

 <b>INSTITUTO POPULAR DE CULTURA</b>	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

## **POLÍTICA DE ADMINISTRACIÓN DEL RIESGO**

**Versión 2**

**Gestión de Planeación Estratégica  
Agosto de 2022**

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

## Contenido

1. INTRODUCCIÓN .....	3
2. MARCO NORMATIVO .....	4
3. OBJETIVO .....	6
4. ALCANCE .....	6
5. ÁMBITO DE APLICACIÓN .....	6
6. TÉRMINOS Y DEFINICIONES .....	6
7. RESPONSABILIDADES .....	10
8. LINEAMIENTOS GENERALES PARA LA ADMINISTRACIÓN DEL RIESGO	14
8.1. Nivel de Aceptación o Tolerancia al Riesgo .....	14
8.2. Definición y clasificación del riesgo.....	14
8.3. Determinar la probabilidad de ocurrencia .....	16
8.4. Niveles para calificar el impacto.....	18
9. EVALUACIÓN DEL RIESGO .....	20
9.1. Análisis preliminar (riesgo inherente) .....	20
9.2. Actividades de control.....	21
9.2.1. Estructura para la descripción del control .....	21
9.2.2. Tipología de controles y los procesos .....	22
9.2.3. Análisis y evaluación de los controles.....	23
9.2.4. Riesgo Residual .....	26
10. TRATAMIENTO Y OPCIONES DE MANEJO .....	27
11. MATERIALIZACIÓN DE LOS RIESGOS.....	29
12. COMUNICACIÓN Y CONSULTA .....	30
13. SEGUIMIENTO Y MONITOREO .....	30
14. RECURSO.....	32

 <b>INSTITUTO POPULAR DE CULTURA</b>	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

## 1. INTRODUCCIÓN

El Instituto Popular de Cultura define su política del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión – MIPG en los procesos, así como los del Modelo Estándar de Control Interno, en lo referente a las líneas de defensa, los lineamientos de la Guía para la Administración del Riesgo (versión 5 de Diciembre de 2020) emitida por el Departamento Administrativo de la Función Pública – DAFP, la cual articula los riesgos de gestión, corrupción y de seguridad digital y la estructura del Sistema Integrado de Gestión – SGI en el módulo de riesgos.

La actualización a la política de riesgos obedece a los cambios introducidos en la versión 5 de la guía, en la cual se precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo. El Instituto Popular de Cultura adopta la guía con el objetivo de unificar los lineamientos para la administración de todo tipo de riesgos al interior del instituto, para fortalecer el enfoque preventivo y gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso del IPC.

Todos los procesos y dependencias deben establecer los lineamientos que permitan la identificación, el análisis, la valoración y el tratamiento de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos, mediante:

- a) La identificación y documentación de riesgos de gestión (financieros, contractuales, jurídicos, entre otros), corrupción y de seguridad digital en los procesos.
- b) El establecimiento de acciones de control preventivas y detectivas para los riesgos identificados.
- c) La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

El Instituto Popular de Cultura en coherencia con el Sistema Integrado de Gestión y de acuerdo con los requerimientos legales y normativos, se compromete a implementar acciones para la administración de sus riesgos a través de la

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

identificación, análisis, valoración, evaluación y tratamiento de los mismos, con el fin de garantizar una gestión pública que responda a las diversas necesidades y expectativas de los usuarios y partes interesadas

## 2. MARCO NORMATIVO

El artículo 73 de la Ley 1474 de 2011 *“Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”*, determinó que *“Cada Entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contempla, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano”*.

El Decreto 1081 de 2015 *“Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República”*, compilatorio del Decreto 2641 de 2012 y reglamentario de los artículos 73 y 76 de la Ley 1474 de 2011, estableció como metodología para diseñar y hacer seguimiento a dicha estrategia la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento *“Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano Versión 2”*.

A través del Decreto 124 del 26 de enero de 2016 *“Por el cual se sustituye el Título IV de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al “Plan Anticorrupción y de Atención al Ciudadano”*, se estableció en su Artículo 2.1.4.1 como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011.

El Decreto 1083 de 2018 en su artículo 2.2.21.5.4 consagra: *“Administración de riesgos. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspecto tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos”*.

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Con la expedición del Decreto 1499 de 2017 “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”, se realizó la articulación entre el Modelo Integrado de Planeación y Gestión MIPG y el Sistema de Control Interno.

A partir de esta actualización, surge dentro de este modelo la Dimensión de Control Interno y en su estructura se detalla el Componente de Evaluación del Riesgo orientado a identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que puedan afectar o impedir el logro de los objetivos institucionales.

A continuación, se listan los diferentes decretos y normativas consideradas para la gestión del riesgo de la Entidad:

Decreto 648 de 2017 “Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública”.

Norma Técnica Colombiana ISO 9001:2015 Sistema de Gestión de la Calidad.

Norma Técnica Colombiana ISO 31000:2018 Gestión del Riesgo.

Norma Técnica Colombiana ISO/IEC 27001:2013 “Sistema de Gestión de la Seguridad de la Información”.

Norma Técnica Colombiana ISO 27005:2018 “Seguridad de la información y las comunicaciones”.

Resolución No. 200.52.04.18.17 “Por medio de la cual se crea el Comité Institucional para la Gestión y el Desempeño del Instituto Popular de Cultura IPC” precedido por la directora y la coordinadora académica general.

El Instituto Popular de Cultura mediante Resolución No. 200.52.04.18.28 “Por medio de la cual se crea el Comité Institucional de Coordinación de Control Interno del Instituto Popular de Cultura IPC” precedido por la directora y la coordinadora académica general.

Y la “*Guía para administración de riesgos y diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital*” Versión 5 de 2020, del Departamento Administrativo de la Función Pública.

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

### 3. OBJETIVO

Establecer lineamientos para la identificación, valoración y tratamiento de los riesgos de gestión, corrupción y seguridad de la información mediante el control y seguimiento de estos, con el fin de disminuir o eliminar su impacto en el logro de los objetivos institucionales en los procesos estratégicos, misionales, de apoyo y de seguimiento y evaluación del Instituto Popular de Cultura.

### 4. ALCANCE

La política de administración del riesgo inicia desde la identificación, análisis, valoración, seguimiento y monitoreo de los riesgos siendo aplicables a todos los niveles de la institución y a los procesos del Modelo Operativo por procesos del Instituto Popular de Cultura.

### 5. ÁMBITO DE APLICACIÓN

La Política de Administración del Riesgo es aplicable a todos los procesos, proyectos, productos de la Entidad y a las acciones ejecutadas por los servidores públicos y contratistas durante el ejercicio de sus funciones.

El Instituto Popular de Cultura se compromete a gestionar sus riesgos definiendo medidas preventivas encaminadas a reducir, evitar, compartir o transferir aquellos que por su probabilidad de ocurrencia y/o impacto, puedan afectar el cumplimiento de los objetivos institucionales, realizando seguimiento periódico a la efectividad de los controles y acciones de control, con el compromiso y participación de las diferentes líneas de defensa institucional, propendiendo por el mejoramiento continuo de la gestión.

### 6. TÉRMINOS Y DEFINICIONES

**Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

**Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. Peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales.

**Apetito de riesgo:** 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.

**Capacidad de riesgo:** 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.

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

**Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

**Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

**Comité Institucional de Coordinación de Control Interno (CICCI):** Es un órgano de asesoría y decisión en los asuntos de control interno del Instituto Popular de Cultura. En su rol de responsable y facilitador, hace parte de las instancias de articulación para el funcionamiento del Sistema de Control Interno.

**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

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

**Control:** Medida que permite disminuir la probabilidad de ocurrencia del riesgo, mitigar el impacto de los riesgos y/o asegurar la continuidad del servicio en caso de llegarse a materializar el riesgo.

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

**Control Correctivo:** Medida que permite mitigar el impacto frente a la materialización del riesgo.

**Control detectivo:** Medida que permite disminuir la probabilidad de ocurrencia del riesgo y detectar que algo ocurre y devuelve el proceso a los controles preventivos.

**Controles Preventivos:** Medida que permite eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.

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

**Evaluación del Riesgo:** Proceso para determinar el nivel de riesgo asociado al nivel de probabilidad de que dicho riesgo se concrete y al nivel de severidad de las consecuencias de esa concreción.

**Factores de Riesgo:** Son las fuentes generadoras de riesgos.

**Fraude externo:** Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

**Fraude interno:** Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

**Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una Entidad con respecto al riesgo y proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

**Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.

**Integridad:** Propiedad de exactitud y completitud.

**Mapa de Riesgos:** Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, haciendo la descripción de cada uno de estos y las posibles consecuencias y sus acciones preventivas o correctivas.

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

**Mapa de Riesgos Institucional:** Contiene los riesgos de mayor criticidad (zona residual extrema y alta) frente al logro de los objetivos institucionales e integra los riesgos de Gestión, Corrupción y Seguridad de la Información.

**Materialización del riesgo:** Ocurrencia del evento que fue determinado como un riesgo, la probabilidad de ocurrencia se materializa convirtiéndose en un hecho o acontecimiento real y concreto.

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

**Plan Anticorrupción y de Atención al Ciudadano:** contempla la estrategia para la lucha contra la corrupción que debe ser implementado por todas las entidades del orden nacional, departamental y municipal.

**Probabilidad:** 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.

**Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. 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.

**Riesgo de Corrupción:** Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado

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

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

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

**Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.

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

**Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

## 7. RESPONSABILIDADES

Tabla 1. Responsabilidades por línea de defensa

Línea de Defensa	Responsables	Responsabilidad Frente al Riesgo
<b>Estratégica</b>	Alta Dirección, Comité Institucional de Coordinación de Control Interno - CICC	<ul style="list-style-type: none"> <li>• Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico.</li> <li>• Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo).</li> <li>• 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>• Realizar seguimiento y análisis periódico a los riesgos institucionales.</li> <li>• Realimentar al Comité de Gestión y Desempeño Institucional - CGDI sobre los ajustes que se deban hacer frente a la gestión del riesgo.</li> <li>• Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.</li> </ul>

 <b>INSTITUTO POPULAR DE CULTURA</b>	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Línea de Defensa	Responsables	Responsabilidad Frente al Riesgo
<b>Primera Línea</b>	Líderes de Procesos	<ul style="list-style-type: none"> <li>• Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera.</li> <li>• Definir, aplicar y hacer seguimiento a los controles de manera cuatrimestral mediante reunión ordinaria con su equipo de trabajo para autoevaluar el resultado de la aplicación de los controles diseñados en cada uno de los riesgos identificados y su concordancia con la medición de los respectivos indicadores de gestión.</li> <li>• Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles y de acuerdo con los resultados obtenidos se tomarán decisiones pertinentes (correctivas o acciones preventivas), que se reportan en el acta de la reunión y que también se podrán registrar en los respectivos planes de mejoramiento para facilitar el seguimiento a su ejecución y resultados.</li> <li>• Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo.</li> <li>• Reportar en el Sistema de Gestión Institucional - SGI los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.</li> <li>• En la última reunión de cada vigencia se deberán identificar, analizar y evaluar los riesgos que de acuerdo al comportamiento de la vigencia actual, aplicarán para la próxima vigencia.</li> </ul>

 <b>INSTITUTO POPULAR DE CULTURA</b>	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Línea de Defensa	Responsables	Responsabilidad Frente al Riesgo
<b>Segunda Línea</b>	Oficina Asesora de Planeación con el acompañamiento del área de gestión de calidad.	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Consolidar el Mapa de Riesgos Institucional y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional.</li> <li>• Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo.</li> <li>• Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.</li> <li>• Supervisar que la primera línea de defensa identifique, evalúe y gestione los riesgos y controles en los temas de su competencia.</li> <li>• Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.</li> <li>• Reportar anualmente a la dirección la materialización de riesgos y las acciones respectivas con los resultados obtenidos de su aplicación.</li> <li>• Proponer ajustes y mejoras a la metodología para la administración del riesgo de acuerdo con la normatividad vigente.</li> <li>• Socializar y publicar la política de administración de riesgos para su aplicación por parte de los líderes de proceso.</li> </ul>

 <b>INSTITUTO POPULAR DE CULTURA</b>	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		VERSIÓN	2
			FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Línea de Defensa	Responsables	Responsabilidad Frente al Riesgo
<b>Segunda Línea</b>	Oficina de gestión de las TIC's	Tiene la función de adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (identificación, análisis, evaluación y tratamiento), asesorar y acompañar a la primera línea de defensa en la identificación de los riesgos de seguridad de la información y el monitoreo cuatrimestral a los planes de tratamiento definidos.
<b>Tercera Línea</b>	Oficina de Control Interno	<ul style="list-style-type: none"> <li>• Realizar examen sistemático e independiente para determinar si las actividades y los resultados relacionados con la administración del riesgo cumplen las disposiciones de las políticas, planes y acciones pre establecidas.</li> <li>• 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>• Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.</li> <li>• Asesorar de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.</li> <li>• Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al CICCI.</li> <li>• Recomendar mejoras a la Política de Administración del Riesgo.</li> </ul>

Elaboración propia

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

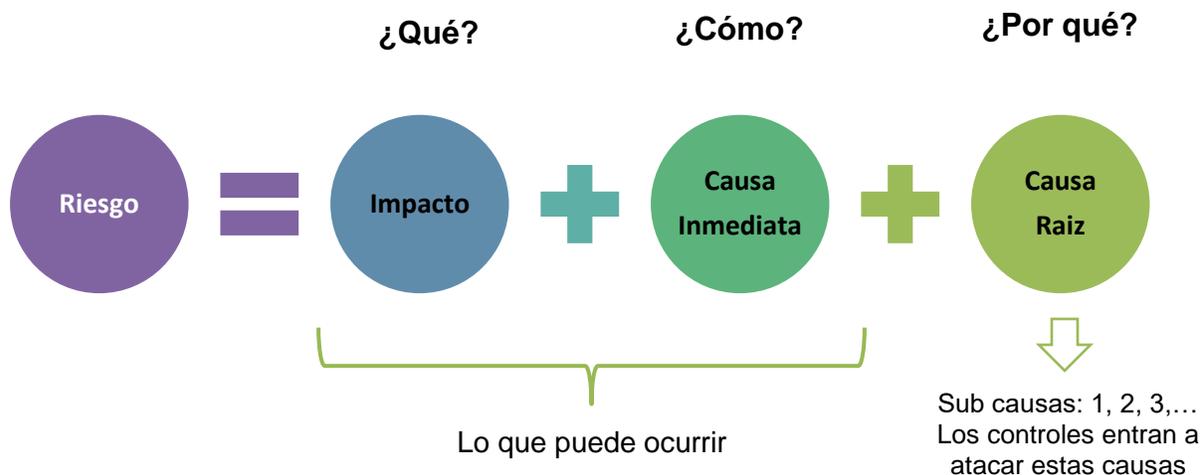
## 8. LINEAMIENTOS GENERALES PARA LA ADMINISTRACIÓN DEL RIESGO

### 8.1. Nivel de Aceptación o Tolerancia al Riesgo

El Instituto Popular de Cultura acepta los riesgos de gestión y de seguridad de la información evaluados en nivel “Bajo” y “Moderado”, con excepción de los **riesgos de corrupción**. La entidad no es flexible en la aceptación de conductas o hechos de corrupción, por lo tanto, **no hay aceptación del riesgo**, su tratamiento se realizará de acuerdo con los lineamientos de esta política.

### 8.2. Definición y clasificación del riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:



La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta se tiene que:

 <b>INSTITUTO POPULAR DE CULTURA</b>	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

- Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo (pérdida económica y/o reputacional)
- Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o sub causas que pueden ser analizadas.

Una vez descrito el riesgo se procederá a clasificarlos de acuerdo con la siguiente tabla:

Tabla 2. Clasificación de los riesgos

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

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Tipo	Descripción
	satisfacer una obligación profesional frente a éstos.
<b>Daños a activos fijos/ eventos externos</b>	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Guía de administración de riesgos versión 5. DAFP

### 8.3. Determinar la probabilidad de ocurrencia

- Para los riesgos de gestión y de seguridad de la información

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Tabla 3. Nivel de probabilidad para riesgos de gestión y de seguridad de la información

Nivel		Frecuencia de la Actividad	Probabilidad
1	Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 4 veces por año	20%
2	Baja	La actividad que conlleva el riesgo se ejecuta de 5 a 18 veces por año	40%
3	Media	La actividad que conlleva el riesgo se ejecuta de 18 a 365 veces por año	60%
4	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 365 veces al año y máximo 3660 veces por año	80%
5	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 3661 veces por año	100%

Elaboración propia

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

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		VERSIÓN	2
			FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Tabla 4. Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
<p>*Tecnología (incluye disponibilidad de aplicativos), tesorería</p> <p>*Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.</p> <p>Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.</p>	Diaria	Muy alta

Fuente: Guía de administración de riesgos versión 5. DAFP

- Para los riesgos de corrupción

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Tabla 5. Nivel de probabilidad para riesgos de corrupción

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

Elaboración propia

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

#### 8.4. Niveles para calificar el impacto

El impacto son las posibles consecuencias o afectaciones económicas y reputacional que se genera por la materialización del riesgo.

Cabe señalar que en la versión 2018 de la Guía de administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

En la tabla 6 se establecen los criterios para definir el nivel de impacto.

Tabla 6. Calificación del impacto para riesgos de gestión y de seguridad de la información

	Afectación Económica (o presupuestal)	Pérdida Reputacional o de imagen
<b>Leve 20%</b>	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
<b>Menor 40%</b>	Entre 10 y 100 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores
<b>Moderado 60%</b>	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
<b>Mayor 80%</b>	Entre 500 y 1.500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

	Afectación Económica (o presupuestal)	Pérdida Reputacional o de imagen
<b>Catastrófico 100%</b>	Mayor a 1.500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

Elaboración propia

Para los riesgos de corrupción, solo se calificará el impacto en los niveles moderado, mayor o catastrófico, considerando que ningún hecho de corrupción tendrá un impacto insignificante o menor. Para evaluar el impacto de los riesgos de corrupción se debe responder a un cuestionario de 19 preguntas con opción de respuesta binaria (Si/No) por cada riesgo identificado, teniendo en cuenta que:

- Si responden afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado.
- Si responden afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.
- Si responden afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.

Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.

Tabla 7. Cuestionario para evaluar el impacto de riesgos de corrupción.

PREGUNTAS	RESPUESTA SÍ/NO
1 ¿Afectar al grupo de funcionarios del proceso?	
2 ¿Afectar el cumplimiento de metas y objetivos de la dependencia?	
3 ¿Afectar el cumplimiento de misión de la entidad?	
4 ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?	
5 ¿Generar pérdida de confianza de la entidad, afectando su reputación?	
6 ¿Generar pérdida de recursos económicos?	
7 ¿Afectar la generación de los productos o la prestación de servicios?	
8. ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?	
9 ¿Generar pérdida de información de la entidad?	

 <b>INSTITUTO POPULAR DE CULTURA</b>	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

PREGUNTAS	RESPUESTA SÍ/NO
10 ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	
11 ¿Dar lugar a procesos sancionatorios?	
12 ¿Dar lugar a procesos disciplinarios?	
13 ¿Dar lugar a procesos fiscales?	
14 ¿Dar lugar a procesos penales?	
15 ¿Generar pérdida de credibilidad del sector?	
<b>16 ¿Ocasionar lesiones físicas o pérdida de vidas humanas?</b>	
17 ¿Afectar la imagen regional?	
18 ¿Afectar la imagen nacional?	
19 ¿Generar daño ambiental?	

Fuente: Guía de administración de riesgos versión 5. DAFP  
Elaboración propia

## 9. EVALUACIÓN DEL RIESGO

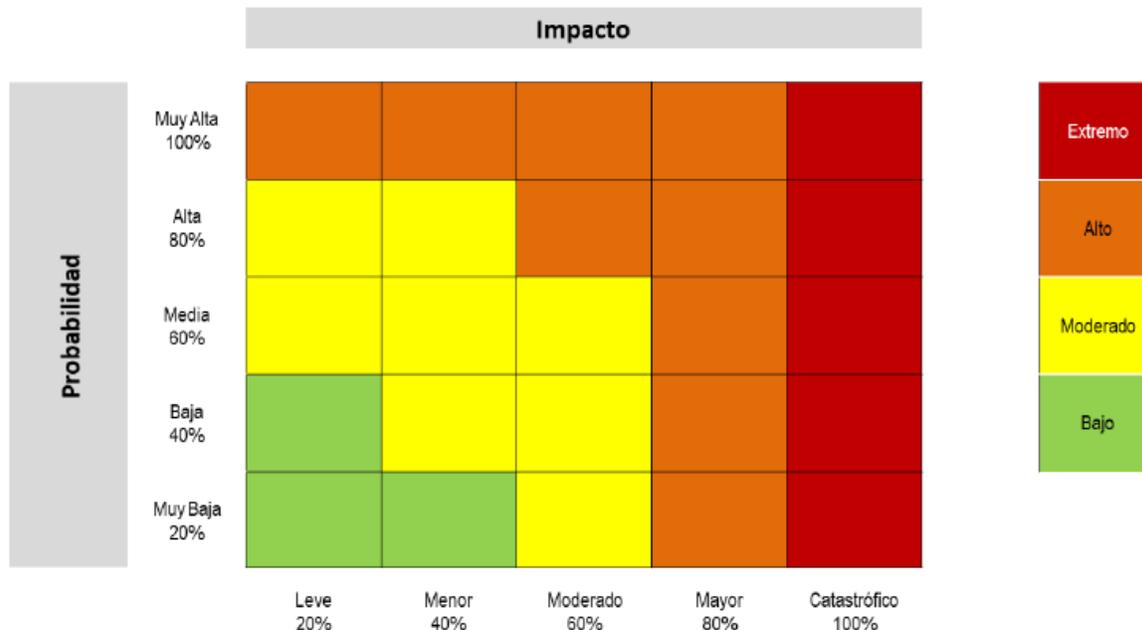
A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

### 9.1. Análisis preliminar (riesgo inherente)

A partir de la identificación de la probabilidad y el impacto, es necesario ubicar en un mapa de calor el nivel de riesgo inicial o riesgo inherente, lo cual llevará a identificar el nivel de severidad del riesgo que se encuentran en 4 zonas (Extremo, Alto, Moderado o Bajo) como se muestra a continuación:

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		VERSIÓN	2
			FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Figura 1. Matriz de calor (niveles de severidad del riesgo)



Fuente: Guía de administración de riesgos versión 5. DAFP

## 9.2. Actividades de control

Las actividades de control son aquellas acciones documentadas e implementadas que contribuyen a mitigar los riesgos que inciden en el cumplimiento de los objetivos, para el diseño de las actividades de control se tendrá en cuenta elementos como el diseño y la ejecución del respectivo control.

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

### 9.2.1. Estructura para la descripción del control

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

Figura 2. Representación de la redacción del control

Responsable	Acción	Complemento
<ul style="list-style-type: none"> <li>• El profesional de Contratación</li> </ul>	<ul style="list-style-type: none"> <li>• verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos acorde con el tipo de contratación</li> </ul>	<ul style="list-style-type: none"> <li>• a través del informe de evaluación y una lista de chequeo donde están los requisitos de la información que debe ser registrada en los sistemas de información en contratación (SECOP y SIA Observa).</li> </ul>

Fuente: Guía de administración de riesgos versión 5. DAFP

### 9.2.2. Tipología de controles y los procesos

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

### 9.2.3. Análisis y evaluación de los controles

La valoración de las actividades de control tiene como objetivo identificar tal como se ha mencionado, si estas se encuentran bien diseñadas y ejecutadas, lo anterior, permitirá la mitigación de los riesgos que enfrentan las entidades.

Para la valoración de las actividades de control con respecto al diseño y la ejecución se tiene en cuenta la siguiente tabla

Tabla 7. Atributos para el diseño del control

Características		Descripción	Peso	
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	30%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	20%
		Correctivo	Permite reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos*	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales,	

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		VERSIÓN	2
			FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Características		Descripción	Peso
			procedimientos, flujogramas o cualquier otro documento propio del proceso.
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.
		Sin registro	El control no deja registro de la ejecución del control.

Fuente: Guía de administración de riesgos versión 5. DAFP  
Elaboración propia

**\*Nota:** Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

A partir de los controles se dará el movimiento en la matriz de calor, puede ser en el eje de probabilidad y/o en el eje de impacto de acuerdo con los tipos de controles.

Ejemplo de aplicación de controles para la mitigación del riesgo.

- Proceso: gestión jurídica  
 Sub proceso: gestión de Adquisición de Bienes, Obras y Servicios  
 Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación  
 Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos  
 Probabilidad Inherente: media 60%  
 Impacto Inherente: mayor 80%  
 Zona de riesgo: alta

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Controles identificados:

**Control 1:** La persona profesional del área verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través del informe de evaluación y una lista de chequeo donde están los requisitos de la información que debe ser registrada en los sistemas de información en contratación (SECOP y SIA Observa).

**Control 2:** la persona asesora y líder del área jurídica verifica en los sistema de información en contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Tabla 8. Aplicación tabla atributos a ejemplo propuesto

Controles y sus características				Peso
La persona profesional del área verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través del informe de evaluación y una lista de chequeo donde están los requisitos de la información que debe ser registrada en los sistemas de información en contratación (SECOP y SIA Observa).	Tipo	Preventivo	X	30%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	
		Sin documentar		
	Frecuencia	Continua	X	
		Aleatoria		
	Evidencia	Con registro	X	
Sin registro				
<b>Total valoración control 1</b>				<b>45%</b>
La persona asesora y líder del área jurídica verifica en los sistema de información en contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	Tipo	Preventivo		
		Detectivo	X	20%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	
		Sin documentar		
	Frecuencia	Continua	X	
		Aleatoria		
	Evidencia	Con registro	X	

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Controles y sus características			Peso
		Sin registro	
<b>Total valoración control 2</b>			<b>35%</b>

Elaboración propia

#### 9.2.4. Riesgo Residual

Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que estos **mitigan el riesgo de forma acumulativa**, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Para mayor claridad, en la tabla 9 se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles

Tabla 9. Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	45%	60% x 45% = 27% 60% - 27% = 33%
	Valor probabilidad para aplicar 2do control	33%	Valoración control 2 detectivo	35%	33% * 35% = 11,55% 33%-11,55% = 21,45%
	<b>Probabilidad Residual</b>	<b>21,45%</b>			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	<b>Impacto Residual</b>	<b>80%</b>			

Elaboración propia

**Para el ejemplo anterior el riesgo residual sería así:**

Proceso: gestión jurídica

Sub proceso: gestión de Adquisición de Bienes, Obras y Servicios

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos

Probabilidad residual: baja a 21,45%

Impacto residual: mayor 80%

Zona de riesgo residual: alta

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

**Nota:** En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

## 10. TRATAMIENTO Y OPCIONES DE MANEJO

A continuación, se describe los tipos de tratamiento para la mitigación de los diferentes riesgos:

- **Aceptar el riesgo:** Aceptar la pérdida residual probable, lo cual permite a la Entidad asumirlo, es decir, el riesgo se encuentra en un nivel que es aceptado por la misma, sin embargo, el líder del proceso deberá realizar un seguimiento a los controles existentes de su mapa de riesgos, sin que esto genere acciones distintas a las existentes con el fin de fomentar lecciones aprendidas.
- **Reducir el riesgo:** Implica implementar controles orientados a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas de protección), con el fin de llevar los riesgos ubicados en zona alta y extrema a la zona baja o moderada que son aquellos que asume la Entidad.
- **Evitar el riesgo:** Implementar medidas para prevenir la materialización de los riesgos ubicados en la zona alta y extrema, siendo necesario eliminar la actividad que genera el riesgo.
- **Compartir el riesgo:** Implica que la responsabilidad económica recae sobre el tercero pero no se transfiere la responsabilidad sobre el tema reputacional. Por ejemplo, cuando se establecen contratos de riesgos compartidos, seguros, etc.

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

Para el tratamiento de los riesgos de gestión y de seguridad de la información se tendrá en cuenta la zona del riesgo, como lo indica la Tabla 10.

Tabla 10. Tratamiento de los riesgos de gestión y de seguridad de la información por zona de riesgo.

Zona de Riesgo	Tratamiento
Zona Baja	Mantener las acciones asociadas a la mitigación del riesgo ya existentes
Zona Moderada	
Zona Alta	Deben tomarse medidas necesarias para reducir, evitar o compartir el riesgo, manteniéndolo identificado y controlado
Zona Extrema	Tratamiento prioritario. Implementar controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección para reducir, evitar o compartir el riesgo, manteniendo identificado y controlado.

Fuente: Política de administración de riesgos. Versión 4. Alcaldía de Santiago de Cali.  
Elaboración propia

Para el tratamiento y manejo de los riesgos de corrupción la Entidad siempre tomará medidas necesarias para reducir, evitar o compartir el riesgo, como lo indica la Tabla 11:

Tabla 11. Tratamiento de los riesgos de corrupción por zona de riesgo.

Zona de Riesgo	Tratamiento
Zona Moderada	Deben tomarse medidas necesarias para reducir, evitar o compartir el riesgo, manteniéndolo identificado y controlado.
Zona Alta	Deben tomarse medidas necesarias para reducir, evitar o compartir el riesgo, manteniéndolo identificado y controlado.
Zona Extrema	Tratamiento prioritario. Implementar controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección para reducir, evitar o compartir el riesgo, manteniéndolo identificado y controlado.

Fuente: Política de administración de riesgos. Versión 4. Alcaldía de Santiago de Cali.  
Elaboración propia

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

## 11. MATERIALIZACIÓN DE LOS RIESGOS

- **Riesgos de gestión y de seguridad de la información**

Si dentro del seguimiento realizado a los riesgos de gestión y de seguridad de la información por cualquiera de las líneas de defensa se identifica que se han materializado uno o más riesgos, las acciones requeridas son las siguientes por parte del líder del proceso:

1. Tomar los correctivos necesarios ante la situación presentada.
2. Identificar las causas que originaron la materialización del riesgo, teniendo en cuenta las metodologías vigentes (Cinco porqués, Árbol de problemas, Causa y efecto, 5W-2H, Patrones de similitud, Lluvia de ideas).
3. Analizar los impactos generados por la materialización del riesgo
4. Realizar revisión y ajuste de controles que permitan disminuir probabilidad de ocurrencia del riesgo y/o mitigar impactos. Tener en cuenta lo siguiente: diseñar controles que ataquen nuevas causas y/o impactos, y ajustar el control si la evaluación es débil en diseño o en ejecución.
5. Dejar registro mediante acta de reunión del análisis donde se especifique los pasos anteriores.
6. Formular el plan de mejoramiento donde se registren las causas y las acciones de mejora identificadas.
7. Analizar y actualizar (si aplica) el mapa de riesgos del proceso en la herramienta, matriz de Excel, denominada "Mapa de riesgos por proceso".
8. Informar a la segunda línea de defensa sobre los riesgos materializados mediante comunicación oficial anexando plan de mejoramiento formulado y acta de análisis, según lo establecido en el numeral 13. Seguimiento y Monitoreo.
9. Informar a la oficina de Gestión de TIC's sobre la materialización de los riesgos de seguridad informática mediante comunicación oficial anexando plan de mejoramiento formulado y acta de análisis, en cumplimiento de la política de Gobierno Digital y Seguridad Digital.
10. Informar en el Comité Institucional de Coordinación de Control Interno las causas que dieron origen a la materialización de los riesgos y las acciones de mejora, donde se tomarán las decisiones pertinentes.

- **Riesgos de corrupción**

Si dentro del seguimiento realizado a los riesgos de corrupción por cualquiera de las líneas de defensa se identifica que se han materializado uno o más riesgos, las acciones requeridas son las siguientes por parte del líder del proceso:

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

1. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo.
2. Identificar las causas que originaron la materialización del riesgo, teniendo en cuenta las metodologías vigentes (Cinco porqués, Árbol de problemas, Causa y efecto, 5W-2H, Patrones de similitud, Lluvia de ideas).
3. Analizar los impactos generados por la materialización del riesgo
4. Realizar revisión y ajuste de controles que permitan disminuir probabilidad de ocurrencia del riesgo y/o mitigar impactos. Tener en cuenta lo siguiente: diseñar controles que ataquen nuevas causas y/o impactos, y ajustar el control si la evaluación es débil en diseño o en ejecución.
5. Dejar registro mediante acta de reunión del análisis donde se especifique los pasos anteriores.
6. Formular el plan de mejoramiento donde se registren las causas y las acciones de mejora identificadas.
7. Analizar y actualizar el mapa de riesgos del proceso en la herramienta metodológica, matriz de Excel, denominada “Mapa de riesgos por proceso”.
8. Informar a la oficina de Gestión de TIC’s sobre los riesgos materializados mediante comunicación oficial anexando plan de mejoramiento formulado y acta de análisis, según lo establecido en el numeral 13. Seguimiento y Monitoreo.
9. Informar en el Comité Institucional de Coordinación de Control Interno las causas que dieron origen a la materialización de los riesgos y las acciones de mejora, donde se tomarán las decisiones pertinentes.

## **12.COMUNICACIÓN Y CONSULTA**

La oficina de gestión de planeación estratégica articulará con la oficina de gestión de comunicación, las estrategias para la difusión de la Política de Administración de Riesgos y cada área o escuela implementará en coordinación con su equipo de trabajo.

La oficina de gestión de planeación estratégica a través de la oficina de Gestión de TIC’s, mantendrá actualizada en el enlace de Transparencia de la página web del Instituto Popular de Cultura, la política de administración de riesgo, los Mapas de Riesgos de los procesos y el Mapa de Riesgos Institucional.

## **13.SEGUIMIENTO Y MONITOREO**

Los líderes de los procesos son los responsables de:

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

- Realizar como actividad de autocontrol el monitoreo establecido al comportamiento de los riesgos de gestión, corrupción y seguridad de la información y la implementación de los controles y acciones, verificando su efectividad, lo cual deberá quedar registrado en la herramienta metodológica, matriz de Excel, denominada “Mapa de riesgos por proceso”.
- Revisar y actualizar al menos una (01) vez en el año, los riesgos de gestión, corrupción y de seguridad de la información en la herramienta definida, teniendo en cuenta los riesgos materializados y los cambios derivados del análisis del contexto con fecha límite el 20 de enero de cada vigencia. Para lo anterior el líder del proceso debe enviar:
  - Oficio justificación de ajuste al mapa de riesgo.
  - Mapa de riesgos modificado en el formato de Excel “Mapa de riesgos por proceso”.

NOTA: Si durante el monitoreo mensual y/o en el seguimiento cuatrimestral realizado a los riesgos de gestión, corrupción y de seguridad de la información, se genera actualización del Mapa de Riesgos, esta deberá reportarse a la oficina de gestión de planeación estratégica mediante comunicación escrita.

- Realizar seguimiento del comportamiento de los riesgos de manera cuatrimestral, dejando registro en acta de reunión del análisis realizado, en conjunto con la oficina de gestión de planeación estratégica dentro de los primeros cinco (05) días hábiles siguientes a las fechas de corte: 30 de abril, 31 de agosto y 31 de diciembre de cada vigencia. Este reporte se debe enviar de manera independiente a las solicitudes de elaboración y/o actualización de riesgos.
- Reportar a los treinta (30) días hábiles de la materialización del riesgo el Plan de Mejoramiento, con su respectiva acta de análisis a la oficina asesora de control interno y la oficina de gestión de planeación estratégica.
- Realizar seguimiento al Plan de Mejoramiento producto de la materialización de los riesgos y enviar a la oficina asesora de control interno y la oficina de gestión de planeación estratégica de manera cuatrimestral durante los cinco (05) días hábiles siguientes a las fechas de corte: 30 de abril, 31 de agosto y 31 de diciembre de cada vigencia.

	<b>POLÍTICA DE ADMINISTRACIÓN DEL RIESGO</b>		
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	17/Ago/2022

La oficina asesora de control interno es responsables de:

- Informar al Comité Institucional de Coordinación de Control Interno de manera consolidada la materialización de riesgos de gestión, corrupción y seguridad de la información reportados por las auditorías internas realizadas de acuerdo al Programa Anual de Auditorías con corte a 30 de junio y 31 de diciembre.
- Realizará el seguimiento a la identificación, calificación, valoración de los riesgos, eficacia de los controles existentes y acciones implementadas para evitar la materialización de los riesgos de corrupción con corte al 30 de abril, 31 de agosto y 31 de diciembre de cada vigencia.

#### 14.RECURSO

La dirección en conjunto con la oficina de gestión de planeación estratégica son responsables de articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión - MIPG y los demás sistemas de gestión que la entidad considere.

Elaborado por: Jennifer López Rodríguez	Cargo: Contratista	Fecha: 08/Jun/2022	Firma:
Revisado por: Carolina Romero Jaramillo	Cargo: Directora	Fecha: 08/Jun/2022	Firma:
Aprobado por: Consejo Directivo IPC	Cargo: No aplica	Fecha: 17/Ago/2022	Firma: