





**IDPAC**



# **GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DEL RIESGO**

|  |  |   |  |   |    |
|--|--|---|--|---|----|
|  <p>ALCALDÍA MAYOR<br/>DE BOGOTÁ D.C.</p> |  |   |  | <b>INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y<br/>ACCIÓN COMUNAL</b> |    |
| <b>SISTEMA INTEGRADO DE GESTIÓN</b>  |  |   |  |   |    |
| <b>GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DEL RIESGO</b>   |  |   |  |   |    |
| <b>CÓDIGO:</b>   |  | IDPAC-PE-GU-01  |  | <b>VERSIÓN</b>  | 07 |
| <b>ELABORÓ</b>   |  | <b>REVISÓ</b>   |  | <b>APROBÓ</b>   |    |
| Silvia Milena Patiño León<br>Nancy Patricia Gómez Martínez   |  | Claudia Milena Salcedo  |  | Comité Institucional de<br>Coordinación de Control<br>Interno       |    |
| Contratistas – Oficina Asesora de<br>Planeación  |  | Jefe Oficina Asesora de<br>Planeación   |  | Comité Institucional de<br>Coordinación de Control<br>Interno       |    |
| <b>FECHA</b>   |  | <b>FECHA</b>  |  | <b>FECHA</b>  |    |
| 15/03/2021   |  | 24/03/2021  |  | 26/03/2021  |    |

| <b>REGISTRO DE MODIFICACIONES</b> |                   |   |
|-----------------------------------|-------------------|---|
| <b>VERSIÓN</b>                    | <b>FECHA</b>      | <b>ÍTEM MODIFICADO – DESCRIPCIÓN</b>  |
| 01                                | 10/11/2008        | Versión Original. Nota: Se aclara que esta guía hacia parte del proceso de Mejoramiento continuo del mapa de procesos del IDPAC, la cual llevo a la versión 3   |
| 02                                | 24/05/2016        | Se actualiza la metodología para la identificación de riesgos y se incluyen lo relacionado con la administración de riesgos institucional, de corrupción y de contratación.                             |
| 03                                | 20/11/2016        | Actualización metodológica de acuerdo con el marco normativo vigente.   |
| 04                                | 27/08/2018        | Se actualiza la metodología debido a la actualización de la ficha técnica de riesgos.   |
| 05                                | 14-<br>16/08/2019 | Se actualiza la metodología para la administración del riesgo a partir de los lineamientos del Departamento Administrativo de la Función Pública y las características de la herramienta SIG participo. |

| <b>REGISTRO DE MODIFICACIONES</b> |              |   |
|-----------------------------------|--------------|---|
| <b>VERSIÓN</b>                    | <b>FECHA</b> | <b>ÍTEM MODIFICADO – DESCRIPCIÓN</b>  |
| 06                                | 20/05/2020   | Se reorganiza el documento con respecto a las fases de la metodología de administración del riesgo definidas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4 Dirección de Gestión y Desempeño Institucional. Octubre 2018 y el Manual Operativo del Modelo Integrado de Planeación y Gestión. Consejo para la Gestión y Desempeño Institucional. Versión 3. diciembre de 2019. |
| 07                                | 26/03/2021   | Se ajusta parcialmente de acuerdo con la Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 5 de diciembre 2020. Se ajusta la Declaración de la Política de Administración del Riesgo y se complementaron los objetivos y las definiciones, así mismo se incluye una tabla sobre las responsabilidades por Línea de Defensa  |

**TABLA DE CONTENIDO**

|   |           |
|---|-----------|
| <b>1. INTRODUCCIÓN</b>  | <b>6</b>  |
| <b>2. OBJETIVOS</b>   | <b>6</b>  |
| <b>2.1. Objetivo general</b>  | <b>6</b>  |
| <b>2.2. Objetivos específicos</b>   | <b>6</b>  |
| <b>3. ALCANCE</b>   | <b>7</b>  |
| <b>4. DEFINICIONES</b>  | <b>7</b>  |
| <b>5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO</b> | <b>11</b> |
| <b>6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO - DECLARACIÓN</b>             | <b>15</b> |
| <b>7. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS</b>                   | <b>15</b> |
| <b>7.1. CONTEXTO DE LA ENTIDAD</b>  | <b>16</b> |
| <b>7.2. IDENTIFICACIÓN DE LOS RIESGOS</b>                                 | <b>23</b> |
| <b>7.2.1. Identificar riesgos por proceso</b>                             | <b>23</b> |
| <b>7.2.2. Identificar la causa del riesgo</b>                             | <b>25</b> |
| <b>7.2.3. Descripción del riesgo</b>                                      | <b>26</b> |
| <b>7.2.4. Clasificación del riesgo</b>                                    | <b>30</b> |
| <b>7.3. ANÁLISIS DEL RIESGO</b>   | <b>30</b> |
| <b>7.3.1. Probabilidad del riesgo</b>                                     | <b>31</b> |
| <b>7.3.2. Impacto del riesgo</b>  | <b>31</b> |
| 7.3.2.1. Análisis del impacto legal y de cumplimiento                     | 32        |
| 7.3.2.2. Análisis del impacto operacional                                 | 32        |
| 7.3.2.3. Análisis del impacto de seguridad de la información              | 33        |
| 7.3.2.4. Análisis de impacto de los riesgos de corrupción                 | 34        |
| 7.3.2.5. Riesgo inherente   | 35        |
| <b>7.4. VALORACIÓN DEL RIESGO</b>   | <b>36</b> |
| <b>7.4.1. Diseño de controles</b>   | <b>36</b> |
| 7.4.1.1. Naturaleza del control   | 38        |
| <b>7.4.2. Valoración de controles</b>                                     | <b>38</b> |
| 7.4.2.1. Riesgo residual  | 40        |
| <b>7.4.3. Tratamiento del riesgo</b>                                      | <b>40</b> |
| 7.4.3.1. Determinación de la opción de tratamiento para el riesgo         | 41        |
| 7.4.3.2. Definición de acciones de contingencia.                          | 41        |



**IDPAC**



|            |   |           |
|------------|---|-----------|
| 7.4.3.3.   | Definición del semáforo del riesgo.                                       | 42        |
| 7.4.3.4.   | Definición de acciones asociadas.   | 42        |
| <b>8.</b>  | <b><i>MONITOREO DE LOS RIESGOS</i></b>                                    | <b>42</b> |
| <b>9.</b>  | <b><i>MODIFICACIONES PARA LOS RIESGOS IDENTIFICADOS</i></b>               | <b>43</b> |
| <b>10.</b> | <b><i>MAPA DE RIESGOS</i></b>   | <b>44</b> |
| <b>11.</b> | <b><i>DIILIGENCIAMIENTO DE LAS ETAPAS DEL RIESGO EN SIG PARTICIPO</i></b> | <b>44</b> |



**IDPAC**



## **1. INTRODUCCIÓN**

La presente guía establece la Política de Administración de Riesgos del Instituto Distrital de la Participación y Acción Comunal - IDPAC. Así como, los lineamientos metodológicos para la identificación, análisis, valoración, evaluación y tratamiento a los riesgos que puedan afectar el cumplimiento de la misión, de los objetivos estratégicos, la gestión de los procesos y la satisfacción de los grupos de interés, de acuerdo con las directrices del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de la línea estratégica y líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI – Dimensión 7 Control Interno y los requerimientos de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 5, esta última de manera parcial hasta tanto se actualice el aplicativo SIG participo en el módulo de riesgos. Actualización que está en proceso por parte del proveedor.

## **2. OBJETIVOS**

### **2.1. Objetivo general**

Establecer los lineamientos para la administración del riesgo en el Instituto Distrital de la Participación y Acción Comunal - IDPAC, de acuerdo con los lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP) en la Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 5, la Norma Técnica Colombiana NTC ISO 31000. Gestión del Riesgo. Principios y Directrices., los requisitos de la norma ISO 27001:2013, la norma ISO 14001 Sistemas de Gestión Ambiental y la normatividad relacionada con la Gestión Ambiental y de Seguridad y Salud en el Trabajo

### **2.2. Objetivos específicos**

- Establecer una metodología integral para la administración de riesgos, de acuerdo con el marco normativo vigente que tenga en cuenta los riesgos de gestión, de corrupción, de seguridad digital, ambiental y de seguridad y salud en el trabajo.
- Dar a conocer el marco general de actuación para la gestión de los riesgos, mediante lineamientos metodológicos para identificar, analizar, valorar, establecer controles, responsables y formular los planes de tratamiento de los riesgos de gestión
- Comunicar a todos los niveles del IDPAC los lineamientos sobre la gestión del riesgo, para comprometer a todos los servidores públicos en la aplicación de la metodología propuesta en la presente guía.
- Asignar responsabilidades y línea estratégica y líneas de defensa para la identificación, formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos de la entidad. Así como su seguimiento y reporte
- Establecer lineamientos para el monitoreo y evaluación de los controles propuestos para la mitigación de los riesgos a partir de la implementación de los lineamientos metodológicos de la presente guía.

### 3. ALCANCE

La guía de administración de riesgos es aplicable a todos los procesos identificados en el Sistema Integrado de Gestión del Instituto Distrital de la Participación y Acción Comunal y en todos los niveles del Instituto.

### 4. DEFINICIONES

Para la administración del riesgo en el Instituto Distrital de la Participación y Acción Comunal, se tendrán en cuenta los siguientes términos y definiciones:

| <b>TÉRMINO</b>                   | <b>DEFINICIÓN</b>  |
|----------------------------------|--|
| <b>ACTIVO</b>                    | En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.                               |
| <b>ADMINISTRACIÓN DE RIESGOS</b> | Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.  |
| <b>AMENAZA</b>                   | Situación externa que no controla la entidad y que puede afectar su operación.   |
| <b>APETITO DE RIESGO:</b>        | Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. |
| <b>CALIFICACIÓN DEL RIESGO</b>   | Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.   |
| <b>CAPACIDAD DE RIESGO:</b>      | Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.   |
| <b>CAUSA</b>                     | Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo<br><br>Medios, circunstancias y/o agentes que generan riesgos  |
| <b>CAUSA INMEDIATA</b>           | Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.  |
| <b>CAUSA RAÍZ</b>                | Causa principal o básica, corresponde a las razones por la cuales se puede presentar   |
| <b>CONFIDENCIALIDAD</b>          | Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados  |

| <b>TÉRMINO</b>                       | <b>DEFINICIÓN</b>   |
|--------------------------------------|---|
| <b>CONSECUENCIA</b>                  | Son 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.  |
| <b>CONTROL</b>                       | Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia o el impacto del riesgo.<br><br>Medida que permite reducir o mitigar un riesgo.  |
| <b>CONTROL PREVENTIVO</b>            | Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.  |
| <b>CONTEXTO DE LA ORGANIZACIÓN</b>   | Corresponde a la determinación de las cuestiones externa e internas que son pertinentes para la gestión institucional y que pueden afectar el logro de los resultados previstos.  |
| <b>DEBILIDAD</b>                     | Situación interna que la entidad puede controlar y que puede afectar su operación.  |
| <b>DISPONIBILIDAD</b>                | Propiedad de ser accesible y utilizable a demanda por el riesgo.  |
| <b>EVALUACIÓN DEL RIESGO</b>         | Resultado del cruce cuantitativo de la calificación de impacto y probabilidad, para establecer la zona donde se ubicará el riesgo.  |
| <b>FACTORES DE RIESGO</b>            | Son las fuentes generadoras de riesgos  |
| <b>FRECUENCIA</b>                    | Ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.  |
| <b>IDENTIFICACIÓN DEL RIESGO</b>     | Etapas de administración del riesgo donde se definen los riesgos con sus causas, agentes generadores asociados a las causas, consecuencias, definición de productos y/o servicios que pueden afectarse con la materialización del riesgo, situaciones de daño antijurídico y clasificación.   |
| <b>IMPACTO</b>                       | Las consecuencias que puede ocasionar a la organización la materialización del riesgo.  |
| <b>INTEGRIDAD</b>                    | Propiedad de exactitud y completitud  |
| <b>MAPA DE RIESGOS</b>               | Organización sistemática que muestra el desarrollo de las etapas de la administración del riesgo.   |
| <b>MAPA DE RIESGOS DE CORRUPCIÓN</b> | Herramienta metodológica para identificar un conjunto sistemático de situaciones de índole administrativa que, por sus características, pueden originar prácticas corruptas, orientan programas de prevención de la corrupción, constituye una opción en la labor de los administradores cuando enfrentan la dirección o conducción de una organización o entidad particular. |
| <b>MATERIALIZACIÓN DEL RIESGO</b>    | Ocurrencia del riesgo identificado.   |
| <b>NIVEL DE RIESGO</b>               | 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  |



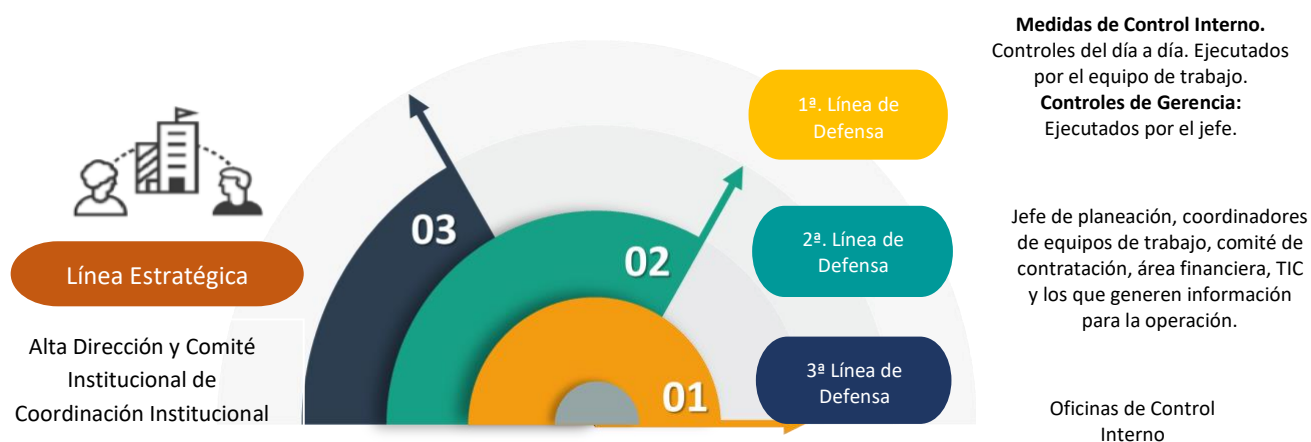
| <b>TÉRMINO</b>                                  | <b>DEFINICIÓN</b>   |
|---|---|
|   | <p>alcanzar los objetivos.</p> <p>En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.</p>   |
| <b>OBSERVACIONES O DESVIACIONES DEL CONTROL</b> | <p>Hace referencia a las acciones que deben tomarse, una vez se aplica el control y se evidencia algún incumplimiento en el proceso controlado; la actividad no debería continuarse hasta que se subsane la situación; si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Ej. El sistema SAP, cada vez que se va a realizar un pago, valida que el proveedor al cual se le va girar el pago, no está reportado en listas restrictivas, comparando el número de identificación tributaria (NIT) o cédula, con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo.</p> <p>En caso de encontrar coincidencias, el sistema no permite realizar el pago.</p> |
| <b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>    | <p>Conjunto de lineamientos, directrices definidas y adoptadas para la gestión del riesgo en la entidad. La política es la declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.</p> <p>La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.</p>  |
| <b>PROBABILIDAD</b>                             | <p>se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.</p> <p>Medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.</p>  |
| <b>PROCESO</b>                                  | <p>Conjunto de operaciones secuenciales que realiza permanentemente la entidad para generar productos/servicios a sus usuarios internos y externos a partir de unos insumos determinados.</p>   |
| <b>PRODUCTO Y/O SERVICIO</b>                    | <p>Cualquier bien material o servicio final que se genera con la operación de un proceso institucional, orientado a satisfacer la necesidad de un grupo de valor interno o externo.</p>   |
| <b>REQUISITOS LEGALES Y OTROS REQUISITOS</b>    | <p>Necesidad o expectativa establecida, generalmente implícita u obligatoria que una organización debe cumplir y otros que una organización decide cumplir.</p>   |

| <b>TÉRMINO</b>   | <b>DEFINICIÓN</b>   |
|--|---|
| <b>REDUCIR EL RIESGO</b>                                   | Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados.   |
| <b>RIESGO</b>  | Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.<br>Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.<br>Evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias. |
| <b>RIESGO DE CORRUPCIÓN</b>                                | Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.   |
| <b>RIESGO DE GESTIÓN</b>                                   | Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos de los procesos o sobre su operación.   |
| <b>RIESGO DE SEGURIDAD DIGITAL</b>                         | 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.   |
| <b>RIESGO DE SEGURIDAD Y SALUD EN EL TRABAJO</b>           | Son aquellos eventos que puedan afectar la seguridad y la salud en los espacios laborales.  |
| <b>RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> | 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).   |
| <b>RIESGO INHERENTE</b>                                    | 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.   |
| <b>RIESGO RESIDUAL</b>                                     | El resultado de aplicar la efectividad de los controles al riesgo inherente.<br>Nivel de riesgo que permanece luego de determinar controles para su administración.   |
| <b>SIG PARTICIPO</b>                                       | Herramienta oficial para la documentación y administración de los riesgos mediante el módulo de “Gestión del riesgo”.   |
| <b>TOLERANCIA DEL RIESGO.</b>                              | Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad  |

| TÉRMINO   | DEFINICIÓN   |
|---|--|
| <b>VALORACIÓN DEL RIESGO</b>                          | Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir y si es necesario, las acciones a desarrollar para el fortalecimiento de controles. |
| <b>VULNERABILIDAD</b>                                 | Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.  |
| <b>PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO</b> | Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal   |

## 5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de la Alta dirección y sus directivos, servidores públicos, y contratistas y/o diferentes grupos de interés o partes interesadas; por esto, es preciso identificar los actores que intervienen, de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión, a partir de la estructuración de las líneas de defensa que se presentan a continuación a partir de las definiciones del MIPG:



**Ilustración 1** Roles y responsabilidades frente a la administración del riesgo.

## RESPONSABILIDADES – LINEAS DE DEFENSA

La responsabilidad frente a la gestión del riesgo está definida mediante las líneas de defensa, así:

| LÍNEA                           | RESPONSABLE   | RESPONSABILIDAD FRENTE AL RIESGO  |
|---------------------------------|---|---|
| <b>LÍNEA ESTRATÉGICA</b>        | <b>ALTA DIRECCIÓN</b><br><br>Comité Directivo<br>Comité de Gestión y Desempeño Institucional<br>Comité Institucional de Control Interno | <ol style="list-style-type: none"> <li>1. Definir y aprobar la política para la administración del riesgo</li> <li>2. Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo).</li> <li>3. Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles.</li> <li>4. Analizar los riesgos, vulnerabilidades, amenazas que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad, gestión de los procesos y capacidades para prestar servicios.</li> <li>5. Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento del plan estratégico</li> </ol>  |
| <b>PRIMERA LÍNEA DE DEFENSA</b> | Líderes de Proceso<br>Secretario General<br>Subdirectores (as)<br>Jefe de Oficina Gerencias<br>Responsable del proyecto                 | <ol style="list-style-type: none"> <li>1. Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a los procesos.</li> <li>2. Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión.</li> <li>3. Ejecutar y 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.</li> <li>4. Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo.</li> <li>5. Reportar en el SGI los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.</li> </ol> |
| <b>SEGUNDA LINEA DE DEFENSA</b> | Oficina Asesora de Planeación   | <ol style="list-style-type: none"> <li>1. Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual.</li> <li>2. Consolidar el mapa de riesgos, riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo</li> </ol>  |

| LÍNEA                                  | RESPONSABLE  | RESPONSABILIDAD FRENTE AL RIESGO   |
|--|--|--|
|  |  | <p>para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno</p> <ol style="list-style-type: none"> <li>3. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo.</li> <li>4. Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente.</li> <li>5. Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.</li> <li>6. Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.</li> <li>7. Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.</li> </ol>   |
| <p><b>SEGUNDA LINEA DE DEFENSA</b></p> | <p>Secretario General,<br/>Coordinadores de Gestión<br/>Coordinadores de los equipos de trabajo:<br/>Administrativa,<br/>Financiera,<br/>Servicio al Ciudadano,<br/>Gestión Documental,<br/>Talento Humano<br/>Responsable del proyecto<br/>Supervisores<br/>Comité de contratación<br/>Delegados de riesgos en cada proceso</p> | <ol style="list-style-type: none"> <li>1. Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles bajo su responsabilidad y los temas a su cargo.</li> <li>2. Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.</li> <li>3. Realizar el seguimiento al mapa de riesgos de su proceso.</li> <li>4. Reportar en el módulo de riesgos del aplicativo SIG participo o delegar a un profesional de la dependencia, el registro de los avances en la gestión del riesgo.</li> <li>5. Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo.</li> <li>6. Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su proceso o responsabilidad.</li> <li>7. Participar en las pruebas del plan de continuidad de negocio y en la implementación</li> <li>8. Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico bajo responsabilidad del Jefe de la Oficina Jurídica</li> <li>9. Comunicar al equipo de trabajo a su cargo la</li> </ol> |

| LÍNEA                           | RESPONSABLE                | RESPONSABILIDAD FRENTE AL RIESGO   |
|---------------------------------|----------------------------|--|
|                                 |                            | responsabilidad y resultados de la gestión del riesgo.   |
| <b>TERCERA LÍNEA DE DEFENSA</b> | Oficina de Control Interno | <ol style="list-style-type: none"> <li>1. Brindar asesoría, orientación técnica, evaluación y seguimiento a la gestión del riesgo</li> <li>2. Brindar asesoría a los responsables y ejecutores de los procesos y proyectos (primera línea de defensa), respecto a metodologías y herramientas para la identificación, análisis y evaluación de riesgos, como complemento a la labor de acompañamiento que deben desarrollar las oficinas de planeación o comités de riesgos (segunda línea de defensa)</li> <li>3. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.</li> <li>4. Pronunciarse sobre la pertinencia y efectividad de los controles. Recomendar mejoras a la política de operación para la administración del riesgo</li> <li>5. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa</li> <li>6. Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles.</li> <li>7. Señalar aquellos aspectos que consideren una amenaza para el cumplimiento de los objetivos de los procesos y, por ende, los objetivos y metas institucionales, en el marco de la evaluación independiente.</li> </ol> |

De igual manera, la Oficina Asesora de Planeación lleva a cabo las siguientes acciones:

- Socializar anualmente la metodología de riesgos.
- Capacitar al grupo de trabajo de cada dependencia en la herramienta SIG participo para la gestión del riesgo
- Liderar las mesas de trabajo de identificación del riesgo
- Socializar y publicar el mapa de riesgos de gestión y de corrupción.

Por su parte, los líderes de proceso tienen la responsabilidad de:



**IDPAC**



- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa
- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán del monitoreo, reporte y socialización del riesgo asociados.

## 6. POLITICA DE ADMINISTRACIÓN DEL RIESGO - DECLARACIÓN

***“La alta dirección y el personal en general del Instituto Distrital de la Participación y Acción Comunal – IDPAC, se comprometen a realizar gestión a los riesgos relacionados con las actividades a ejecutar desde todos sus procesos, para garantizar el cumplimiento de los objetivos institucionales y la transparencia en la gestión. La entidad en su tarea de implementar la adecuada gestión de los riesgos, considera que los dueños de los procesos tendrán en cuenta la importancia del riesgo que han identificado analizando el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento que podrán ser aceptar, reducir, evitar y/o compartir el riesgo. Los riesgos de corrupción, son inaceptables y en consecuencia no se pueden asumir. En todo caso se deberán adelantar acciones para su mitigación.”***

El contenido del presente documento hace parte integral de la Política de Administración del Riesgo, al desarrollar en detalle: La metodología, los pasos a seguir en el aplicativo SIG participo, los factores de riesgo, los criterios asociados al contexto interno y externo, la periodicidad para la actualización de los mapas de riesgos y su monitoreo, niveles de aceptación y manejo, tabla de impactos, criterios de calificación del impacto, entre otros

Para lograr lo anteriormente enunciado, la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan implementar la metodología de administración del riesgo y ejecutar eficientemente la formulación, calificación y evaluación de los riesgos.

## 7. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

El proceso de administración de riesgos del IDPAC señalado en la presente guía desarrolla una metodología para todos los riesgos de la entidad teniendo en cuenta las particularidades de cada uno de acuerdo con los requerimientos normativos existentes. A continuación, se describe el proceso general para la gestión del riesgo por parte de todos los procesos:



**IDPAC**



## **Ilustración 2** Etapas para la administración del riesgo

La metodología anterior se aplica para la administración de los riesgos de gestión, riesgos de corrupción, riesgos de seguridad digital, riesgos ambientales, riesgos de seguridad y salud en el trabajo y riesgos de seguridad y privacidad de la información. Para lograr esta integración de todos los riesgos en la misma metodología, esta guía propone desde la Oficina Asesora de Planeación un modelo de evaluación de riesgos que tiene en cuenta las particularidades de cada forma de calificación de acuerdo con lineamientos de cada tipo de riesgo.

Los numerales siguientes presentan cada una de las etapas a desarrollar durante la administración del riesgo. En la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que deben tenerse en cuenta; la explicación del desarrollo de cada etapa se realizará de acuerdo con el tipo de riesgo.

Teniendo en cuenta las etapas anteriores, esta guía establece que para la administración del riesgo al interior del IDPAC se tendrán en cuenta parcialmente los lineamientos de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 5. Una vez el aplicativo SIG participo sea actualizado a la versión 5 de la guía realizaremos los ajustes pertinentes

A continuación, se desarrollan cada una de las etapas.

### **7.1. CONTEXTO DE LA ENTIDAD**

El establecimiento del contexto es la definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo, y establecimiento del alcance y los criterios



del riesgo<sup>1</sup>, estos últimos para el IDPAC serán los relacionados con los lineamientos normativos del Departamento Administrativo de la Función Pública, el Manual Operativo del Modelo Integrado de Planeación y Gestión, el Decreto 1073 de 2015, la Norma Técnica Colombiana ISO 31000 sobre Gestión del Riesgo, la Norma Técnica Colombiana Ambiental ISO 14000 y la Norma Técnica Colombiana ISO 27000 y los lineamientos normativos aplicables a la gestión del riesgo visto desde un componente ambiental así como el de seguridad y salud en el trabajo.

La identificación del contexto interno y externo hace referencia a las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos del IDPAC. La definición del contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo porque permite conocer las situaciones generadoras de riesgos que facilita la formulación de controles que impidan el cumplimiento de los objetivos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional: *“Garantizar a la ciudadanía del Distrito Capital el derecho a la participación incidente y fortalecer las organizaciones sociales, mediante información, formación y promoción, para la construcción de democracia”* y sus objetivos para tener una visión sistémica de la gestión, de manera tal que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa se fundamenta en la identificación de los agentes internos (debilidades) y/ o externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Para efectos de la presente guía el análisis de contexto estará armonizado con el ejercicio de planeación estratégica institucional, en el que se identifican agentes internos (debilidades y fortalezas) y externos (amenazas y oportunidades) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales. Este DOFA será insumo para la identificación de los riesgos de la entidad.

| <b>ANÁLISIS DOFA</b>   |   |
|--|---|
| <b>DEBILIDADES</b>   | <b>OPORTUNIDADES</b>  |
| <ul style="list-style-type: none"> <li>• Procesos y procedimientos desactualizados.</li> <li>• Tecnología obsoleta en sistemas de información.</li> <li>• Manejo del archivo débil (No existencia de Tablas de Valoración Documental).</li> <li>• Desarticulación de las dependencias debido a que se trabaja por funciones y no bajo el enfoque de procesos.</li> <li>• Ausencia de datos e información sistematizado sobre los procesos liderados por el IDPAC</li> <li>• Crisis económica y social por causa de la</li> </ul> | <ul style="list-style-type: none"> <li>• La utilización de nuevas tecnologías para incentivar procesos de participación y articulación ciudadana.</li> <li>• Aprovechamiento de las TIC.</li> <li>• Componentes de participación en todas las políticas públicas poblacionales.</li> <li>• Reingeniería institucional.</li> <li>• Convenios Interadministrativos con entidades del orden nacional y Organismos Multilaterales.</li> <li>• Nueva Ley 1757 de 2015 la cual dicta disposiciones en materia de promoción y</li> </ul> |

<sup>1</sup> Numeral 2.9. Norma Técnica Colombia NTC-ISO 31000. Gestión del riesgo. Principios y Directrices.

| <b>ANÁLISIS DOFA</b>  |   |
|---|---|
| <p>declaratoria de emergencia del país de cara a la pandemia.</p>   | <p>protección del derecho a la participación democrática.</p> <ul style="list-style-type: none"> <li>• Implementación de sistemas de gestión basado en normas internacionales y de cumplimiento legal como la NTC ISO</li> <li>• Articulación del nuevo Plan de Desarrollo Distrital Un nuevo contrato social, ambiental para el siglo XXI, con los Objetivos de Desarrollo Sostenible.</li> </ul>  |
| <b>FORTALEZAS</b>   | <b>AMENAZAS</b>   |
| <ul style="list-style-type: none"> <li>• Entidad que impulsa nuevas prácticas, metodologías y políticas sobre participación ciudadana.</li> <li>• Conocimiento y talento humano especializado.</li> <li>• Experiencia y conocimiento del territorio y su realidad.</li> <li>• Conocimiento de las organizaciones sociales y sus líderes.</li> <li>• Reconocimiento ciudadano en especial desde lo comunal.</li> <li>• Contar con diferentes herramientas para la construcción de metodologías de participación.</li> <li>• Compromiso, capacidad de trabajo y convocatoria, las relaciones construidas con líderes, organizaciones, nuevas ciudadanías, equipos institucionales de nivel local y distrital.</li> <li>• Capacidad de asesoría y orientación en procesos de planeación local participativa y en formulación y ejecución de proyectos sociales y de participación en el marco de las normas existentes.</li> </ul> <p>Un nuevo contrato social, ambiental para el siglo XXI, que permitirá enfrentar efectos del COVID 19.</p> | <ul style="list-style-type: none"> <li>• Pérdida de credibilidad de la comunidad en los procesos del IDPAC durante los últimos años</li> <li>• Vacíos en la norma comunitaria.</li> <li>• Actores externos desarrollando la misionalidad del Instituto.</li> <li>• Débil línea base en materia de planeación, participación y presupuestario participativa a nivel local y distrital.</li> <li>• Recursos presupuestales limitados</li> <li>• Cumplimiento de requisitos legales ambientales y de seguridad y salud en el trabajo por parte de proveedores y demás grupos de interés.</li> <li>• Alta contaminación Ambiental y Falta de calidad de Aire (Capitales)</li> </ul> |

Para la identificación de los riesgos es importante tener en cuenta los agentes generadores de riesgo que son el resultado del análisis del contexto estratégico, por lo tanto, son el insumo para determinar las causas del riesgo; por esta razón, cada una de las causas del riesgo identificado, se deben asociar a un agente externo o interno de riesgo, según corresponda.

A continuación, se presentan los agentes generadores de riesgo internos y externos definidos a partir de los insumos de la Planeación Estratégica que permitirán que identifique mejor la causa del riesgo:

| <b>FACTORES DE RIESGO INTERNOS</b> |   |  |
|------------------------------------|---|--|
| <b>Dirección</b>                   | Resultados y decisiones de los diferentes comités de la Entidad, lineamientos y políticas institucionales.  | <ul style="list-style-type: none"> <li>• Decisiones de la alta dirección, toma de decisiones sin atención de las condiciones institucionales y las recomendaciones de los equipos de trabajo (Toma de decisiones no sustentadas en evidencias)</li> <li>• Falta de apoyo de los Gerentes Públicos para adelantar iniciativas institucionales</li> </ul>  |
| <b>Estructura organizacional</b>   | Organización de la entidad, distribución de roles y responsabilidades, cambios en los directivos.   | <ul style="list-style-type: none"> <li>• Multiplicidad de funciones concentradas en un sólo cargo o dependencia</li> <li>• Cambios en la estructura y funcionamiento de las dependencias</li> <li>• Asignación de nuevas funciones</li> <li>• Ausencia de criterios para la definición de niveles de responsabilidad y autoridad</li> <li>• Alta rotación en el nivel directivo</li> <li>• Falencias de liderazgo por parte de los gerentes públicos</li> </ul>  |
| <b>Talento Humano</b>              | Disponibilidad de personal, estabilidad, capacidad operativa y de respuesta de los servidores y contratistas del IDPAC en el desarrollo de sus funciones y obligaciones, competencias y capacitación. | <ul style="list-style-type: none"> <li>• Capacidad del Talento Humano disponible para dar respuesta a las funciones asignadas</li> <li>• Demoras en los procesos a causa del desconocimiento de las funciones</li> <li>• Falencias en la habilidades y capacidades de los servidores públicos</li> <li>• Debilidad de programas de bienestar laboral y capacitación</li> <li>• Acciones u omisiones de los servidores que intervienen en la gestión</li> <li>• Alta rotación de contratistas o poca continuidad de equipos de trabajo existentes</li> <li>• Falta de personal con los conocimientos y/o habilidades para adelantar la gestión institucional</li> </ul> |
| <b>Ético</b>                       | Compromiso y comportamiento ético (principios y valores) de los trabajadores.   | <ul style="list-style-type: none"> <li>• Deficiencias en el proceso de selección al validar las competencias comportamentales</li> <li>• Falta de ética de los servidores y/o contratistas en el desempeño de su labor</li> </ul>  |

| <b>FACTORES DE RIESGO INTERNOS</b>     |   |  |
|--|---|--|
| <i>Seguridad y salud en el trabajo</i> | Condiciones de trabajo producto de las emociones de los integrantes de un equipo o de toda la Entidad; contempla aspectos físicos y emocionales, e influye de manera directa en la motivación de los empleados. | <ul style="list-style-type: none"> <li>• Espacio físico, instalaciones, temperatura</li> <li>• Conflictos en los equipos de trabajo</li> <li>• Debilidad en las relaciones interpersonales</li> <li>• Estabilidad laboral</li> <li>• Remuneración laboral</li> <li>• Política de ascenso</li> <li>• Bajo nivel de participación de los servidores en procesos de formación y capacitación</li> <li>• Organización inadecuada del trabajo</li> <li>• Planeación inadecuada del tiempo de trabajo</li> <li>• Carga mental elevada</li> <li>• Resistencia al cambio</li> <li>• Desinterés de los servidores o equipos de trabajo</li> <li>• Acoso laboral</li> <li>• Pandemias</li> </ul> |
| <i>Mecanismos de Control</i>           | Estado, características y disponibilidad de los mecanismos de seguimiento y medición institucionales.   | <ul style="list-style-type: none"> <li>• Insuficientes, deficientes o inadecuados mecanismos de seguimiento y control</li> <li>• Sobrestimación de los mecanismos de control dispuestos sin ser adecuados con las condiciones institucionales</li> <li>• Interpretación errónea de normas que implican la implementación de mecanismos de control</li> <li>• Observaciones erradas por parte de los actores de evaluación y seguimiento</li> <li>• Falta de aplicación de los mecanismos de control establecidos</li> <li>• Definición desmedida de mecanismos de control que dificultan la gestión institucional</li> </ul>   |
| <i>Comunicación e información</i>      | Flujos de información y comunicación formales e informales de la Entidad.   | <ul style="list-style-type: none"> <li>• Integridad de la información</li> <li>• Debilidades en la disposición y consulta de la información interna como insumo para la gestión de los procesos</li> <li>• Calidad, vigencia y pertinencia de la información interna que se requiere para generar resultados.</li> <li>• Debilidad en la implementación de las estrategias de comunicación informativa y organizacional</li> <li>• Debilidad o ausencia de canales de comunicación internos</li> </ul>   |

| <b>FACTORES DE RIESGO INTERNOS</b> |   |  |
|------------------------------------|---|--|
| <i>Sistemas Tecnológicos</i>       | Operación, disponibilidad, vigencia, pertinencia y estado de los sistemas de información y comunicación de la Entidad.                                | <ul style="list-style-type: none"> <li>• Obsolescencia o insuficiencia de los sistemas tecnológicos y modelos para la administración de la información con los que cuenta la Entidad</li> <li>• Sistemas tecnológicos que no se adaptan a la naturaleza institucional</li> <li>• Lentitud y caídas en los sistemas.</li> <li>• Sistemas no integrados o sin interface.</li> <li>• Congestión en los sistemas por demandas en el servicio.</li> <li>• Falta o inadecuado mantenimiento preventivo y correctivo de sistemas de información</li> <li>• Retrasos en la modernización de sistemas de información</li> <li>• Fugas de información</li> </ul>   |
| <i>Financiero</i>                  | Capacidad financiera de la entidad y administración de los recursos disponibles.  | <ul style="list-style-type: none"> <li>• Inadecuada programación presupuestal</li> <li>• Inadecuados procesos de planeación y ejecución presupuestal</li> <li>• Políticas internas de austeridad del gasto</li> <li>• Inadecuado seguimiento presupuestal</li> <li>• Falta de recursos para garantizar el cumplimiento legal ambiental aplicable a la entidad.</li> </ul>  |
| <i>Gestión por procesos</i>        | Operación, articulación e interrelación de los procesos, procedimientos y metodologías que orientan la gestión institucional.                         | <ul style="list-style-type: none"> <li>• Falencias en la definición del modelo de operación por procesos institucional</li> <li>• Objetivo y alcance de los procesos inadecuado o impreciso</li> <li>• Inconvenientes en la operación de los procesos institucionales</li> <li>• Pertinencia de los documentos asociados a los procesos y falta de claridad frente a la operación</li> <li>• Falta de efectividad en la interrelación de procesos o relaciones entre procesos con inconsistencias</li> <li>• Desconocimiento del modelo de operación por procesos (Documentos, políticas, prácticas de gestión)</li> </ul>   |
| <i>Sistemas de gestión</i>         | Operación, aplicación, adaptación y mejoramiento de los modelos de planeación y gestión adoptados por el IDPAC para el fortalecimiento de su gestión. | <ul style="list-style-type: none"> <li>• Definición inadecuada del Direccionamiento Estratégico Institucional</li> <li>• Planeación institucional que no corresponde con las necesidades del gobierno o con las condiciones de la entidad</li> <li>• Falta de continuidad en planes y proyectos institucionales</li> <li>• Operación inadecuada de los modelos de gestión</li> <li>• Incumplimiento de lineamientos de gestión establecidos por el gobierno.</li> <li>• Deficiencia en la planeación estratégica.</li> <li>• Debilidad institucional en la interpretación y aplicación de normas.</li> <li>• Vigencia de lineamientos de gestión establecidos</li> <li>• Desarticulación de requisitos de los modelos de gestión</li> <li>• Pertinencia de los lineamientos</li> </ul> |

| <b>FACTORES DE RIESGO EXTERNOS</b> |  |  |
|------------------------------------|--|--|
| <b>Interinstitucional</b>          | Relaciones interinstitucionales con las entidades del sector, gobierno y demás partes interesadas. | <ul style="list-style-type: none"> <li>• Reglamentación y/o capacidad operativa de las entidades</li> <li>• Disponibilidad de información de Entidades con las que el IDPAC debe operar de manera articulada</li> <li>• Disposición de Entidades Públicas y/o partes interesadas</li> <li>• Planes de acción de políticas públicas sin la capacidad operativa para su implementación y articulación entre entidades</li> </ul> |
| <b>Social</b>                      | Condiciones sociales de los habitantes de la ciudad.   | <ul style="list-style-type: none"> <li>• Políticas migratorias o emigración</li> <li>• Desplazamiento</li> <li>• Asonadas</li> <li>• Secuestros</li> <li>• Extorsión</li> <li>• Vandalismo</li> <li>• Delincuencia común</li> <li>• Corrupción social</li> <li>• Terrorismo</li> <li>• Declaratorias de emergencias con componente social</li> </ul>   |
| <b>Político</b>                    | Cambios de gobierno, legislación, planes, políticas públicas, decisiones de gobernantes.           | <ul style="list-style-type: none"> <li>• Decisiones políticas que afecten la operación institucional</li> <li>• Influencias políticas que pueden afectar la operación institucional</li> <li>• Cambios de gobierno.</li> <li>• Decisiones administrativas nacionales y/o distritales</li> <li>• Respaldo deficiente del Concejo</li> <li>• Reformas</li> </ul>   |
| <b>Cultural</b>                    | Condiciones de interacción y relación con los usuarios y partes interesadas de la Entidad.         | <ul style="list-style-type: none"> <li>• Malinterpretación de conceptos</li> <li>• Percepciones equivocadas de la operación institucional</li> <li>• Coordinación interinstitucional</li> <li>• Convenios interinstitucionales</li> </ul>  |
| <b>Económico</b>                   | Disponibilidad y lineamientos para la administración de recursos económicos.                       | <ul style="list-style-type: none"> <li>• Disponibilidad de capital para la operación institucional</li> <li>• Aspectos y directrices a tener en cuenta para la administración de recursos financieros asignados a la Entidad</li> </ul>  |
| <b>Ambiental</b>                   | Cambios en los impactos ambientales adversos o beneficiosos para la entidad.                       | <ul style="list-style-type: none"> <li>• Situaciones de emergencias</li> <li>• Cambios climáticos</li> <li>• Contaminación</li> <li>• Gestión de residuos</li> <li>• Cambios normativos y de aplicabilidad institucional</li> </ul>  |

| <b>FACTORES DE RIESGO EXTERNOS</b> |  |  |
|------------------------------------|--|--|
| <b>Tecnológico</b>                 | Cambios, avances o exposiciones tecnológicas relacionadas con:   | <ul style="list-style-type: none"> <li>• Evoluciones tecnológicas</li> <li>• Modificación de plataformas tecnológicas</li> <li>• Interrupciones en las redes de comunicación</li> <li>• Vulnerabilidad en los sistemas de seguridad de la información</li> <li>• Cambios tecnológicos que generen obsolescencia de los sistemas y modelos con que cuenta la Entidad</li> </ul> |
| <b>Legal</b>                       | Cambios en las normas que rigen la operación de la Entidad.  | <ul style="list-style-type: none"> <li>• Nuevos criterios jurisprudenciales</li> <li>• Cambios normativos nacionales o distritales</li> </ul>  |
| <b>Imagen</b>                      | Credibilidad, interpretación de conceptos, percepciones de la realidad y del funcionamiento u operación de la entidad y de lo público. | <ul style="list-style-type: none"> <li>• Poca o nula credibilidad en la gestión institucional</li> <li>• Percepción negativa de la gestión institucional por parte de las partes interesadas</li> <li>• Publicidad negativa</li> <li>• Acciones, decisiones y trámites errados</li> <li>• Inadecuada atención al usuario</li> </ul>  |

## 7.2. IDENTIFICACIÓN DE LOS RIESGOS

La etapa de identificación de riesgos tiene varios componentes que se señalan a continuación:

### 7.2.1. Identificar riesgos por proceso

En la etapa de identificación de riesgos estratégicos, riesgos operativos, riesgos de corrupción, riesgos de imagen, riesgos de cumplimiento, riesgos financieros, riesgos tecnológicos, riesgos ambientales y riesgos de seguridad y salud en el trabajo será importante revisar los objetivos de los procesos y/o los compromisos establecidos en la planeación institucional con el fin de determinar los eventos que potencialmente puedan afectar el cumplimiento de los objetivos institucionales.

Dentro de la etapa de identificación de riesgos es importante aclarar que para los riesgos de seguridad digital y riesgos ambientales y de seguridad y salud en el trabajo se tendrán en cuenta criterios adicionales que se presentan a continuación: para seguridad digital, se debe realizar la identificación de los activos de seguridad de información, un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO. Para identificar estos activos, la entidad debe cumplir con seis (6) pasos:



LISTAR LOS ACTIVOS  
POR CADA PROCESO



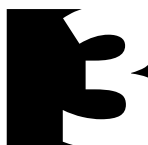
CLASIFICAR LA  
INFORMACIÓN



IDENTIFICAR EL  
DUEÑO DE LOS  
ACTIVOS



DETERMINAR LA  
CRITICIDAD DEL  
ACTIVO



CLASIFICAR LOS  
ACTIVOS



IDENTIFICAR SI EXISTE  
INFRAESTRUCTURA CRÍTICA  
CIBERNÉTICA

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública<sup>2</sup>. Para efectos de esta guía, es importante precisar que existen tres (3) tipos de riesgos inherentes de seguridad digital que se deben identificar:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización<sup>2</sup>. Las amenazas representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. Existen amenazas comunes cuyo origen puede ser deliberado (D), fortuito (F) o Ambiental (A) como el mal funcionamiento del equipo, el fuego y/o la saturación del sistema de información y otras serán amenazas dirigidas por el hombre como, por ejemplo: ataques contra el sistema y/o hurto de información. Con respecto a las vulnerabilidades, estas últimas pueden ser: mantenimiento insuficiente, conexión deficiente de cableado y/o red eléctrica inestable.

**NOTA:** La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

1

<sup>2</sup> Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Ministerio de Tecnologías de la Información y las Comunicaciones. Viceministerio de Economía Digital. Dirección de gobierno digital.



Recuerde que esta guía propone lineamientos para la identificación de los riesgos de corrupción, para esta actividad es importante tener en cuenta que un riesgo de corrupción es *“la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. “Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes N° 167 de 2013)”. Por ejemplo:* Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

Teniendo en cuenta que el propósito de esta guía es desarrollar la metodología para todos los riesgos de la entidad recuerde que es necesario también identificar los riesgos de seguridad y salud en el trabajo. El propósito general de la identificación de los peligros y la valoración de los riesgos en Seguridad y Salud en el trabajo (SG-SST), es entender los peligros que se pueden generar en el desarrollo de las actividades, con el fin de que la organización pueda establecer los controles necesarios, al punto de asegurar que cualquier riesgo sea aceptable<sup>3</sup>.

El peligro se define como la fuente, situación o acto con potencial de daño en términos de enfermedad o lesión a las personas, o una combinación de éstos. La identificación del riesgo se realiza determinando: el cargo, el proceso, la zona o lugar de la actividad, la tarea y la identificación de esta última como rutinaria o no dentro del formato diseñado para tal fin. Esta identificación sigue los lineamientos establecidos en la Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional (GTC 45).

Para la identificación de los riesgos de seguridad y salud en el trabajo, se debe realizar una descripción y clasificación de los peligros. Los peligros pueden clasificarse de acuerdo con los siguientes criterios (Biológicos, condiciones de seguridad, fenómenos naturales, físicos, psicosociales, químicos, biomecánicos y/o ergonómicos).

Para la identificación de los riesgos ambientales y de seguridad y salud en el trabajo, se tendrá en cuenta el análisis visto desde la definición del contexto interno y externo, así como las necesidades y expectativas de las partes interesadas y los requisitos legales aplicables a la organización que afecten o no permitan el logro de los objetivos institucionales.

### 7.2.2. Identificar la causa del riesgo

La etapa de identificación de riesgos permite conocer los eventos potenciales, -estén o no bajo el control del IDPAC-, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores internos y externos, las causas, la descripción del riesgo identificado y sus consecuencias.

---

<sup>3</sup> Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional (GTC 45)

Las causas son los medios, circunstancias y/o agentes generadores de riesgos; la definición de las causas es de gran relevancia para lograr una adecuada administración del riesgo. Se debe garantizar la coherencia entre las causas y el riesgo identificado, teniendo en cuenta que los controles estarán orientados a la eliminación de las causas o mitigación de las consecuencias o impacto, asociadas al riesgo. Recuerde que una definición inadecuada de las causas conlleva a un tratamiento incipiente y poco efectivo de los riesgos identificados por definición errada de los controles.

### 7.2.3. Descripción del riesgo

La redacción del riesgo debe cumplir con los criterios de redacción para lograr una adecuada imagen del evento. Para describir el riesgo será importante evitar iniciar con palabras negativas como: “No...”, “Que no...”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en...”.

**Por ejemplo:** Si el objetivo del proceso de Gestión Contractual el objetivo es “Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación”. La redacción del riesgo sería:

**RIESGO DEL PROCESO:** “Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad”. **RIESGO DE CORRUPCIÓN:** “posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato”.

**2**

A continuación, se presentan algunos ejemplos de descripción del riesgo documentados en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4 Dirección de Gestión y Desempeño Institucional. Octubre 2018.

#### Para riesgo de tipo operativo:

| RIESGO  | DESCRIPCIÓN  | TIPO      | CAUSAS  | CONSECUENCIAS  |
|---|--|-----------|---|--|
| Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad | La combinación de factores como insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación pueden ocasionar inoportunidad en la | Operativo | 1.Carencia de controles en el procedimiento de contratación<br>2.Insuficiente capacitación del personal de contratos<br>3.Desconocimiento de los cambios en la regulación contractual | 1. Parálisis en los procesos<br>2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor<br>3. Demandas y demás acciones jurídicas<br>4. Detrimento de la imagen de la entidad ante sus grupos de valor<br>5. Investigaciones |

| RIESGO | DESCRIPCIÓN   | TIPO | CAUSAS                             | CONSECUENCIAS  |
|--------|---|------|------------------------------------|----------------|
|        | adquisición de los bienes y servicios requeridos por la entidad y, en consecuencia, afectar la continuidad de su operación. |      | Inadecuadas políticas de operación | disciplinarias |

**Para riesgo de corrupción:**

| RIESGO   | DESCRIPCIÓN  | TIPO       | CAUSAS   | CONSECUENCIAS   |
|--|--|------------|--|---|
| Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato”. | Situaciones como: debilidades en la etapa de la planeación del contrato, la excesiva discrecionalidad, las presiones indebidas, la carencia de controles, la falta de conocimiento y/o experiencia, sumados a la falta de integridad pueden generar un riesgo de corrupción en la contratación, como por ejemplo “exigencias de condiciones en los procesos de selección que solo cumple un determinado proponente”. | Corrupción | <ol style="list-style-type: none"> <li>1. Debilidades en la etapa de planeación, que faciliten la inclusión en los estudios previos, y/o en los pliegos de condiciones de requisitos orientados a favorecer a un proponente.</li> <li>2. Presiones indebidas.</li> <li>3. Carencia de controles en el procedimiento de contratación.</li> <li>4. Falta de conocimiento y/o experiencia del personal que maneja la contratación</li> <li>5. Excesiva discrecionalidad</li> <li>6. Adendas que modifican las condiciones generales del proceso de contratación para</li> </ol> | <ol style="list-style-type: none"> <li>1. Pérdida de la imagen institucional.</li> <li>2. Demandas contra el Estado.</li> <li>3. Pérdida de confianza en lo público.</li> <li>4. Investigaciones penales, disciplinarias y fiscales.</li> <li>5. Detrimiento patrimonial.</li> <li>6. Obras inconclusas.</li> <li>7. Mala calidad de las obras.</li> <li>8. Enriquecimiento ilícito de contratistas y/o servidores públicos.</li> </ol> |

|  |  |  |                               |  |
|--|--|--|-------------------------------|--|
|  |  |  | favorecer a un<br>proponente. |  |
|--|--|--|-------------------------------|--|

Esta metodología de descripción la puede utilizar para los riesgos estratégicos, riesgos operativos, riesgos de corrupción, riesgos de imagen, riesgos de cumplimiento, riesgos financieros, riesgos tecnológicos y riesgos ambientales. No obstante, para la descripción de riesgos de seguridad y salud en el trabajo y riesgos de seguridad digital deberá tener en cuenta los siguientes lineamientos:

**Riesgos de seguridad digital:**

| RIESGO                  | ACTIVO                   | DESCRIPCIÓN DEL RIESGO   | AMENAZA                    | TIPO              | CAUSAS/<br>VULNERABILIDADES  | CONSECUENCIAS  |
|-------------------------|--------------------------|--|----------------------------|-------------------|--|--|
| Base de datos de nómina | Pérdida de la integridad | La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina. | Modificación no autorizada | Seguridad digital | Falta de políticas de seguridad digital<br>Ausencia de políticas de control de acceso<br>Contraseñas sin protección<br>Autenticación débil | Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina. |

**Riesgos de seguridad y salud en el trabajo:** La descripción de los peligros está relacionada con el tipo de peligro (Biológicos, Condiciones de seguridad, Fenómenos naturales, Físicos, Psicosociales,

Químicos, Biomecánicos y/o Ergonómicos que se haya documentado en la etapa de identificación de la causa, para el caso de los riesgos de SST lo denominamos peligro:

| RIESGO    | DESCRIPCIÓN   | TIPO                            | CAUSAS  | CONSECUENCIAS   |
|-----------|---|---------------------------------|---|---|
| Biológico | Contagio a causa del COVID 19, en las actividades que requieren trabajo de campo y contacto con la comunidad durante las medidas de aislamiento preventivo. | Seguridad y Salud en el trabajo | <ol style="list-style-type: none"> <li>1. No implementación del protocolo de bioseguridad.</li> <li>2. Mal uso de los elementos de protección personal como tapabocas, guantes, careta, entre otros.</li> <li>3. No cumplir con medidas de preventivas de lavado de mano y distanciamiento social.</li> </ol> | <ol style="list-style-type: none"> <li>1. Aumento de contagio de coronavirus en la entidad.</li> <li>2. Pérdida de la capacidad laboral o hasta la muerte a causa de la enfermedad.</li> <li>3. Demandas y demás acciones jurídicas</li> <li>4. Investigaciones disciplinarias</li> </ol> |

**Riesgos de gestión ambiental:** La descripción de los riesgos está asociado al análisis del contexto interno y externo que no permita el logro de los objetivos, así como a las situaciones de emergencia que se presenten y que afecten la capacidad administrativa y operativa de la entidad.

| RIESGO   | DESCRIPCIÓN  | TIPO      | CAUSAS  | CONSECUENCIAS   |
|--|--|-----------|---|---|
| Ausencia de planificación en la gestión ambiental asociada con los aspectos ambientales identificados en la ejecución de los proyectos de la entidad | Corresponde al posible incumplimiento por la no identificación de los aspectos y posibles impactos ambientales generados por las actividades que adelanta el IDPAC relacionados con sus proyectos. | Ambiental | <ol style="list-style-type: none"> <li>1. Ausencia en la identificación de los aspectos e impactos ambientales</li> <li>2. Debilidad en la definición de controles y oportunidad en la gestión del riesgo.</li> </ol> | <p>Afectación ambiental e incumplimiento de requisitos legales.</p> <p>Imposición de multas y procesos sancionatorios ambientales</p> |

#### 7.2.4. Clasificación del riesgo

Para la clasificación de los riesgos tenga en cuenta la tipología de los riesgos que se presenta a continuación:

- **Riesgos Estratégicos:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la entidad.
- **Riesgos Operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos de la entidad.
- **Riesgos de Cumplimiento/Institucional:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
- **Riesgos de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgos de seguridad digital:** Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, 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.
- **Riesgos Financieros:** Posibilidad de ocurrencia de eventos que afecten los recursos de la entidad y todos aquellos temas relacionados con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, ejecución presupuestal, estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
- **Riesgo de Imagen:** Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
- **Riesgos Tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- **Riesgos de SST:** Incluyen las condiciones de seguridad y salud o las necesidades y expectativas de las partes interesadas que pueden afectar la capacidad de la organización para lograr los resultados previstos en el Sistema Integrado de Gestión
- **Riesgo Ambiental:** Incluyen las condiciones ambientales o las necesidades y expectativas de las partes interesadas que pueden afectar la capacidad de la organización para lograr los resultados previstos en el Sistema Integrado de Gestión.

#### 7.3. ANÁLISIS DEL RIESGO

La etapa de análisis busca establecer la probabilidad de ocurrencia del riesgo y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información cuantitativa y cualitativa para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, **Probabilidad e Impacto**. Por la primera, se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida a partir de la determinación de la frecuencia de ocurrencia del riesgo; por Impacto, se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La calificación del riesgo se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar su materialización.

### 7.3.1. Probabilidad del riesgo

La probabilidad representa el número de veces que el riesgo puede materializarse en un determinado número de repeticiones, se prefiere este tipo de análisis y no una escala temporal pues no todos los eventos generadores de riesgo se presentan con la misma frecuencia en un periodo de tiempo, una actividad que se repite 10 veces en el día con una probabilidad de presentar un resultado inesperado de 1/10 deberá tener la misma calificación de probabilidad que una que se repite 10 veces en el mes y tiene la misma probabilidad de fallo de 1/10. Si se utilizara una escala de tiempo la primera tendría 30 veces más calificación de probabilidad, lo que generaría una distorsión en el análisis de riesgo. Para la determinación de la calificación del riesgo, con base en la probabilidad se debe tener en cuenta la siguiente tabla:

| NIVEL               | PROBABILIDAD | CONCEPTO  |
|---------------------|--------------|---|
| <b>RARO</b>         | 0 - 1%       | el riesgo se materializa una de cada 100 veces    |
| <b>IMPROBABLE</b>   | 1% - 5%      | entre una y cinco veces por cada 100 repeticiones |
| <b>MODERADA</b>     | 5% - 20%     | entre 5 y 20 veces por cada 100 repeticiones      |
| <b>PROBABLE</b>     | 20 - 50%     | entre 2 y 5 veces por cada 10 repeticiones        |
| <b>CASI CERTEZA</b> | > 50%        | más de 6 veces por cada 10 repeticiones           |

### 7.3.2. Impacto del riesgo

La calificación de impacto del riesgo se basa en establecer las consecuencias que puede tener la materialización del riesgo en diferentes niveles de la organización. Para esto, se utilizan criterios tanto cualitativos como cuantitativos, y se debe tener en cuenta que un mismo riesgo puede tener impacto en diferentes aspectos, por lo que es fundamental evaluarlos todos.

### 7.3.2.1. Análisis del impacto legal y de cumplimiento

El análisis del impacto legal y de cumplimiento aborda las consecuencias que tienen los resultados no deseados sobre los aspectos legales, estratégicos, presupuestales y de imagen, ante la materialización del riesgo, y se califican con los siguientes criterios:

| Nivel                 | Legal  | Estratégico  | Presupuestal  | Imagen  |
|-----------------------|--|--|---|---|
| <b>INSIGNIFICANTE</b> | Genera un requerimiento interno                                | Afecta el cumplimiento de algunas actividades contempladas en los planes de acción | Afecta hasta el 5% de la ejecución presupuestal de la entidad           | Afecta a un grupo de servidores del proceso         |
| <b>MENOR</b>          | Genera hallazgos administrativos                               | Afecta el cumplimiento de las iniciativas estratégicas                             | Afecta entre el 5% y el 10% de la ejecución presupuestal de la entidad  | Afecta a los servidores del proceso                 |
| <b>MODERADO</b>       | Genera investigaciones disciplinarias y/o fiscales y/o penales | Afecta el cumplimiento de los objetivos estratégicos del IDPAC                     | Afecta entre el 10% y el 25% de la ejecución presupuestal de la entidad | Afecta a todos los servidores del IDPAC             |
| <b>MAYOR</b>          | Genera sanciones para uno o más funcionarios del IDPAC         | Afecta el cumplimiento de la misión del IDPAC                                      | Afecta entre el 25% y el 50% de la ejecución presupuestal de la entidad | Afecta el Sector Gobierno                           |
| <b>CATASTRÓFICO</b>   | Genera sanciones para el IDPAC                                 | Afecta el cumplimiento de las metas distritales                                    | Afecta más del 50% de la ejecución presupuestal de la entidad           | Afecta al Distrito y a todos los usuarios del IDPAC |

### 7.3.2.2. Análisis del impacto operacional

El impacto operacional de los riesgos se evalúa frente a la estandarización de los procesos, la operación tecnológica y el tiempo de recuperación, entendido este último como el tiempo que le toma a la entidad restaurar su operación a niveles normales una vez se materializa el riesgo. Se incluyen también los impactos ambientales y los impactos sobre la salud y la seguridad de los trabajadores.

| Nivel | Estandarización | Tecnología/Operación | Tiempo de recuperación | Ambiental | SST |
|-------|-----------------|----------------------|------------------------|-----------|-----|
|-------|-----------------|----------------------|------------------------|-----------|-----|



| Nivel                 | Estandarización                             | Tecnología/Operación                                    | Tiempo de recuperación | Ambiental   | SST  |
|-----------------------|---|---|------------------------|---|--|
| <b>INSIGNIFICANTE</b> | Genera ajustes a una actividad concreta     | Afecta una o varias actividades de un procedimiento     | Hasta 4 horas          | Inadecuado manejo de residuos del IDPAC   | Los efectos no requieren interrupción de la actividad normal                 |
| <b>MENOR</b>          | Genera ajustes en los procedimientos        | Afecta varios procedimientos de un mismo proceso        | 4 - 24 Horas           | Inadecuado manejo de recursos naturales y/o residuos que generan un impacto en el ambiente                      | No requiere incapacidad, aunque posiblemente interrupción de las actividades |
| <b>MODERADO</b>       | Genera ajustes o cambios en los procesos    | Afecta varios procesos de apoyo de la entidad           | 2 - 14 días            | Afectación de recursos naturales (agua, suelo, aire, fauna y flora) en desarrollo de actividades de un proyecto | Incapacidad temporal   |
| <b>MAYOR</b>          | Genera intermitencia en el servicio         | Afecta uno o varios procesos Misionales de la Entidad   | 2 - 4 semanas          | Afectación de recursos naturales (agua, suelo, aire, fauna y flora) en desarrollo de procesos operativos        | Incapacidad permanente o invalidez   |
| <b>CATASTRÓFICO</b>   | Genera paro total del proceso y/o del IDPAC | Afecta uno o varios procesos Estratégicos de la Entidad | > 4 semanas            | Afectación de recursos naturales (agua, suelo, aire, fauna y flora) a nivel local o regional                    | Muerte   |

### 7.3.2.3. Análisis del impacto de seguridad de la información

En cuanto al impacto sobre la seguridad de la información, se evalúan las consecuencias frente a tres atributos de los datos que hacen parte del proceso sobre el cuál se hace el análisis de riesgos, la Confidencialidad, la Integridad y la Disponibilidad.

La **confidencialidad** está relacionada con la prevención de la divulgación no autorizada de la información. La **integridad** se refiere a que la información se mantenga inalterada, es decir que los registros de las actividades no sufran cambios accidentales o maliciosos. Y la **disponibilidad** evalúa

la capacidad del sistema<sup>4</sup> que contiene la información de mantenerse trabajando sin sufrir restricciones al acceso.

| Nivel                 | Confidencialidad de la información                              | Integridad de la información                                    | Disponibilidad de la Información                                |
|-----------------------|---|---|---|
| <b>INSIGNIFICANTE</b> | Hasta el 10% de la información o registros del proceso          | Hasta el 10% de la información o registros del proceso          | Hasta el 10% de la información o registros del proceso          |
| <b>MINOR</b>          | Entre el 10% y el 20% de la información o registros del proceso | Entre el 10% y el 20% de la información o registros del proceso | Entre el 10% y el 20% de la información o registros del proceso |
| <b>MODERADO</b>       | Entre el 20% y el 30% de la información o registros del proceso | Entre el 20% y el 30% de la información o registros del proceso | Entre el 20% y el 30% de la información o registros del proceso |
| <b>MAYOR</b>          | Entre el 30% y el 50% de la información o registros del proceso | Entre el 30% y el 50% de la información o registros del proceso | Entre el 30% y el 50% de la información o registros del proceso |
| <b>CATASTRÓFICO</b>   | Más del 50% de la información o registros del proceso           | Más del 50% de la información o registros del proceso           | Más del 50% de la información o registros del proceso           |

#### 7.3.2.4. Análisis de impacto de los riesgos de corrupción

La definición del impacto de los riesgos de corrupción, de acuerdo con la Guía para la Administración de Riesgos de Corrupción del Departamento Administrativo de la Función Pública, debe realizarse respondiendo de manera afirmativa o negativa en el siguiente cuestionario:

| Nº | <b>PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...</b> | <b>SI</b> | <b>NO</b> |
|----|--|-----------|-----------|
| 1  | ¿Afectar al grupo de funcionarios del proceso?                       | X         |           |
| 2  | ¿Afectar el cumplimiento de metas y objetivos de la dependencia?     | X         |           |

<sup>4</sup> Cuando se hace referencia a un sistema de almacenamiento de información, no se limita a software o almacenamiento digital, deben considerarse todos los medios de almacenamiento de información, como archivos de gestión, centrales, y archivos muertos.

|    |   |    |   |
|----|---|----|---|
| 3  | ¿Afectar el cumplimiento de misión de la entidad?   | X  |   |
| 4  | ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?   |    | X |
| 5  | ¿Generar pérdida de confianza de la entidad, afectando su reputación?   | X  |   |
| 6  | ¿Generar pérdida de recursos económicos?  | X  |   |
| 7  | ¿Afectar la generación de los productos o la prestación de servicios?   | X  |   |
| 8  | ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?   |    | X |
| 9  | ¿Generar pérdida de información de la entidad?  |    | X |
| 10 | ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?  | X  |   |
| 11 | ¿Dar lugar a procesos sancionatorios?   | X  |   |
| 12 | ¿Dar lugar a procesos disciplinarios?   | X  |   |
| 13 | ¿Dar lugar a procesos fiscales?   | X  |   |
| 14 | ¿Dar lugar a procesos penales?  |    | X |
| 15 | ¿Generar pérdida de credibilidad del sector?  |    | X |
| 16 | ¿Ocasionar lesiones físicas o pérdida de vidas humanas?   |    | X |
| 17 | ¿Afectar la imagen regional?  |    | X |
| 18 | ¿Afectar la imagen nacional?  |    | X |
| 19 | ¿Generar daño ambiental?  |    | X |
|    | Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico | 10 |   |
|    | <b>MODERADO:</b> Genera medianas consecuencias sobre la entidad   |    |   |
|    | <b>MAYOR:</b> Genera altas consecuencias sobre la entidad.  |    |   |
|    | <b>CATASTRÓFICO:</b> Genera consecuencias desastrosas para la entidad.  |    |   |

### 7.3.2.5. Riesgo inherente

El riesgo inherente es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto, y se obtiene comparando los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define

la zona de ubicación del riesgo inherente; esta evaluación se realiza de manera automática por SIG participo.

|                                 |   |                     |                       |                      |                      |                     |                     |
|---------------------------------|---|---------------------|-----------------------|----------------------|----------------------|---------------------|---------------------|
| <b>PROBABILIDAD</b>             | 5 | <b>CASI CERTEZA</b> | Zona riesgo alta      | Zona riesgo alta     | Zona riesgo extrema  | Zona riesgo extrema | Zona riesgo extrema |
|                                 | 4 | <b>PROBABLE</b>     | Zona riesgo moderada  | Zona riesgo alta     | Zona riesgo alta     | Zona riesgo extrema | Zona riesgo extrema |
|                                 | 3 | <b>MODERADA</b>     | Zona riesgo baja      | Zona riesgo moderada | Zona riesgo alta     | Zona riesgo extrema | Zona riesgo extrema |
|                                 | 2 | <b>IMPROBABLE</b>   | Zona riesgo baja      | Zona riesgo baja     | Zona riesgo moderada | Zona riesgo alta    | Zona riesgo extrema |
|                                 | 1 | <b>RARO</b>         | Zona riesgo baja      | Zona riesgo baja     | Zona riesgo moderada | Zona riesgo alta    | Zona riesgo alta    |
| <b>MATRIZ DE ZONA DE RIESGO</b> |   |                     | <b>INSIGNIFICANTE</b> | <b>MENOR</b>         | <b>MODERADO</b>      | <b>MAYOR</b>        | <b>CATASTRÓFICO</b> |
|                                 |   |                     | 1                     | 2                    | 3                    | 4                   | 5                   |
|                                 |   |                     | <b>IMPACTO</b>        |                      |                      |                     |                     |

#### 7.4. VALORACIÓN DEL RIESGO

Es la etapa de administración del riesgo mediante la cual se realiza la descripción detallada y calificación de los controles asociados al riesgo; se debe realizar en los siguientes pasos:

- Paso 1:** Identificar y describir cada una de las características de los controles (preventivos o detectivos), que pueden disminuir la probabilidad de ocurrencia o mitigar el impacto del riesgo
- Paso 2:** Evaluar los controles a partir de su operación y la información documentada sobre las características de estos.

Con base en los resultados consolidados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo.

##### 7.4.1. Diseño de controles

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas identificadas para el riesgo con el fin de eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se diseñen, documenten, apliquen y sean efectivos para prevenir o

mitigar los riesgos. A continuación, se presentan los aspectos mínimos que se deben tener al momento de formular los controles:

- **Nombre del control:** asignar un nombre al control que debe tener explícita la ejecución de una acción; ejemplo: Realizar la tabulación mensual de las encuestas de satisfacción de usuarios.
- **Descripción:** definir de manera detallada cómo se ejecuta el control. Ejemplo: Para un control denominado validar el cumplimiento de los bienes a recibir, la descripción es: El profesional de almacén revisa las características de los bienes a recibir de acuerdo con la orden del pedido y las características definidas en el contrato, diligenciando el formato de recepción de bienes.
- **Propósito:** determinar para qué se realiza el control; ejemplo: Para un control denominado validar el cumplimiento de los bienes a recibir, el propósito es determinar si los bienes recibidos cumplen con las características definidas en el contrato de acuerdo con las necesidades establecidas.
- **Documentación:** indique el documento del proceso en el cual se describe el control. Ejemplo: en el procedimiento de administración de bienes y servicios. No es una opción válida para este campo indicar de forma genérica que se encuentra en los documentos del proceso.
- **Responsable:** persona asignada para ejecutar el control; la persona asignada, debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas (Riesgos de corrupción). Ejemplo: El coordinador de operaciones. Cuando un control se hace de manera manual (ejecutado por personas) es importante establecer el cargo responsable de su realización; cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es importante establecer como responsable de ejecutar el control al sistema o aplicación.
- **Periodicidad:** el control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Hay controles que no tienen una periodicidad específica como, por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores solo se ejecutan cuando se contratan proveedores. La periodicidad debe quedar redactada de tal forma que indique: que cada vez que se desarrolla la actividad se ejecuta el control.
- **Observaciones o desviaciones:** El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Ejemplo: En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación.

- **Evidencias de aplicación:** El control debe dejar evidencia de su ejecución. Esta evidencia permite validar la información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos. Ejemplo: Como evidencia: la respectiva lista de chequeo diligenciada con la información de la carpeta del cliente y correos solicitando la información faltante en los casos que aplique.

#### 7.4.1.1. Naturaleza del control

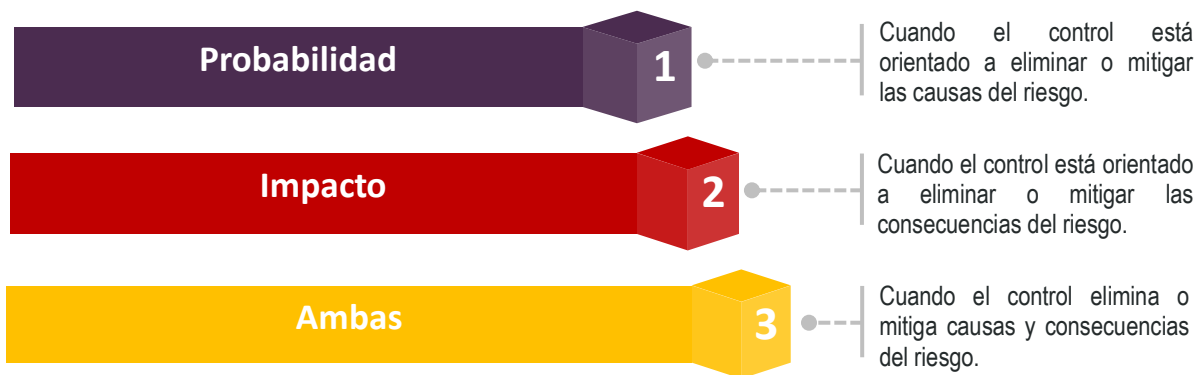
Los controles deben diseñarse para atacar las causas y/o consecuencias (mitigar y/o eliminar) del riesgo, bien sea disminuyendo la probabilidad de ocurrencia o minimizando el impacto. Las acciones de tratamiento se agrupan en:

\* **Disminuir la probabilidad:** acciones encaminadas a gestionar las causas del riesgo.

\* **Disminuir el impacto:** acciones encaminadas a disminuir las consecuencias del riesgo

Se debe preferir el diseño de *controles preventivos*, los cuales, están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos. Los *controles detectivos* están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Una vez se determina si el control descrito es preventivo o detectivo, se debe determinar qué escala (probabilidad, impacto o ambas) se afecta positivamente con la aplicación del control, teniendo en cuenta las siguientes indicaciones:



#### 7.4.2. Valoración de controles

La valoración de los controles está relacionada con las características del diseño del control y la ejecución del mismo, es decir, si este último cumple con las características de diseño y si se ejecuta o no, en las condiciones en las que fue diseñado. Para obtener la evaluación del diseño del control es necesario responder a una serie de preguntas que se presentan a continuación:

| <i>CRITERIO DE EVALUACIÓN</i>                        | <i>OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN</i> | <i>PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL</i> |
|--|--|---|
| <i>Asignación del responsable</i>                    | Asignado   | 15  |
|  | No asignado  | 0   |
| <i>Segregación y autoridad del responsable</i>       | Adecuado   | 15  |
|  | Inadecuado   | 0   |
| <i>Periodicidad</i>                                  | Oportuna   | 15  |
|  | Inoportuna   | 0   |
| <i>Propósito</i>                                     | Prevenir   | 15  |
|  | Detectar   | 10  |
|  | No es un control                                     | 0   |
| <i>Cómo se realiza la actividad de control</i>       | Confiable  | 15  |
|  | No confiable   | 0   |
| <i>Qué pasa con las observaciones o desviaciones</i> | Se investigan y resuelven oportunamente              | 15  |
|  | No se investigan y resuelven oportunamente           | 0   |
| <i>Evidencia de la ejecución del control</i>         | Completa   | 10  |
|  | Incompleta   | 5   |
|  | No existe  | 0   |

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado. Los resultados se presentan a continuación:

| <i>RANGO DE CALIFICACIÓN DEL DISEÑO</i> | <i>RESULTADO - PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL</i> |
|---|---|
| <i>Fuerte</i>                           | Calificación entre 96 y 100                                     |
| <i>Moderado</i>                         | Calificación entre 86 y 95                                      |
| <i>Débil</i>                            | Calificación entre 0 y 85                                       |

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados<sup>5</sup>.

<sup>5</sup> Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4 Dirección de Gestión y Desempeño Institucional. Octubre 2018.

Para la evaluación de la ejecución del control se deberá validar si la ejecución del control se ha dado de forma consistente. Para esto, es importante precisar que, en la administración del riesgo no es suficiente tener un control bien diseñado, sino que la primera línea de defensa debe asegurarse de que el control se ejecute. En este sentido, el responsable del proceso debe contar con la evidencia de la ejecución para que posteriormente la ejecución sea confirmada con las actividades de evaluación realizadas por auditoría interna o control interno. Los rangos de calificación se presentan a continuación:

| <i><b>RANGO DE CALIFICACIÓN DE LA EJECUCIÓN</b></i> | <i><b>RANGO DE CALIFICACIÓN DE LA EJECUCIÓN</b></i>                    |
|---|--|
| <i><b>Fuerte</b></i>                                | El control se ejecuta de manera consistente por parte del responsable. |
| <i><b>Moderado</b></i>                              | El control se ejecuta algunas veces por parte del responsable.         |
| <i><b>Débil</b></i>                                 | El control no se ejecuta por parte del responsable.                    |

Posteriormente, y una vez se ha evaluado el diseño y la ejecución del control, será importante identificar si los controles sirven o no para mitigar los riesgos identificados. La evaluación del diseño del control, así como su ejecución son aspectos importantes para garantizar una solidez de controles adecuada para mitigar los riesgos.

#### **7.4.2.1. Riesgo residual**

El riesgo residual está relacionado con el desplazamiento del riesgo inherente en el mapa de riesgos, es decir, dado que ningún riesgo con una medida de tratamiento se puede evitar o eliminar, se deberá tener en cuenta el desplazamiento de un riesgo inherente (antes de formular controles) en su probabilidad o impacto para el cálculo del riesgo residual (después de formulados los controles). Es importante precisar que, para los riesgos de corrupción únicamente hay disminución de probabilidad, pero nunca de impacto.

#### **7.4.3. Tratamiento del riesgo**

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, para lo cual, tendrán en cuenta el efecto que puede tener la materialización del riesgo para el IDPAC, así como su probabilidad e impacto y la relación costo-beneficio de las medidas identificadas para su tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar,



compartir o reducir el riesgo<sup>6</sup>. Para la entidad se tendrán en cuenta los siguientes criterios dentro del tratamiento de riesgo:

#### 7.4.3.1. Determinación de la opción de tratamiento para el riesgo

Para esta etapa deberán tenerse en cuenta las siguientes opciones:

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

Estas opciones se determinan teniendo en cuenta la ubicación del riesgo residual y la calificación del conjunto de controles:

| ZONA DE RIESGO | OPCIONES DE MANEJO  |
|----------------|---|
| BAJA           | Asumir el riesgo / Reducir el riesgo                                    |
| MODERADA       | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |
| ALTA           | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |
| EXTREMA        | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |

#### 7.4.3.2. Definición de acciones de contingencia.

La definición de acciones de contingencia aplica para todos los riesgos, independiente de su evaluación residual o de los controles existentes y consiste en la definición de acciones inmediatas a desarrollar en el caso de materialización del riesgo; estas acciones son la respuesta inicial a la materialización del riesgo y se enfocan en las correcciones que se deben desarrollar de acuerdo con las consecuencias definidas.

<sup>6</sup> Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4 Dirección de Gestión y Desempeño Institucional. Octubre 2018.

#### 7.4.3.3. Definición del semáforo del riesgo.

Esta opción permite definir la opción mediante el cual la herramienta SIG participo presentará los riesgos y su semáforo; las opciones disponibles en el sistema son:

- Sobre el estado y documentación oportuna de las acciones que se asocien para el manejo del riesgo
- Sobre el estado y reporte que se realice de los indicadores que se asocien al riesgo
- Sobre el cumplimiento de las fechas de monitoreo establecidas en la Entidad para que cada responsable
- A partir de la evaluación residual del riesgo

De acuerdo con los lineamientos institucionales, el semáforo de todos los riesgos se debe calcular con la opción de evaluación residual del riesgo y esto se realiza en el aplicativo del SIG PARTICIPO.

#### 7.4.3.4. Definición de acciones asociadas.

Se deben asociar acciones de manera obligatoria cuando la calificación del conjunto de controles sea inferior al 100%; las acciones deben estar orientadas al mejoramiento y fortalecimiento de los controles identificados; estas acciones se registrarán en el sistema como acciones de tipo preventivo.

### 8. MONITOREO DE LOS RIESGOS

Esta etapa permite el seguimiento periódico a la gestión de los riesgos mediante el monitoreo a la operación adecuada de los controles; cada cuatro meses (abril, agosto y diciembre), los responsables deben realizar seguimiento al estado, pertinencia y calificación de los controles, la vigencia de la información registrada en cada una de las etapas del riesgo, posibles situaciones de materialización y citar las evidencias de aplicación de los controles, mediante el reporte de información relacionada con:

- **Estado de aplicación del control:** descripción de la operación para cada control durante el periodo, de acuerdo con los cortes de monitoreo establecidos.
- **Evidencias de operación del control:** se deben adjuntar los soportes que evidencien la operación del control durante el periodo o citar la URL donde se encuentran ubicadas.
- **Efectividad del control:** se debe indicar si el control ha sido efectivo o no en la gestión del riesgo durante el periodo; en caso de identificar un control no efectivo; se deben realizar los ajustes correspondientes en la etapa de valoración.

A partir de la información registrada por los responsables en el monitoreo, la Oficina Asesora de Planeación realizará seguimiento al estado de aplicación de la práctica. Posteriormente, la Oficina de Control Interno, de acuerdo con los ciclos establecidos en el plan de auditoría, realizará la evaluación independiente de los riesgos identificados y gestionados en la Entidad.



**AUTOCONTROL.** Cada cuatro meses los responsables deberán registrar el monitoreo de los riesgos identificados.



**PLANEACIÓN.** Realiza el informe de seguimiento cuatrimestral con base en la información reportada por los responsables.



**CONTROL INTERNO.** Realiza la evaluación independiente para determinar

## 9. MODIFICACIONES PARA LOS RIESGOS IDENTIFICADOS

Cuando el proceso requiera crear un nuevo riesgo, hacer ajustes en la información documentada, o eliminar un riesgo existente, se deberá registrar la solicitud correspondiente en SIG participo:

| <b>TIPO DE SOLICITUD</b>                 | <b>DESCRIPCIÓN</b>  | <b>TIEMPOS DE GESTIÓN</b>  |
|--|---|--|
| <b>Crear riesgos</b>                     | Registrar la solicitud con la justificación correspondiente en el flujo de solicitudes del SIG.   | Los tiempos de gestión para dar respuesta a esta solicitud, se encuentran estandarizados en el flujo de solicitudes.<br><br><b>Nota:</b> se debe tener en cuenta que para crear riesgos es importante generar mesas de trabajo con el fin de registrar la información de cada etapa. Estas reuniones y el cierre de la solicitud dependerán de la programación que se realice de las mesas de trabajo. |
| <b>Ajustar la información del riesgo</b> | Registrar en SIG participo la solicitud de la devolución de la etapa indicando los ajustes a realizar con la justificación correspondiente. | De acuerdo con la justificación, la Oficina Asesora de Planeación tendrá cinco días hábiles para verificar cada caso y aprobar la devolución a la etapa del riesgo, según la solicitud. Una vez aprobada la devolución de la etapa, el responsable tendrá diez días hábiles para registrar los ajustes en la información de las etapas del riesgo.   |

| <i>TIPO DE SOLICITUD</i> | <i>DESCRIPCIÓN</i>   | <i>TIEMPOS DE GESTIÓN</i>   |
|--------------------------|--|---|
| <i>Eliminar riesgos</i>  | Mediante la opción disponible en el módulo de riesgos, registrar la solicitud con la justificación correspondiente | Una vez registrada la solicitud debidamente justificada; la Oficina tendrá cinco días hábiles para inactivar el riesgo en SIG participo o pronunciarse al respecto. |

## 10. MAPA DE RIESGOS

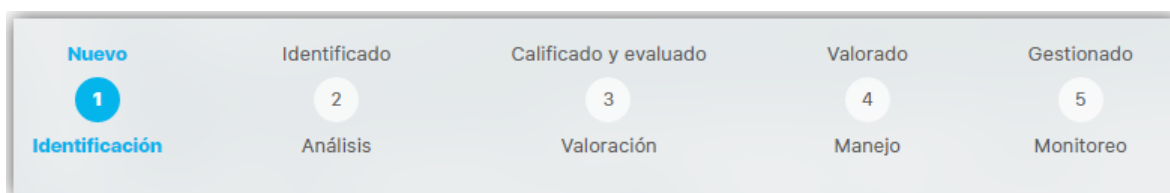
El mapa de riesgos estará disponible para la consulta de todos los servidores, en SIG participo. Los líderes de procesos y sus equipos de trabajo deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y vigente. Cualquier ajuste que se deba realizar de esta información, debe ser tramitada con la Oficina Asesora de Planeación.

Será la Oficina Asesora de Planeación la responsable de la publicación del mapa de riesgos de corrupción en la página web de la Entidad; esta publicación se realizará cada vez que se realicen ajustes a la información registrada por los procesos, o máximo cada cuatro meses, durante abril, agosto y diciembre de cada vigencia; la publicación se realizará en datos abiertos (Archivo de Excel) para facilitar la consulta por las partes interesadas.

## 11. DILIGENCIAMIENTO DE LAS ETAPAS DEL RIESGO EN SIG PARTICIPIO

A continuación, se presentan las etapas que deben gestionarse en el aplicativo SIGPARTICPIO para la implementación de la metodología de administración del riesgo de la entidad. Se debe precisar que el aplicativo cuenta con notas de ayuda para el desarrollo de todo el proceso de los lineamientos metodológicos descritos en el presente documento.

### a) Etapa de identificación



## 1. Identificación del riesgo

Nombre\* NOMBRE DEL RIESGO

Responsable\* RESPONSABLE Gestor GESTOR

Descripción:\*\* DESCRIPCIÓN DEL RIESGO CON LOS ASPECTOS QUE SE NECESITEN ACLARAR RESPECTO AL NOMBRE DEL RIESGO IDENTIFICADO; EVITE EN ESTE ESPACIO INCLUIR CAUSAS O CONSECUENCIAS DEL RIESGO

Clase\* Cumplimiento

¿Este riesgo es institucional?\*

Sí, afecta toda la organización

No

¿Por qué?

JUSTIFIQUE EL "SI O NO" SEGÚN CORRESPONDA, DE ACUERDO CON LAS CARACTERÍSTICAS ESTABLECIDAS PARA LOS RIESGOS INSTITUCIONALES (INCLUYEN LOS DE CORRUPCIÓN, LOS DE CLASE ESTRATÉGICA, LOS QUE AFECTAN AL USUARIO EXTERNO Y LOS QUE EN LA EVALUACIÓN RESIDUAL SE UBICAN EN ZONA ALTA O EXTREMA)

¿Este riesgo es de corrupción?

Sí

No

¿Por qué?\*

JUSTIFIQUE EL "SI O NO" SEGÚN CORRESPONDA, DE ACUERDO CON LAS CARACTERÍSTICAS ESTABLECIDAS PARA LOS RIESGOS DE CORRUPCIÓN

Registrar materialización Guardar Siguiente

Diligencie la información de acuerdo con el contenido metodológico de la guía; en esta etapa, se recomienda utilizar la opción de guardar a medida que se avanza en el diligenciamiento de la información para evitar perder la información registrada.

Opción de guardar

### 1.1 Objetivos o áreas afectadas por el riesgo\*\* (Debe seleccionar por lo menos un tipo de objetivo o área)

Objetivos estratégicos

| Objetivo | Perspectiva | BSC |
|----------|-------------|-----|
|          |             |     |

Registrar materialización Guardar Siguiente

Agregar +

Mediante la opción agregar, se deben asociar los objetivos estratégicos que se pueden afectar de manera directa con la materialización del riesgo; esta asociación debe ser coherente con la alineación estratégica de la Entidad a partir de la planeación

## Buscador de Objetivos estratégicos

[Ayuda](#)



Nombre Todos

**Buscar**

1 - 24 de 24 400 Elementos en página AZ **Exportar**

| Objetivo   | Perspectiva                    | BSC           |
|--|--------------------------------|---------------|
| <input checked="" type="checkbox"/> Fortalecer la capacidad operativa del IDPAC  | Recursos Internos              | PEI 2016 2020 |
| <input type="checkbox"/> Adecuar y mantener el Sistema Integrado de Gestión del IDPAC  | Eficiencia Administrativa      | PEI 2016 2020 |
| <input type="checkbox"/> Fortalecer las herramientas tecnológicas del IDPAC  | Eficiencia Administrativa      | PEI 2016 2020 |
| <input type="checkbox"/> Modernizar la participación en el Distrito Capital  | Gestión misional y de gobierno | PEI 2016 2020 |
| <input type="checkbox"/> Desarrollar conocimiento y capacidades de la ciudadanía y sus organizaciones para ejercer el derecho a la participación | Gestión misional y de gobierno | PEI 2016 2020 |
| <input type="checkbox"/> Fortalecer la gestión de la ciudadanía y sus procesos, espacios e instancias de participación                           | Gestión misional y de gobierno | PEI 2016 2020 |

**Agregar** **Agregar y Cerrar** **Cerrar**

Quando se utiliza la opción de agregar, se despliega el buscador de objetivos estratégicos para seleccionar los que se van a asociar

Una vez seleccionados los objetivos, utilice la opción de agregar y cerrar para continuar con el diligenciamiento de la información de la etapa

### Iniciativas estratégicas

| D | Nombre | Responsable | Fecha Inicial | Fecha Final | Estado |
|---|--------|-------------|---------------|-------------|--------|
|   |        |             |               |             |        |

**Agregar** +

### Objetivos de proceso

1 - 1 de 1

| Nombre  | Proceso                |
|---|------------------------|
| <input type="checkbox"/> Planeación Estratégica | Planeación Estratégica |

**Agregar** +

### Áreas organizativas

1 - 1 de 1

| Nombre   | Sigla | Responsable           | Área organizativa superior | Estado |
|--|-------|-----------------------|----------------------------|--------|
| <input type="checkbox"/> Oficina Asesora de Planeación | OAP   | Veronica Basto Mendez |                            | Activo |

**Agregar** +

Para la asociación de las iniciativas estratégicas, objetivos del proceso y áreas organizativas, tenga en cuenta las mismas orientaciones de los objetivos estratégicos

## 1.2 Causas y efectos del riesgo\*\*

Causas:\*\*

Para asociar los agentes generadores, utilice el recuadro con los tres puntos para consultarlos e identificar el agente adecuado de acuerdo con cada causa identificada

| Agente generador**                                    | Descripción de la causa**     | Concepto asociado    |
|---|-------------------------------|----------------------|
| <input type="checkbox"/> b) Estructura organizacional | CAUSA 1 DEL RIESGO DEL RIESGO | <input type="text"/> |
| <input type="checkbox"/> d) Competencia del personal  | Causa 2                       | <input type="text"/> |
| <input type="checkbox"/> b) Estructura organizacional | Causa 3                       | <input type="text"/> |
| <input type="checkbox"/> e) Ético                     | Causa 4                       | <input type="text"/> |

Agregar 

Mediante la opción agregar, incluya las filas necesarias para registrar todas las causas identificadas del riesgo



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.

IDPAC



**Agentes Cumplimiento**

**Ambiental** *Externo*  
Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible. Algunas conductas asociadas a este agente generador son: -Terremotos - Inundaciones -Cambios climáticos -Contaminación -Gestión de residuos

**Comunicación e información** *Interno*  
Flujos de información y comunicación formales e informales de la Entidad. Algunas conductas asociadas a este agente generador son: -Integridad de la información -Debilidades en la disposición y consulta de la información interna como insumo para la gestión de los procesos -Calidad, vigencia y pertinencia de la información interna que se requiere para generar resultados. -Debilidad en la implementación de las estrategias de comunicación informativa y organizacional -Debilidad o ausencia de canales de comunicación internos

**Cultural** *Externo*  
Condiciones de interacción y relación con los usuarios y partes interesadas de la Entidad. Algunas conductas asociadas a este agente generador son: Malinterpretación de conceptos -Percepciones equivocadas de la operación institucional -Coordinación interinstitucional -Convenios interinstitucionales

**Dirección** *Interno*  
Resultados y decisiones de los diferentes comités de la Entidad, lineamientos y políticas institucionales. Algunas conductas asociadas a este agente generador son: -Decisiones de la alta dirección, toma de decisiones sin atención de las condiciones institucionales y las recomendaciones de los equipos de trabajo (Toma de decisiones no sustentadas en evidencias) - Falta de apoyo de los Gerentes Públicos para adelantar iniciativas institucionales

**Crear Agente**

Seleccione el agente interno o externo que enmarca cada causa identificada; una vez se seleccione se cerrara esta ventana para continuar con el diligenciamiento de la etapa



## Causas\*\*

| Agente generador**                                  | Descripción de la causa**     | Concepto asociado |
|---|-------------------------------|-------------------|
| <input type="checkbox"/> Comunicación e información | CAUSA 1 DEL RIESGO DEL RIESGO |                   |
| <input type="checkbox"/> Cultural                   | Causa 2                       |                   |
| <input type="checkbox"/> Comunicación e información | Causa 3                       |                   |
| <input type="checkbox"/> Ambiental                  | Causa 4                       |                   |

Agregar +

Registrar materialización

Guardar

Siguiente

Recuerde usar constantemente la opción de guardar en esta etapa

## Efectos\*\*

1  
1 - 4 de 4

| Descripción del efecto                  |
|---|
| <input type="checkbox"/> Consecuencia 1 |
| <input type="checkbox"/> Consecuencia 2 |
| <input type="checkbox"/> Consecuencia 3 |
| <input type="checkbox"/> Consecuencia 4 |

Agregar +

Mediante la opción agregar, incluya las filas necesarias para registrar todas las consecuencias o efectos identificados para el riesgo

Guarde la información registrada

Registrar materialización

Guardar

Siguiente

### 1.3 Información adicional \*\*

Información adicional

Mediante este botón, despliegue la información adicional que se debe diligenciar en la etapa de identificación del riesgo

### Definición del riesgo de corrupción

Acción u omisión  
Uso del poder  
Desviar la gestión de lo público  
Beneficio privado

El primer campo en información adicional es exclusivo para los riesgos de corrupción; se deben seleccionar de la lista las situaciones que se pueden presentar en el riesgo identificado.  
Si es necesario marcar varias opciones de la lista; utilice los comandos control + clic izquierdo del mouse de manera simultanea

Productos y/o servicios finales del proceso que se pueden afectar con la m...

- PE - Plan Estratégico Institucional
- PE - Plan de Acción Institucional
- PE - Anteproyecto de Presupuesto Gastos de Inversión
- PE - Plan operativo anual de inversión - POAI
- PE - Planes - programas o proyectos actualizados

Productos y/o Servicios Adicionales que podrían verse afectados

De la lista disponible, seleccione los productos del proceso al que está asociado el riesgo, que se pueden afectar con la materialización de este; si el producto afectado no se encuentra en la lista, utilice el campo de escritura disponible.

Incidencia en el usuario externo\*

Seleccione si el riesgo tiene una incidencia directa en el usuario externo

Incidencia jurídica del riesgo\*

| Si el riesgo se materializa ¿Puede generar inconvenientes jurídicos para la Entidad?* | Descripción *        |
|---|----------------------|
| <input type="checkbox"/>  | <input type="text"/> |

[Agregar](#) +

Utilice la opción agregar para incluir la fila donde se diligenciará la información relacionada con la incidencia jurídica del riesgo; en primer lugar determine si el riesgo tiene o no incidencia jurídica y justifique la respuesta

[Registrar materialización](#)
[Guardar](#)
[Siguiente](#)

Con la determinación de la incidencia jurídica del riesgo se finaliza el diligenciamiento de la etapa; para continuar en la siguiente, utilice la opción siguiente



**¡Operación Exitosa!**

## b) Etapa de análisis

|                |                     |                       |          |            |
|----------------|---------------------|-----------------------|----------|------------|
| Nuevo          | <b>Identificado</b> | Calificado y evaluado | Valorado | Gestionado |
| 1              | <b>2</b>            | 3                     | 4        | 5          |
| Identificación | <b>Análisis</b>     | Valoración            | Manejo   | Monitoreo  |

Probabilidad\* MODERADA

[+ Más información en rangos de Probabilidad](#)

Para determinar la probabilidad puede usar la lista desplegable disponible; sin embargo se recomienda definirla a partir la información que se despliega cuando se ingresa por la opción "+ información de rangos de probabilidad"

Al ingresar por + información se despliega la matriz de probabilidad; identifique la opción adecuada de acuerdo con cada riesgo y utilice la opción seleccionar

Criterios de Probabilidad de ocurrencia de un riesgo

|   |   |
|---|---|
| <input type="radio"/> RARO                | <input type="radio"/> Concepto: Puede que no se haya presentado u ocurrir sólo en circunstancias excepcionales - Frecuencia: Nunca o no se ha presentado<br><input type="radio"/> Ninguna de las anteriores |
| <input type="radio"/> IMPROBABLE          | <input type="radio"/> Concepto: Pudo ocurrir en algún momento, es poco común o frecuente - Frecuencia: Al menos una vez en los últimos 16 meses<br><input type="radio"/> Ninguna de las anteriores          |
| <input checked="" type="radio"/> MODERADA | <input type="radio"/> Concepto: Puede ocurrir en algún momento - Frecuencia: Al menos una vez en los últimos 12 meses<br><input checked="" type="radio"/> Ninguna de las anteriores                         |
| <input type="radio"/> PROBABLE            | <input type="radio"/> Concepto: Probablemente ocurrirá en la mayoría de las circunstancias - Frecuencia: Al menos una vez en los últimos 8 meses<br><input type="radio"/> Ninguna de las anteriores         |
| <input type="radio"/> CASI CERTEZA        | <input type="radio"/> Concepto: Se espera que ocurra en la mayoría de las circunstancias - Frecuencia: Al menos una vez en los últimos 4 meses<br><input type="radio"/> Ninguna de las anteriores           |

Impacto\* CATASTRÓFICO

[+ Más información en rangos de Impacto](#)

Para determinar el impacto puede usar la lista desplegable disponible; sin embargo se recomienda definirla a partir la información que se despliega cuando se ingresa por la opción "+ información en rangos de impacto"

Criterios de Impacto de ocurrencia de un riesgo

|                                      |   |
|--------------------------------------|---|
| <input type="radio"/> INSIGNIFICANTE | <input type="radio"/> Cumplimiento - Genera un requerimiento<br><input checked="" type="radio"/> Estratégico - Afecta el cumplimiento de algunas actividades contempladas en los planes de acción<br><input type="radio"/> Financiero - La pérdida financiera no afecta la operación normal del IDPAC<br><input type="radio"/> Imagen - Afecta a un grupo de servidores del proceso<br><input type="radio"/> Operativo - Genera ajustes a una actividad concreta<br><input type="radio"/> Tecnología - Afecta a una persona o una actividad del proceso.<br><input type="radio"/> Ninguna de las anteriores |
| <input type="radio"/> MENOR          | <input type="radio"/> Cumplimiento - Genera investigaciones disciplinarias, y/o fiscales y/o penales<br><input type="radio"/> Estratégico - Afecta el cumplimiento de las iniciativas estratégicas<br><input type="radio"/> Financiero - La pérdida financiera afecta algunos servicios del IDPAC<br><input type="radio"/> Imagen - Afecta a los servidores del proceso<br><input type="radio"/> Operativo - Genera ajustes en los procedimientos<br><input type="radio"/> Tecnología - Afecta el proceso<br><input type="radio"/> Ninguna de las anteriores  |
| <input type="radio"/> MODERADO       | <input type="radio"/> Cumplimiento - Genera interrupciones en la prestación del bien o servicio<br><input type="radio"/> Estratégico - Afecta el cumplimiento de los objetivos estratégicos del IDPAC<br><input type="radio"/> Financiero - La pérdida financiera afecta considerablemente al IDPAC<br><input type="radio"/> Imagen - Afecta a todos los servidores del IDPAC<br><input type="radio"/> Operativo - Genera ajustes o cambios en los procesos<br><input type="radio"/> Tecnología - Afecta varios procesos del IDPAC<br><input type="radio"/> Ninguna de las anteriores                       |

Al ingresar por + información se despliega la matriz de impacto con los diferentes niveles y orientaciones para determinar el impacto de acuerdo con la clase del riesgo previamente seleccionada. Identifique la opción adecuada de acuerdo con cada riesgo y utilice la opción seleccionar

Preguntas para riesgos de corrupción

|   | Preguntas DAFP           | Observaciones        |
|---|--------------------------|----------------------|
| 01. ¿Afecta al grupo de funcionarios del proceso?   | <input type="checkbox"/> | <input type="text"/> |
| 02. ¿Afecta el cumplimiento de metas y objetivos de la dependencia?   | <input type="checkbox"/> | <input type="text"/> |
| 03. ¿Afecta el cumplimiento de misión de la Entidad?  | <input type="checkbox"/> | <input type="text"/> |
| 04. ¿Afecta el cumplimiento de la misión del sector al que pertenece la Entidad?  | <input type="checkbox"/> | <input type="text"/> |
| 05. ¿Genera pérdida de confianza de la Entidad, afectando su reputación?  | <input type="checkbox"/> | <input type="text"/> |
| 06. ¿Genera pérdida de recursos económicos?   | <input type="checkbox"/> | <input type="text"/> |
| 07. ¿Afecta la generación de los productos o la prestación de servicios?  | <input type="checkbox"/> | <input type="text"/> |
| 08. ¿Da lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos? | <input type="checkbox"/> | <input type="text"/> |
| 09. ¿Genera pérdida de información de la Entidad?   | <input type="checkbox"/> | <input type="text"/> |
| 10. ¿Genera intervención de los órganos de control, de la Fiscalía, u otro ente?  | <input type="checkbox"/> | <input type="text"/> |
| 11. ¿Da lugar a procesos sancionatorios?  | <input type="checkbox"/> | <input type="text"/> |
| 12. ¿Da lugar a procesos disciplinarios?  | <input type="checkbox"/> | <input type="text"/> |

Quando el riesgo es de corrupción, se desplegará el listado de preguntas para que se marquen aquellas que podrían presentarse con la materialización del riesgo. Después de seleccionar utilice las opciones guardar y cerrar

Calificación

Zona **ZONA RIESGO EXTREMA**

Matriz


| Probabilidad      | Zonas de riesgo  |  |  |   |   |
|-------------------|--|--|--|---|---|
| 5<br>CASI CERTEZA | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo  | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 4<br>PROBABLE     | <b>ZONA RIESGO MODERADA</b><br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 3<br>MODERADA     | <b>ZONA RIESGO BAJA</b><br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO MODERADA</b><br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 2<br>IMPROBABLE   | <b>ZONA RIESGO BAJA</b><br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO BAJA</b><br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO MODERADA</b><br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo    | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 1<br>RARO         | <b>ZONA RIESGO BAJA</b><br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO BAJA</b><br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO MODERADA</b><br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo    | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo    |

Con la selección de la probabilidad y el impacto, el sistema de manera automática mostrará la ubicación del riesgo inherente en la matriz

| Probabilidad      | Zonas de riesgo  |  |  |
|-------------------|--|--|--|
| 5<br>CASI CERTEZA | <b>ZONA RIESGO EXTREMA</b> 15<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b> 20<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b> 25<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 4<br>PROBABLE     | <b>ZONA RIESGO ALTA</b> 12<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo    | <b>ZONA RIESGO EXTREMA</b> 16<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b> 20<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 3<br>MODERADA     | <b>ZONA RIESGO ALTA</b> 9<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO EXTREMA</b> 12<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b> 15<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 2<br>IMPROBABLE   | <b>ZONA RIESGO MODERADA</b> 6<br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b> 8<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO EXTREMA</b> 10<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 1<br>RARO         | <b>ZONA RIESGO MODERADA</b> 3<br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b> 4<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO ALTA</b> 5<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     |
| Impacto           | MODERADO 3   | MAYOR 4  | CATASTRÓFICO 5   |

Quando el riesgo es de corrupción la matriz solo habilita los tres mayores niveles de impacto

Comentario\*



DESCRIPCIÓN DEL ESTABLECIMIENTO DE LA PROBABILIDAD Y EL IMPACTO DEL RIESGO]

body

Registrar materialización
Guardar
Siguiente

Después de la matriz de evaluación inherente del riesgo, se debe diligenciar el campo comentario con el análisis de los resultados de la evaluación inherente; una vez se diligencie este campo, utilice la opción siguiente para ir a la etapa posterior



**Conservar controles**

¿Desea conservar los controles de la última valoración?

**Aceptar** **Cancelar**

Al iniciar la etapa de valoración el sistema genera la alerta que se presenta en la imagen; se recomienda siempre usar la opción **ACEPTAR** para evitar perder la información de los controles. En caso de seleccionar **CANCELAR**, se borrará toda la información de los controles existentes

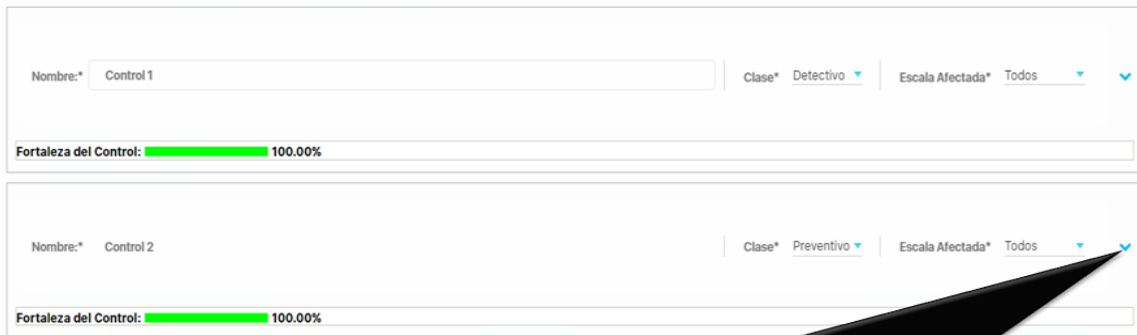
### c) Etapa de valoración





Agregar un control **Nuevo** Existente

Para crear controles, utilice la opción de nuevo; si el proceso que se está surtiendo es de actualización, el sistema mostrará los controles actualmente asociados al riesgo



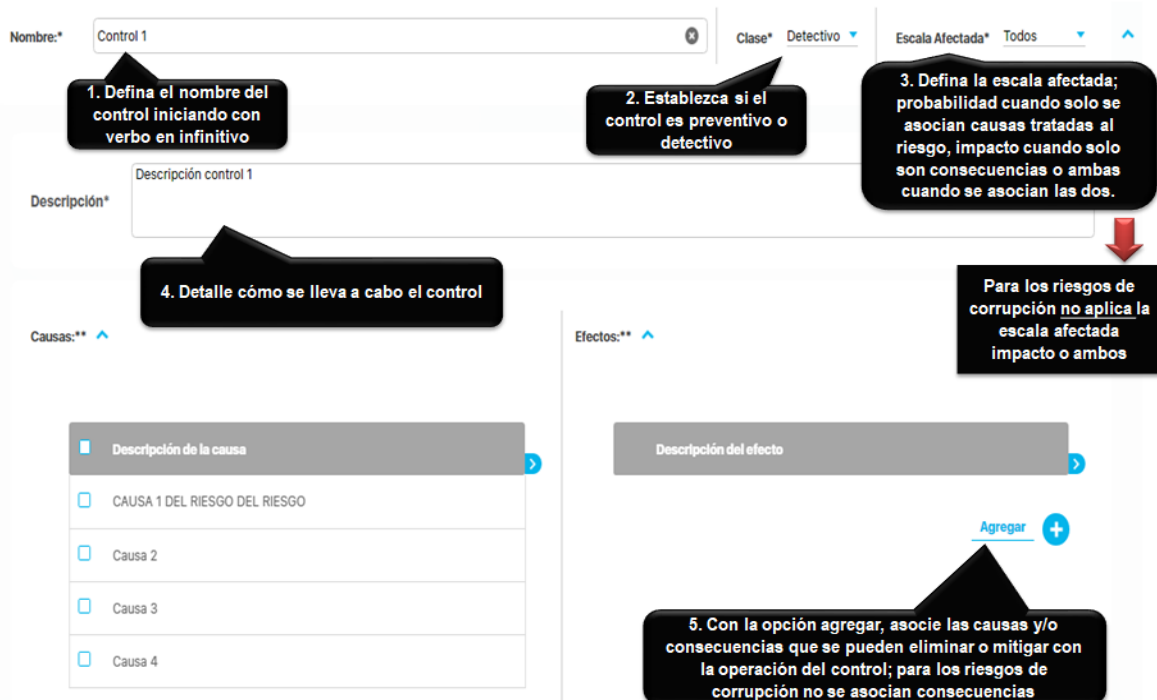
Nombre:\* Control 1 Clase\* Detectivo Escala Afectada\* Todos

Fortaleza del Control: 100.00%

Nombre:\* Control 2 Clase\* Preventivo Escala Afectada\* Todos

Fortaleza del Control: 100.00%

Para desplegar el detalle de la información de cada control utilice la opción señalada



Nombre:\* Control 1 Clase\* Detectivo Escala Afectada\* Todos

1. Defina el nombre del control iniciando con verbo en infinitivo

2. Establezca si el control es preventivo o detectivo

3. Defina la escala afectada; probabilidad cuando solo se asocian causas tratadas al riesgo, impacto cuando solo son consecuencias o ambas cuando se asocian las dos.

Descripción\* Descripción control 1

4. Detalle cómo se lleva a cabo el control

Causas:\*\*

- Descripción de la causa
- CAUSA 1 DEL RIESGO DEL RIESGO
- Causa 2
- Causa 3
- Causa 4

Efectos:\*\*

Descripción del efecto

5. Con la opción agregar, asocie las causas y/o consecuencias que se pueden eliminar o mitigar con la operación del control; para los riesgos de corrupción no se asocian consecuencias

Para los riesgos de corrupción no aplica la escala afectada impacto o ambos

Agregar +

### Propósito\*

Determinar para qué se realiza el control, ejemplo: Para un control denominado validar el cumplimiento de los bienes a recibir, el propósito es determinar si los bienes recibidos cumplen con las características definidas en el contrato de acuerdo con las necesidades establecidas.

### Documentación del control\*

Indique el documento del proceso en el cual se describe el control. Ejemplo: en el procedimiento de administración de bienes y servicios. No es una opción válida para este campo indicar de forma genérica que se encuentra en los documentos del proceso.

### Responsable\*

Persona asignada para ejecutar el control, la persona asignada, debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas (Riesgos de corrupción). Ejemplo: El coordinador de operaciones. Cuando un control se hace de manera manual (ejecutado por personas) es importante establecer el cargo responsable de su realización; cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es importante establecer como responsable de ejecutar el control al sistema o aplicación.

### Periodicidad\*

El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Hay controles que no tienen una periodicidad específica como, por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores solo se ejecutan cuando se contrata proveedores. La periodicidad debe quedar redactada de tal forma que indique: que cada vez que se desarrolla la actividad se ejecuta el control.

[Registrar materialización](#) [Guardar](#) [Siguiente](#)

De acuerdo con las orientaciones conceptuales y metodológicas de la guía, registre la información requerida en cada espacio

### Desviaciones y observaciones\*

El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Ejemplo: En caso de encontrar

### Evidencias\*

El control debe dejar evidencia de su ejecución. Esta evidencia permite validar la información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos. Ejemplo: Como evidencia: la respectiva lista de chequeo diligenciada con la información de la carpeta del cliente y correos solicitando la información faltante en los casos que aplique.

De acuerdo con las orientaciones conceptuales y metodológicas de la guía, registre la información requerida en cada espacio

**Descripción** - ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?

- Confiable
- No confiable

**Responsable** - ¿Existe un responsable asignado para la ejecución del control?

- Asignado
- No Asignado

**Periodicidad** - ¿La oportunidad en la que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?

- Oportuna
- Inoportuna

**Evidencia de aplicación del control** - ¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?

- Completa
- Incompleta
- No existe evidencia

**Propósito** - ¿Las actividades que se desarrollan en el control buscan prevenir o detectar las causas que dan origen al riesgo?

- Prevenir
- Detectar
- No es un control

**Responsable** - ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?

- Adecuado
- Inadecuado

**Observaciones o desviaciones** - ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?

- No investigan y resuelven oportunamente
- Se investigan y resuelven oportunamente

A partir de la información cualitativa documentada previamente para el control, marque para cada pregunta la respuesta adecuada.

Cancelar cambios

Eliminar

Guardar control

Cuando se diligencie toda la información del control, se debe guardar cada control de manera independiente; si solo se utiliza la opción general de la etapa para guardar, se perderá la información de los controles

Cobertura de las causas: 100.00%      Calificación del conjunto: **I=100.00%**      **P=100.00%**

|                                       |                   |                        |
|---------------------------------------|-------------------|------------------------|
| Nombre* Control1                      | Clase* Detectivo  | Escala Afectada* Todos |
| Fortaleza del Control: <b>100.00%</b> |                   |                        |
| Nombre* Control2                      | Clase* Preventivo | Escala Afectada* Todos |
| Fortaleza del Control: <b>100.00%</b> |                   |                        |

Después de registrar la información de cada control el sistema muestra el nivel de fortaleza de cada control y la calificación del conjunto de controles

| Probabilidad      | Zona de riesgo residual  |  |  |  |  |
|-------------------|--|--|--|--|--|
| 5<br>CASI CERTEZA | <b>ZONA RIESGO ALTA</b> 5<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO ALTA</b> 10<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo    | <b>ZONA RIESGO EXTREMA</b> 15<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b> 20<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b> 25<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 4<br>PROBABLE     | <b>ZONA RIESGO MODERADA</b> 4<br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b> 8<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO ALTA</b> 12<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo    | <b>ZONA RIESGO EXTREMA</b> 16<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b> 20<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 3<br>MODERADA     | <b>ZONA RIESGO BAJA</b> 3<br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO MODERADA</b> 6<br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b> 9<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO EXTREMA</b> 12<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo | <b>ZONA RIESGO EXTREMA</b> 15<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 2<br>IMPROBABLE   | <b>ZONA RIESGO BAJA</b> 2<br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO BAJA</b> 4<br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO MODERADA</b> 6<br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b> 8<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO EXTREMA</b> 10<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo |
| 1<br>RARO         | <b>ZONA RIESGO BAJA</b> 1<br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO BAJA</b> 2<br>Asumir el riesgo<br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir     | <b>ZONA RIESGO MODERADA</b> 3<br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir | <b>ZONA RIESGO ALTA</b> 4<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     | <b>ZONA RIESGO ALTA</b> 5<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo     |
| Impacto           | INSIGNIFICANTE 1   | MENOR 2  | MODERADO 3   | MAYOR 4  | CATASTRÓFICO 5   |

A partir de la calificación del conjunto de controles, el sistema establecerá de manera automática la evaluación del riesgo residual

| Probabilidad      | Zona de riesgo residual   |   |   |
|-------------------|---|---|---|
| 5<br>CASI CERTEZA | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>15 | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>20 | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>25 |
| 4<br>PROBABLE     | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>12    | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>16 | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>20 |
| 3<br>MODERADA     | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>9     | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>12 | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>15 |
| 2<br>IMPROBABLE   | <b>ZONA RIESGO MODERADA</b><br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>6 | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>8     | <b>ZONA RIESGO EXTREMA</b><br>Evitar el riesgo<br>Reducir el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>10 |
| 1<br>RARO         | <b>ZONA RIESGO MODERADA</b><br>Asumir el riesgo<br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>3 | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>4     | <b>ZONA RIESGO ALTA</b><br>Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir<br>Asumir el riesgo<br>5     |
| Impacto           | MODERADO 3  | MAYOR 4   | CATASTRÓFICO 5  |

Quando el riesgo es de corrupción, en la evaluación residual solo se podrán presentar desplazamientos en la escala de probabilidad; el impacto no debe modificarse

Plan de contingencia:

Requiere  No

La definición de acciones de contingencia aplica para todos los riesgos, independiente de su evaluación residual o de los controles existentes y consiste en la definición de acciones inmediatas a desarrollar en el caso de materialización del riesgo; estas acciones son la respuesta inicial a la materialización del riesgo y se enfocan en las correcciones que se deben desarrollar de acuerdo con las consecuencias definidas.

**Describe las acciones de contingencia de acuerdo con los lineamientos establecidos**

Comentario de valoración\*

**Registre el comentario de análisis de la evaluación residual del riesgo**

### d) Etapa de manejo

|                |              |                       |                 |            |
|----------------|--------------|-----------------------|-----------------|------------|
| Nuevo          | Identificado | Calificado y evaluado | <b>Valorado</b> | Gestionado |
| 1              | 2            | 3                     | <b>4</b>        | 5          |
| Identificación | Análisis     | Valoración            | <b>Manejo</b>   | Monitoreo  |

Etapa 4: Manejo 24/may/2019 11:41

Opciones de manejo:\*\*

- Asumir el riesgo
- Reducir el riesgo
- Evitar el riesgo
- Compartir o transferir

De acuerdo con la ubicación del riesgo residual en la matriz de evaluación, seleccione la opción de manejo que corresponda

Calcular semáforo del riesgo basado en\*

Según la zona de riesgo

Para el semáforo del riesgo, seleccione la opción "Según la zona de riesgo"

Fecha programada de monitoreo\*

dd/MM/aaaa hh:mm

Enviar correo de recordatorio con

0

días de anticipación

Programa la fecha del siguiente monitoreo y establezca los tiempos para activar el recordatorio de registro del monitoreo

Comentario de manejo\*

Rich text editor with toolbar and text area.

Registre el comentario general del manejo del riesgo

Archivos adjuntos (0)

Conceptos asociados (0)

(\* Campos obligatorios para pasar a la etapa de monitoreo.

Nota: Para aplicar los cambios realizados deberá oprimir el botón "Guardar", de lo contrario ningún cambio será tenido en cuenta.

Historial de comentarios

Historial de cambio de responsable y gestor

Historial de activación y desactivación

Utilice la opción de siguiente para ir a la etapa de monitoreo

Registrar materialización

Guardar

Siguiente

## e) Etapa de monitoreo

Nuevo

1

Identificación

Identificado

2

Análisis

Calificado y evaluado

3

Valoración

Valorado

4

Manejo

Gestionado

5

Monitoreo

Etapa 5: Monitoreo 31/jul/2019 08:44

Registre la fecha del monitoreo

Fecha de monitoreo\*  [Matriz de evolución actual](#) Para monitorear tenga en cuenta ⓘ

Registro de monitoreo periódico del riesgo\*

| Nombre del control *  | Estado de aplicación del control * | Evidencias de aplicación del control * | ¿El control permitió evitar la materialización del riesgo? * | Observaciones adicionales                    |
|---|------------------------------------|--|--|--|
| <input type="checkbox"/> <input type="text" value="Cualquier texto"/> | <input type="text"/>               | <input type="text"/>                   | <input type="text"/>   | <input type="text" value="Cualquier texto"/> |
| <input type="checkbox"/> <input type="text" value="Cualquier texto"/> | <input type="text"/>               | <input type="text"/>                   | <input type="text"/>   | <input type="text" value="Cualquier texto"/> |

[Agregar](#) +

Mediante la opción agregar, incluya la cantidad de filas igual al número de controles asociados al riesgo y registre la información solicitada en cada espacio

Comentario de monitoreo\*

En el campo general del monitoreo, registre el periodo al que hace referencia el monitoreo registrado; ejemplo: se registra el monitoreo del riesgo para el periodo comprendido entre el 01 de mayo y el 31 de agosto de 2019

Archivos adjuntos (0) v

Conceptos asociados (0) v

Adjunte de manera organizada las evidencias que soportan la operación de cada control; se deben adjuntar en carpetas comprimidas para cada control asociado al riesgo; cuando el volumen de evidencias para cada control es elevado, se recomienda adjuntar una muestra

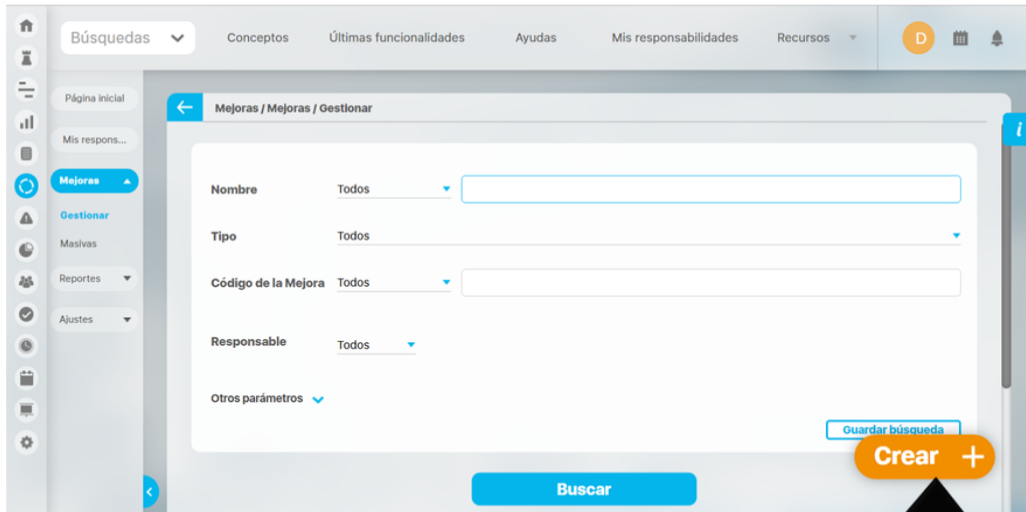
Fecha de próximo monitoreo\*  Enviar correo de recordatorio con  días de anticipación ⓘ

Registrar materialización
Inactivar
Volver a valorar
Programar otro monitoreo

Programar las fechas del siguiente monitoreo y utilizar la opción "Programar otro monitoreo" para guardar la información



## f) Solicitudes de creación, modificación o eliminación de riesgos



Para crear riesgos, registre la solicitud en el módulo de mejoras, mediante el flujo de solicitudes del SIG. Como mecanismo de control, solo la Oficina Asesora de Planeación tiene habilitada la opción del registro inicial de riesgos en el sistema

|   |  |
|---|--|
| Etapa 1: Identificación 31/jul/2019 08:54 | <a href="#">Volver a identificar</a> ▼ |
| Etapa 2: Análisis 31/jul/2019 08:56       | <a href="#">Volver a analizar</a> ▼    |
| Etapa 3: Valoración 31/jul/2019 09:30     | <a href="#">Volver a valorar</a> ▼     |
| Etapa 4: Manejo 31/jul/2019 09:30         | <a href="#">Volver a manejar</a> ▼     |

Para modificaciones, cuando se ingresa al sistema a consultar la información del riesgo, para los roles de gestor y responsable de cada riesgo, se habilitan las opciones de volver a las diferentes etapas del riesgo; al ingresar por estas opciones, se despliega un campo de comentario que se debe diligenciar con la justificación de devolución de las etapas del riesgo



Una vez se ingresa y guarda la justificación, la Oficina Asesora de Planeación verifica la solicitud y si es viable devuelve a etapa del riesgo

← Gestión del riesgo / Mis responsabilidades

### Gestión del Riesgo

[Ver matriz de evolución](#)

|                |              |                       |          |            |
|----------------|--------------|-----------------------|----------|------------|
| Nuevo          | Identificado | Calificado y evaluado | Valorado | Gestionado |
| 1              | 2            | 3                     | 4        | 5          |
| Identificación | Análisis     | Valoración            | Manejo   | Monitoreo  |

**Nombre:** NOMBRE DEL RIESGO

**Responsable:** Dayssi Tatiana Santos Yates | **Gestor:** Dayssi Tatiana Santos Yates

**Descripción:** DESCRIPCIÓN DEL RIESGO CON LOS ASPECTOS QUE SE NECESITEN ACLARAR RESPECTO AL NOMBRE DEL RIESGO IDENTIFICAR INCLUIR CAUSAS O CONSECUENCIAS DEL RIESGO

**Clase:** Cumplimiento

¿Este riesgo es institucional? +

[Registrar materialización](#) [Inactivar](#) [Volver a valorar](#) [Programar otro monitoreo](#)

Para eliminación de riesgos, los gestores y responsables siempre que consulten el riesgo tienen la opción de inactivar habilitada; para la cual deberán registrar un comentario con la justificación correspondiente. Una vez registrada la justificación la Oficina Asesora de Planeación verificará y tramitará la solicitud