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.
3	07/10/2021	Actualización de la Política, de acuerdo con los nuevos lineamientos establecidos en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* del Departamento Administrativo de la Función Pública – DAFP del 2020.

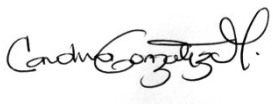
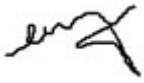
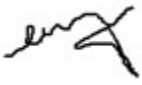
ELABORADO POR:		**REVISADO Y ESTANDARIZADO POR:**	**APROBADO POR:**
			Acta de Comité Institucional de Coordinación de Control Interno No. 04 del 7 de octubre de 2021
Maribel Carolina González Moreno Contratista Subgerencia de Planeación y Administración de Proyectos	**Lady Vanesa López Tovar** Contratista Subgerencia de Planeación y Administración de Proyectos	**Osiris Viñas Manrique** Gerente 039 Subgerencia de Planeación y Administración de Proyectos	
			
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 Coordinación de Control Interno**

Tabla de contenido

1. PRESENTACIÓN

La Empresa, con el liderazgo de la Alta Dirección se compromete a gestionar de manera efectiva los riesgos de gestión, de corrupción y de seguridad de la información, que pueden afectar el logro de la misión, objetivos estratégicos, planes, programas, proyectos y procesos, a través de la aplicación de la **Política para la Administración del Riesgo**, identificando los riesgos, determinando y aplicando las acciones oportunas y efectivas de control tanto detectivas como preventivas, que contribuyan a evitar la materialización y definir actuaciones de contingencia inmediatas que permitan, en caso de eventualidades, mitigar las posibles consecuencias con el fin de mantener los niveles de riesgo aceptables.

Por lo anterior, este documento se constituye en la guía que establece los lineamientos que orienten las acciones necesarias para gestionar los riesgos a los cuales está expuesta la Empresa.

Finalmente, es importante precisar, que esta política está incluida y articulada con 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.

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

Apetito del riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

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

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

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

Control: medida que permite reducir o mitigar un riesgo).

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 y Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. Diciembre de 2020.

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 diseño, implementación y cambio asegurando en todo momento que se dispone de las métricas necesarias para su correcta monitorización, evaluación y eventual mejora.

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

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

Plan de contingencia[2]: procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio. Se enmarca dentro del Plan de Continuidad de Negocio y se consideraría un control correctivo.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Puntos de riesgo: son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

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 de la información: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo inherente: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo residual: resultado de aplicar la efectividad de los controles al riesgo inherente.

[2] Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC.

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

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 de la información, la cual aplica para las operaciones de todos los procesos de la Empresa.

5. NIVELES DE ACEPTACIÓN DEL RIESGO

De acuerdo con lo establecido en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* del DAFP del 2020, se definen 4 zonas de severidad en la matriz de calor, a través de la combinación entre la probabilidad y el impacto:

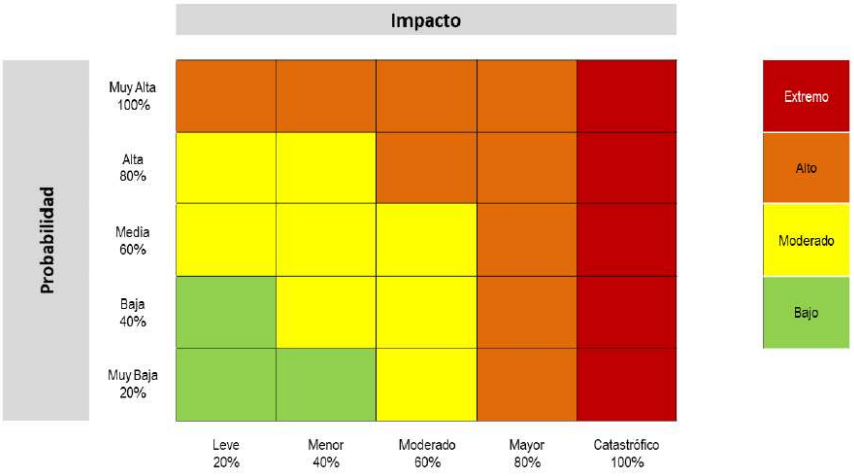


Figura 1. Matriz de calor (niveles de severidad del riesgo)
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2018, (adaptada).

De acuerdo con lo anterior, el nivel de riesgo que la empresa puede aceptar, que podría permitir el logro de los objetivos institucionales se describe a continuación.

- Para los riesgos que se encuentren en **zona de riesgo baja**, la Empresa está dispuesta a **aceptar** el riesgo, conociendo los efectos de su posible materialización y para los cuales no se requiere la definición y valoración de controles, sin embargo, se deben monitorear conforme a la periodicidad establecida.

- Para los riesgos calificados de **zona modera a extrema**, se deben establecer los controles que los mitiguen o reduzcan y se deben monitorear conforme a la periodicidad establecida.

- Los riesgos asociados a posibles actos de corrupción **no admiten aceptación** del riesgo y se deben definir los lineamientos para su tratamiento. De igual manera, se deben monitorear conforme a la periodicidad establecida.

- 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.

- Los líderes de proceso ante la materialización de los riesgos que impliquen la interrupción de las operaciones deben implementar los planes de contingencia y/o continuidad correspondientes.

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

6. ESTRUCTURA PARA LA GESTIÓN Y ADMINISTRACIÓN DEL RIESGO

Metodología a utilizar

La metodología definida será la contemplada en la *Guía para la administración del riesgo 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. A continuación. se presenta la estructura general de la metodología, para poder tener una visión global y entendimiento de la misma, a la hora de identificar los riesgos:

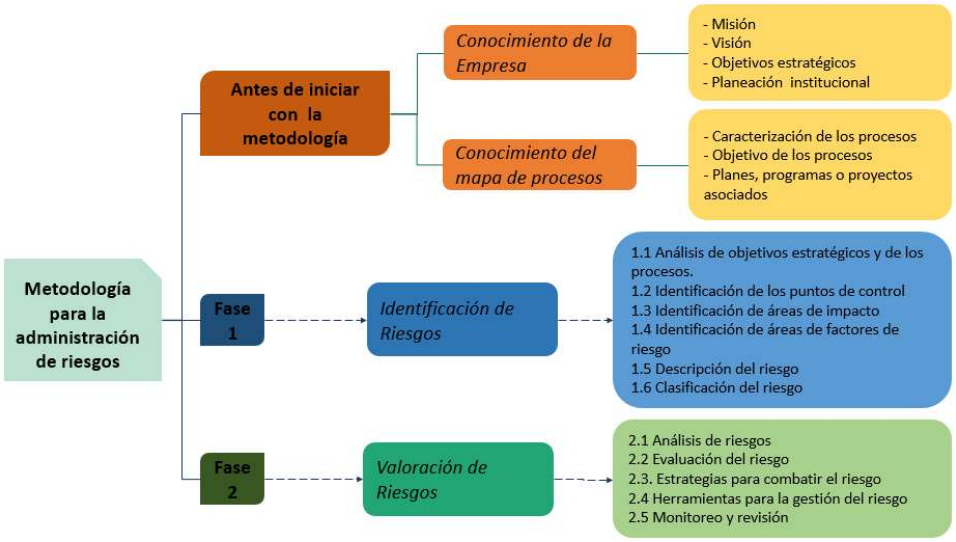


Figura 2. Metodología para la administración del riesgo
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2018, (adaptada).

Herramienta a utilizar

La herramienta dispuesta para la gestión y administración de riesgos es Excel, adaptando la matriz que pone a disposición el Departamento Administrativo de la Función Pública – DAFP, la cual cumple con todos los estándares para la administración de riesgos bajo la nueva metodología.

Lineamientos o políticas de operación

- La Subgerencia de Planeación y Administración de Proyectos, en coordinación y apoyo de la Oficina de Control Interno y la Subgerencia de Gestión Corporativa, 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.

- La actualización de los mapas de riesgos se debe realizar de manera permanente dado su naturaleza, los cambios en el contexto, actividades de comunicación y consulta, el seguimiento realizado por el líder del proceso, el ejercicio de monitoreo, entre otros, por lo cual es importante que como mínimo éstos sean actualizados al menos una vez en cada vigencia, así:

    - **Riesgos de corrupción**: en diciembre de cada vigencia, debido a que deben ser publicados 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.
    - **Riesgos de gestión y de seguridad de la información**: en el primer trimestre de cada vigencia, permitiendo así su oportuna socialización a los interesados y realizar respectivamente sus seguimientos y monitoreos.

- Los líderes de proceso son los responsables de aprobar las actualizaciones de los mapas de riesgos y de enviarlos 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. En caso de presentarse eliminaciones de riesgos, se debe enviar la respectiva justificación.

- 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.

- Los riesgos de seguridad de la información se deben gestionar de acuerdo con los criterios diferenciales descritos en el Modelo de Seguridad y Privacidad de la Información de la empresa.

- Se deben identificar riesgos de corrupción en trámites y otros procedimientos administrativos – OPA, de acuerdo con los lineamientos dados por el Departamento Administrativo de la Función Pública y por la Secretaría General de la Alcaldía Mayor de Bogotá.

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

- 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.

- 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 correspondientes. Los Planes de mejoramiento estarán documentados de acuerdo con lo establecido en el proceso Evaluación y Seguimiento.

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

- 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.

- 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 y de manera especial, en la página web de la Empresa se dispone del botón de visible para que los ciudadanos puedan presentar las denuncias por posibles actos de corrupción, existencia de inhabilidades, incompatibilidades o conflicto de intereses. De igual manera, en cumplimiento del principio de armonización de canales, la Secretaría General de la Alcaldía Mayor de Bogotá, D. C., pone a disposición los siguientes canales:

    - *Línea 195*; por este canal los usuarios tienen la posibilidad de presentar denuncias, y obtener orientación personalizada frente a sus casos, con el fin de registrar y direccionar adecuadamente las solicitudes.
    - *Sistema Distrital para la Gestión de Peticiones Ciudadanas – "Bogotá te escucha"*; a través de la ruta https://bogota.gov.co/sdqs/denuncias-por-actos-de-corrupcion
    - Puntos de atención al ciudadano presencial de las entidades distritales.
    - Red CADE.
    - De manera física en las oficinas de correspondencia de las entidades distritales.

- 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 presentarlos a la Alta Dirección.

- La empresa no tomará represalias contra los colaboradores y terceros que denuncien hechos sospechosos y mantendrá su confidencialidad, con el fin de proteger su identidad e integridad.

- 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 y sólo aplica para riesgos de gestión o de seguridad de la información.

Periodicidad para el monitoreo, revisión y seguimiento de los riesgos

El monitoreo, revisión y seguimiento de los riesgos 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, establecido en la Circular ERU 009 de 2017.
  c. Informes de evaluación independiente del Sistema de Administración de Riesgos de la Empresa.
  d. Las novedades o recomendaciones del Comité Institucional de Coordinación de Control Interno.
  e. Los informes de monitoreo.

  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.

- Los líderes de proceso deben realizar cuatrimestralmente el seguimiento a los mapas de riesgos y entregar el informe con los resultados obtenidos, dentro de los 5 primeros días hábiles posteriores al cierre, a la Oficina de Control Interno; el cual incluirá el análisis de los riesgos y los controles para determinar si requiere de algún ajuste.

- Cuando haya materialización de riesgos, los líderes de proceso deben hacer monitoreo mínimo una vez cada dos meses y hasta que se dé por finalizado el plan de mejoramiento establecido y se realice una nueva valoración del riesgo.

- La Subgerencia de Planeación y Administración de Proyecto cuatrimestralmente elaborará los informes de monitoreo como Segunda Línea de Defensa y los socializará a los líderes de proceso para la toma de acciones.

- 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, 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. Lo anterior en armonía con el seguimiento a los riesgos de corrupción y el Plan Anticorrupción y de Atención al Ciudadano.

7. NIVELES DE RESPONSABILIDAD SOBRE LA GESTIÓN Y ADMINISTRACIÓN DEL RIESGO

Además de las responsabilidades establecidas en la sección *6.4 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.
- 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.
- Socializar al interior del equipo de trabajo el mapa de riesgos y sus controles.
- Revisar y evaluar 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.
- 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 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.
- 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 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 éstos.
- 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.
- 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 Primera 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.

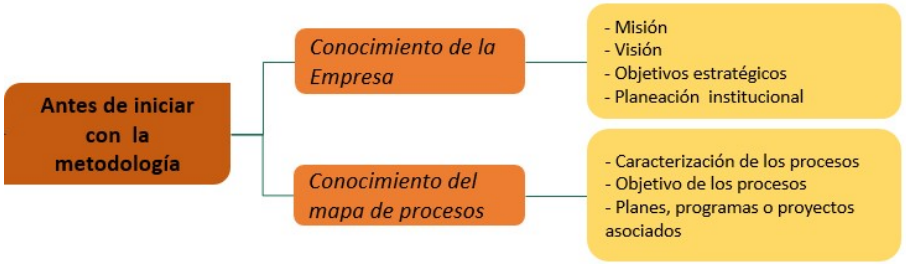
8. IMPLEMENTACIÓN DE LA HERRAMIENTA DISPUESTA PARA LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS

Con el fin de facilitar la implementación de la herramienta dispuesta para la gestión y administración de riesgos, cada campo contiene su descripción correspondiente como comentario, sin embargo, a continuación, se describen los pasos para la identificación de los riesgos y se detallan aquellos campos que requieren una ilustración o explicación más amplia.

Paso 1: Análisis de objetivos estratégicos y de los procesos

Para identificar los riesgos para cada uno de los procesos, se debe tener en cuenta el contexto estratégico en el que opera la empresa, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Por lo tanto, todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.



Nota: es importante que los objetivos estratégicos se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos.

El contexto se relaciona con las condiciones internas y externas que pueden generar eventos que afectan negativamente o positivamente al cumplimiento de la misión y objetivos de la empresa, a partir de los cuales, es posible establecer las causas de los riesgos a identificar en cada vigencia.

Con el fin de facilitar identificación del contexto interno, externo de la Empresa, en la siguiente tabla se describe cada uno de los contextos con sus factores asociados, a partir de los cuales se determina el contexto del proceso:

TIPO DE CONTEXTO	FACTOR
CONTEXTO EXTERNO *En éste se determinan las características o aspectos esenciales del entorno en el cual opera la empresa.* *Se pueden considerar factores como:*	**Políticos**: cambios de gobierno, legislación, políticas públicas, regulación.
	Económicos y financieros: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Sociales y culturales: demografía, responsabilidad social, orden público.
	Tecnológicos: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	Ambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Legales y reglamentarios: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO *En éste se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.* *Se pueden considerar factores como:*	**Financieros**: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	Personal: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	Procesos: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	Estratégicos: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	Comunicación Interna: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO *En éste se determinan las características o aspectos esenciales del proceso y sus interrelaciones.* *Se pueden considerar factores como:*	**Diseño del proceso**: claridad en la descripción del alcance y objetivo del proceso.
	Interacciones con otros procesos: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	Procedimientos asociados: pertinencia en los procedimientos que desarrollan los procesos.
	Responsables del proceso: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos.
	Activos de seguridad digital del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Tabla 1. Factores para cada categoría del contexto.
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2018.

Nota: El registro del Contexto del proceso, se debe diligenciar en la herramienta "**Mapa de oportunidades por proceso**".

Paso 2: Identificación de los puntos de riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

En la herramienta se debe diligenciar el campo **Frecuencia con la cual se realiza la actividad** y allí se deben escribir el número de veces con la que se lleva a cabo una actividad en el periodo de 1 año.

Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Tabla 2. Actividades relacionadas con la gestión en entidades públicas.
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2020.

De acuerdo con lo anterior, en la siguiente tabla se establecen los criterios para definir el nivel de probabilidad.

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Tabla 3. Criterios para definir el nivel de probabilidad.
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2020.

Paso 3: Identificación de áreas de impacto

Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo.

Paso 4: Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la herramienta se debe diligenciar el campo **Clasificación del Riesgo**. A continuación, se describen las categorías en las cuales se deben clasificar los riesgos:

Clasificación	Descripción
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

Clasificación	Descripción
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Tabla 4 Clasificación de riesgos.
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2020.

Ahora bien, para facilitar la clasificación de riesgos, a continuación, se definen un listado con ejemplo de factores generadores de riesgo y su interrelación con la clase de riesgo:

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal

Clasificación
Ejecución y administración de procesos

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Clasificación
Fraude externo

Factor	Definición		Descripción
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Clasificación
Daños a activos fijos/ eventos externos

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Factor	Definición		Descripción
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)

Clasificación
Fraude interno

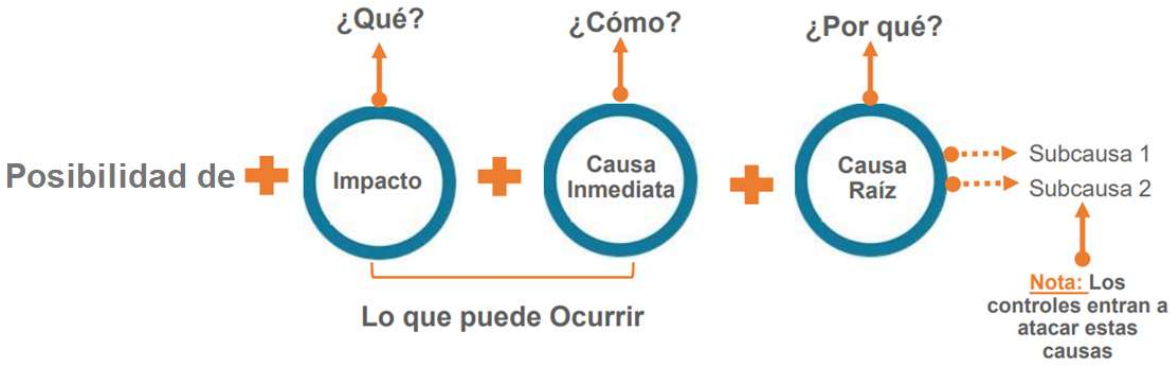
Factor	Definición		Descripción
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas

Clasificación
Fallas tecnológicas

Nota: Para el caso de ***Relaciones laborales*** y ***Usuarios, productos y prácticas***, pueden asociarse a varios factores.

Paso 5: Descripción del riesgo

Debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento. La siguiente es la estructura que se debe utilizar para facilitar su redacción y claridad se inicia con POSIBILIDAD DE:



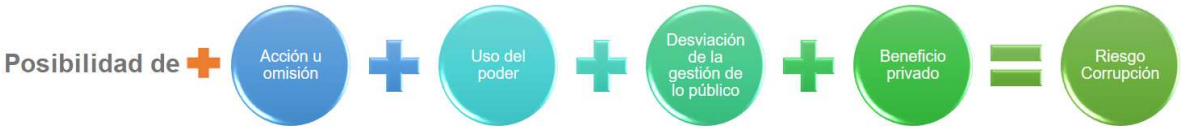
En la herramienta se deben diligenciar los siguientes campos, que facilitan la descripción del riesgo:

- **Impacto:** en este campo se selecciona si la consecuencia en caso de materializarse el riesgo es económica o reputacional.

- **Causa inmediata**: en este campo se deben describir las circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo. Dado que éstas son utilizadas para la redacción del riesgo de gestión, se recomienda no registrar más de dos causas inmediatas.

- **Causa raíz**: en este campo se debe describir la causa principal o la razón por la cual se puede presentar el riesgo. Dado que es utilizada para la redacción del riesgo de gestión y para la definición de controles en la etapa de valoración del riesgo, se recomienda no registrar más de dos causas raíz.

De otra parte, es importante tener en cuenta que para los riesgos de corrupción se debe respetar la siguiente estructura:



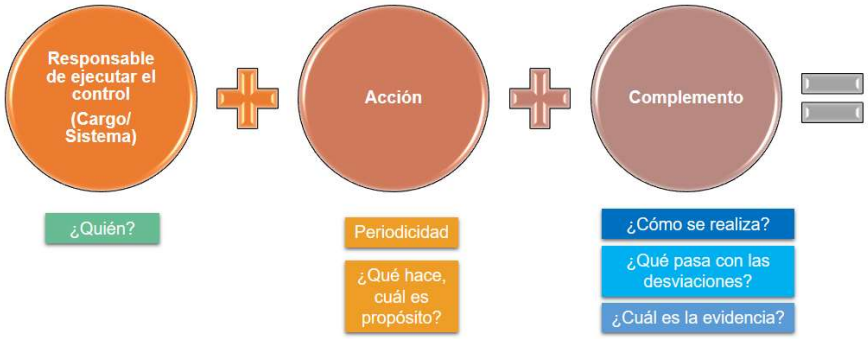
Paso 6: Valoración de riesgo

Para el establecimiento de la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgo inherente) se utilizarán la **Tabla de Probabilidad** y **Tabla de Impacto** establecidas en *la Guía para la administración del riesgo y el diseño de controles en entidades públicas* del DAFP 2020.

En la herramienta se deben diligenciar los campos de la sección "**Frecuencia con la cual se realiza la actividad**" la cual depende del dato reportado en el campo **Frecuencia con la cual se realiza la actividad** y de manera automática determina las zonas de riesgo.

Paso 7: Descripción del control

Los controles se deben redactar teniendo en cuenta las siguientes variables, para que mitigue de manera adecuada el riesgo:

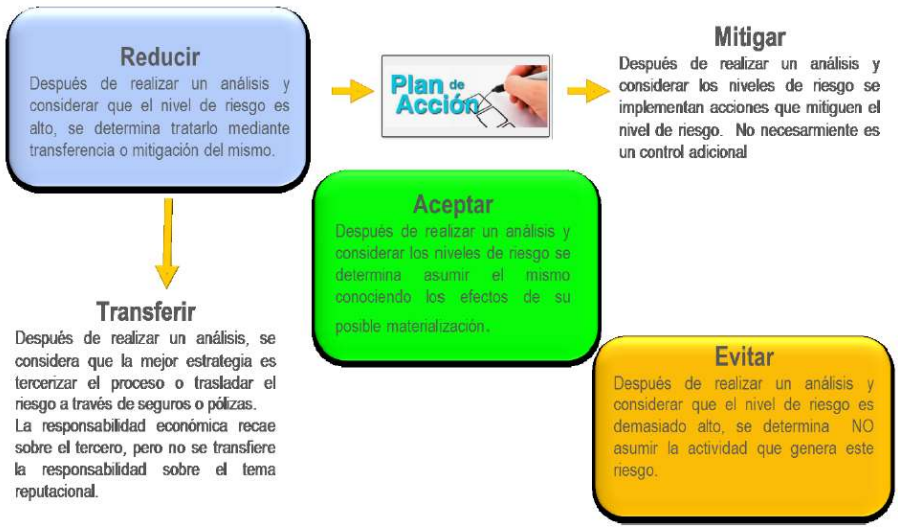


Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas. DAFP 20218.

Una vez definidos, se deben calificar los atributos para el diseño del control, teniendo en cuenta las características relacionadas con la eficiencia y la formalización de los mismos, en los campos de la herramienta que se encuentran bajo el título **Atributos** (*Tipo, Implementación, Documentación, Frecuencia, Evidencia*).

Paso 8: Estrategia para combatir el riesgo

La empresa adopta las *Estrategias para combatir el riesgo*, definidas en la Guía del DAFP:



Es importante mencionar, que cuando se seleccione la opción de reducir, se debe definir un plan de acción, para lo cual se deben diligenciar los siguientes campos en la herramienta:

- **Acción de Tratamiento**: en este campo se deben describir las medidas encaminadas a fortalecer los controles, a fin de mantener los riesgos en niveles tolerables.

- **Periodicidad de seguimiento**: cuando se plantee una **Acción de Tratamiento**, se deberá establecer la periodicidad de seguimiento de la misma, puede ser: diaria, semanal, mensual, anual, entre otras.

- **Fecha Inicio**: cuando se plantee una **Acción de Tratamiento**, se deberá establecer la fecha en la que se iniciará su ejecución. Cuando se trate de acciones permanentes, se puede diligenciar el campo con la palabra “Permanente”.

- **Fecha Fin**: cuando se plantee una **Acción de Tratamiento**, se deberá establecer la fecha en la que se finalizará su ejecución. Cuando se trate de acciones permanentes, se puede diligenciar el campo con la palabra “Permanente”.

- **Acción de Contingencia ante posible materialización**: en este campo se deben describir las acciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez materializado el riesgo, con el fin de garantizar la continuidad de las funciones críticas del proceso.