a procesos de gobierno abierto, generación de valor público, transparencia y bienestar, a través de una gestión pública efectiva*".

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.

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

Apetito del riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

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).

Fraude: aquella conducta intencional que desarrollen los colaboradores, consistente en la modificación, ajuste, cambio, alteración, reemplazo, ocultamiento, omisión o destrucción de información que deba ser revelada o soporte la actividad de la empresa, así como el engaño a terceros con información de la empresa y el uso indebido de información privilegiada.

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

Integridad: propiedad de exactitud y completitud.

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

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

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 fraude: para la empresa la materialización de cualquiera de las categorías o tipologías de fraude definidas en el presente documento se clasificará como riesgo de fraude y su tratamiento será de acuerdo con lo establecido para los riesgos de corrupción.

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.

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

- Identificar, gestionar, tratar, manejar, hacer seguimiento y evaluar los riesgos institucionales de la empresa articulándola con las demás políticas y planes existentes para contribuir al desempeño y asegurar razonablemente el logro de los propósitos y metas institucionales.

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

4. ALCANCE

Esta política contempla la administración de los riesgos de gestión, de corrupción, de fraude y de seguridad digital la cual aplica para las operaciones de todos los procesos de la Empresa.

5. NIVELES DE ACEPTACIÓN O TOLERANCIA DEL 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	Estrategia de Manejo
Riesgo de corrupción / fraude	Moderado	Inaceptable	Para EVITAR a toda costa su materialización, los líderes de proceso deberán realizar un seguimiento continuo 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 deben 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 en la herramienta dispuesta para la gestión y administración de riesgos.
	Alto	Inaceptable	
	Extremo	Inaceptable	
Riesgo de gestión	Bajo	Aceptable	Los líderes de proceso podrán ASUMIR los riesgos que quedan ubicados en esta zona, aplicando permanentemente los controles establecidos y las actividades propias del proceso asociado y realizando un seguimiento continuo. El registro de seguimiento se realizará cuatrimestralmente en la herramienta dispuesta para la gestión y administración de riesgos.
	Moderado	Aceptable	Los líderes de proceso deben establecer acciones de control que permitan REDUCIR la probabilidad de ocurrencia del riesgo. El registro de seguimiento se realizará cuatrimestralmente en la herramienta dispuesta para la gestión y administración de riesgos.
	Alto	Inaceptable	Los líderes de proceso deben establecer acciones de control que permitan REDUCIR la materialización del riesgo. El registro de seguimiento se realizará cuatrimestralmente en la herramienta dispuesta para la gestión y administración de riesgos.
	Extremo	Inaceptable	Los líderes de proceso deben establecer acciones de control que permitan EVITAR la materialización del riesgo, así como realizar un seguimiento continuo de los controles establecidos, 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 deben 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 en la herramienta dispuesta para la gestión y administración de riesgos.
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 en la herramienta dispuesta para la gestión y administración de riesgos.
	Moderado	Aceptable	Los líderes de proceso deben establecer acciones de control que permitan REDUCIR la probabilidad de ocurrencia del riesgo. El registro de seguimiento se realizará cuatrimestralmente en la herramienta dispuesta para la gestión y administración de riesgos.
	Alto	Inaceptable	Los líderes de proceso deben establecer acciones de control que permitan REDUCIR la materialización del riesgo.

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación	Estrategia de Manejo
			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 en la herramienta dispuesta para la gestión y administración de riesgos.
	Extremo	Inaceptable	Los líderes de proceso deben establecer acciones de control que permitan EVITAR la materialización del riesgo así como realizar un seguimiento continuo de los controles establecidos, 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 en la herramienta dispuesta para la gestión y administración de riesgos.

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.

Adicionalmente, los líderes de proceso 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.

De igual manera, los líderes de proceso ante la materialización de los riesgos que impliquen la interrupción de las operaciones se deben implementar los planes de contingencia y/o continuidad correspondientes.

Para mitigar/tratar los riesgos de seguridad digital se deben emplear como los controles del anexo A de la ISO/IEC 27001:2013 que apliquen.

6. NIVELES PARA CALIFICAR EL IMPACTO

Los líderes de proceso deben analizar y calificar el impacto 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.
- *Disminuir la probabilidad y el impacto*: acciones encaminadas a gestionar las causas del riesgo y 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 será evitar 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 los controles del anexo A de la ISO/IEC 27001:2013 que apliquen.

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

- Se deberán realizar, al menos una vez al año, actividades de capacitación y divulgación a todos los colaboradores de la empresa en gestión del riesgo para fortalecer la cultura de prevención y control.

- Los líderes de proceso deberán revisar el mapa de riesgos por lo menos una vez en el año y actualizarlo si se requiere, y una vez aprobado por el líder del proceso, enviarlo a través de correo institucional a la Subgerencia de Planeación y Administración de Proyectos para su consolidación y publicación en la ERUNET y 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.

- Como resultado del seguimiento realizado por el líder del proceso al mapa de riesgos, se podrá en cualquier momento eliminar, incluir o modificar riesgos, ajustar su análisis, valoración, acciones, indicadores, responsables, tiempos, entre otros, con la debida justificación. Los ajustes realizados y aprobados por el líder del proceso deberán ser remitidos a través de correo institucional a la Subgerencia de Planeación y Administración de Proyectos para su consolidación y publicación en la ERUNET y 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.

- La Subgerencia de Planeación y Administración de Proyectos deberá consolidar y publicar el Mapa de riesgos de la Empresa en la ERUNET y 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 empresa 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. De igual manera, ante la materialización de los riesgos que impliquen la interrupción de las operaciones se deben implementar los planes de contingencia y/o continuidad correspondientes.

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

- 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.

- A continuación, se describen las categorías que permitirá determinar los riesgos de fraude a los que la empresa se encuentra expuesta:

Categoría	Definición
Malversación de Activos	Uso indebido de recursos, sin autorización alguna, a operaciones o actividades diferentes a las pactadas inicialmente por la empresa.
Conflicto de Intereses	Cuando exista un interés particular, propio o de un tercero, directo o indirecto en su regulación, gestión, control o decisión, que pueda oponerse al mejor interés de la Empresa. En este caso, el colaborador de la empresa tiene la obligación legal de declararse impedido.
Omisión de controles	Omitir de forma intencionada el cumplimiento de alguno o todos los controles establecidos en la empresa, obteniendo así un beneficio para sí mismo o para un tercero.
Soborno	Cuando una persona da u ofrece dádivas para que se realice u omita un acto propio del cargo de un funcionario público, o para que se ejecute uno contrario a sus funciones.
Hurto	Apropiación indebida por parte de un servidor o tercero de propiedad física, financiera o intelectual de la empresa.
Suplantación de identidad	Consiste en hacerse pasar por otra persona para obtener un provecho para sí o para otro, o causar daño.
Daño o alteración no autorizada de activos de información	Cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos de los activos de información de la empresa.
Falsedad en documentación	Alteración o falsificación de los elementos esenciales de un documento, para obtener algún beneficio de la empresa.

- Los eventos identificados que impliquen fraude o posible riesgo de fraude serán tratados de acuerdo con la metodología establecida para los riesgos de corrupción 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.

- Los eventos identificados que impliquen fraude o posible riesgo de fraude serán investigados con el fin de establecer las responsabilidades a que haya lugar y tomar las medidas administrativas pertinentes.

- La empresa pone a disposición de sus colaboradores y de terceros, todos los canales de comunicación que permitirán obtener información sobre la potencial ocurrencia de prácticas de corrupción y fraude, internas o externas.

- Todo colaborador de la empresa está obligado a comunicar a través de cualquiera de los canales de comunicación, todo acto irregular de otro colaborador o tercero, que afecte o pueda lesionar los intereses de la empresa, así como cualquier situación de fraude y actos de corrupción.

- Las denuncias o quejas sobre situaciones de fraude y actos de corrupción que se reciban por cualquier canal de comunicación se deberán remitir al Defensor del Ciudadano y a la Oficina de Control Interno.

- El Defensor del Ciudadano es el responsable de consolidar y generar los informes sobre denuncias o quejas sobre situaciones de fraude y actos de corrupción que se reciban para presentaros a la Alta Dirección.

- La empresa no tomará represalias contra los colaboradores y terceros que denuncien hechos sospechosos y mantendrá su confidencialidad.

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 los líderes de procesos revisarán completamente el mapa de riesgos, y para ello tomarán como insumo:

  a. Los resultados de las auditorías realizadas por la Oficina de Control Interno y Organismos de Control.
  b. Lo reportado en los Comités de Autoevaluación y Seguimiento en relación a la administración de riesgos.
  c. Informes de evaluación independiente del Sistema de Administración de Riesgos de la Empresa.
  d. 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 líder del proceso y su equipo de trabajo, y si lo requiere 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.

- Cuatrimestralmente y dentro de los 5 primeros días hábiles posteriores al cierre, los líderes de proceso realizarán la revisión y seguimiento correspondiente y entregará a la Oficina de Control Interno y 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.

- Cuatrimestralmente la Subgerencia de Planeación y Administración de Proyecto elaborará los informes de monitoreo en el marco de la segunda línea de defensa y los presentará al Comité de Coordinación de Control Interno, cuando éstos impliquen toma de decisiones por la Alta Dirección.

- Cuatrimestralmente la Oficina de Control Interno evaluará el estado del Sistema de Administración de Riesgos y presentará informes de seguimiento al Comité de Coordinación de Control Interno, con el fin de evidenciar si se materializó algún riesgo, si es necesario actualizar los mapas de riesgos o si se requiere eliminar alguno que con el tiempo no aplique a 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 empresa 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.

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.

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.
- Definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento.
- Realizar seguimiento y análisis periódico a los riesgos, y emitir instrucciones sobre las acciones apropiadas para la mejora, cuando aplique.
- Revisar los cambios en el direccionamiento estratégico y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Determinar los ajustes necesarios que se deban hacer frente a la gestión del riesgo.
- Solicitar las intervenciones e informes necesarios a las diferentes dependencias con el fin de facilitar la toma de decisiones.
- Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones para su fortalecimiento.

Primera Línea de Defensa

Responsables: Líderes o responsables de los procesos.

Responsabilidad frente al riesgo:

- Identificar y valorar los riesgos que pueden afectar los procesos a su cargo y diseñar, implementar y monitorear los controles que permitan gestionar de manera directa los riesgos.
- Identificar riesgos de servicios o actividades tercerizadas, cuando aplique.
- Revisar el mapa de riesgos por lo menos una vez en el año y actualizarlo si se requiere, y una vez aprobado por el líder del proceso, enviarlo a través de correo institucional a la Subgerencia de Planeación y Administración de Proyectos para su publicación en la ERUNET quienes solicitarán 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.
- 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 trimestralmente 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 cuatrimestralmente 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, el cual incluirá el análisis de los riesgos y los controles para determinar si requiere de algún ajuste.
- 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.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar los planes de mejoramiento 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.
- Proponer mejoras a la gestión del riesgo de su proceso.
- Revisar y analizar los informes de evaluación y auditoria en materia de riesgos, y tomar las acciones necesarias que correspondan.
- 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. De igual manera, ante la materialización de los riesgos que impliquen la interrupción de las operaciones se deben implementar los planes de contingencia y/o continuidad correspondientes.

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.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos.
- 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 revisar la gestión del riesgo y la efectividad de los controles establecidos, cuando éstos impliquen toma de decisiones por la Alta Dirección.
- Revisar y analizar los informes de evaluación y auditoria en materia de riesgos, y tomar las acciones necesarias que correspondan.
- 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 una evaluación objetiva y razonable sobre la efectividad de la gestión del riesgo y control en todas sus etapas, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
- 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 acerca de las metodologías, herramientas y técnicas para la identificación y administración de los riesgos y 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 y fraude.
- 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 la evaluación independiente de la gestión de los riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno y publicarlos en la página web de la empresa.
- Recomendar mejoras a la política de administración del riesgo.
- Identificar y evaluar cambios que podrían tener impacto significativo en el sistema de control interno que se identifiquen durante evaluaciones periódicas de riesgos y en los trabajos de auditoría interna.
- Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Promover ejercicios de autocontrol para que cada proceso monitoree los niveles de eficiencia, eficacia y efectividad de los controles.
- Revisar cuatrimestralmente el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para su fortalecimiento
- Revisar de manera independiente la adecuada definición y 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 perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.