

 Indeportes CAUCA	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 1 de 59

POLÍTICA ADMINISTRACIÓN DEL RIESGO

**MAYO
2024**

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 2 de 59

CONTENIDO

1. INTRODUCCIÓN.....	4
2. OBJETIVOS.....	5
3. NORMATIVIDAD	5
4. ALCANCE	6
5. RESPONSABILIDADES	6
6. TÉRMINOS Y DEFINICIONES	7
7. DESARROLLO	8
7.1. Beneficios de la Gestión de los Riesgos.	9
7.2. Institucionalidad	9
7.3. Metodología para la administración de los riesgos en INDEPORTES CAUCA.	10
7.4. Contexto Estratégico	11
7.5. Paso 1: Política de Administración de Riesgos	14
7.6. Paso 2: Identificación del Riesgo.	15
7.6.1. Análisis de objetivos estratégicos y de los procesos:	15
7.6.2. Identificación de los puntos de riesgo:.....	16
7.6.3. Identificación de áreas de impacto:	16
7.6.4. Identificación de áreas de factores de riesgo:.....	16
7.6.5 Descripción del riesgo:	18
7.7. Paso 3. Valoración del Riesgo.	21
7.7.1. Análisis de riesgos:	22
7.7.2. Determinar la probabilidad:	22
7.7.3 Determinar el impacto:	23
7.7.4. Evaluación de riesgos:	25
7.7.4.1. Análisis preliminar (riesgo inherente):	25
7.4.4.2. Valoración de controles:.....	25
7.4.4.3. Estructura para la descripción del control:.....	25
7.4.4.4. Tipología de controles y los procesos:.....	26
7.4.4.5. Análisis y evaluación de los controles – Atributos:	27
7.4.4.6. Nivel de Riesgo Residual:	28
7.4.4.7. Tratamiento del Riesgo (medidas de respuesta)	29
7.5. Estrategias para combatir el Riesgo:.....	30

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 3 de 59

7.6. Herramientas para la gestión del riesgo:	30
7.6.1. Gestión de eventos:	31
7.6.2. Indicadores claves de Riesgo:.....	31
7.7. Lineamientos para el riesgo fiscal	32
7.7.1. Control fiscal interno y prevención del riesgo fiscal:	32
7.7.2. Definición y elementos el Riesgo Fiscal:	33
7.7.3. Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales:	34
7.7.3.1 Paso 1: Identificación de Riesgos Fiscales:.....	34
7.7.3.2. Paso 2: Valoración el Riesgo Fiscal (Ver Ítem 7.4.4.2 de esta política)	37
7.7.7.3. Paso 3. Valoración de controles.....	39
7.7.7.4. Nivel de riesgo (riesgo residual): (Ver ítem 4.4.4.6 de esta Política).....	40
7.8. Lineamientos sobre los riesgos relacionados con posibles actos de corrupción.....	40
7.8.1. Identificación del riesgo de corrupción	42
7.8.2. Valoración de riesgos de Corrupción.....	42
7.8.3. Análisis de la probabilidad.....	42
7.8.4. Análisis del impacto	43
7.8.5. Análisis del Riesgo Inherente	44
7.8.6. Valoración de controles y tratamiento del riesgo	45
7.8.7. Seguimiento riesgos de corrupción	46
7.8.8. Monitoreo de Riesgos de Corrupción	46
7.8.9. Acciones a seguir en caso de materialización de Riesgos de Corrupción	46
7.9. Lineamientos para la Identificación de Seguridad de la Información	47
7.9.1. Gestión de los riesgos de seguridad digital	47
7.9.2. Identificación de los activos de seguridad de la información.....	47
7.9.3. Como identificar los activos.....	48
7.9.4. Identificación del Riesgo de Seguridad de la Información	49
7.9.5 Valoración del riesgo de seguridad de la información	51
7.9.6. Controles asociados a la seguridad de la información.....	52
8. SEGUIMIENTO Y EVALUACIÓN.....	55
8.1. Monitoreo y revisión:	55
8.2. Líneas de Defensa.....	55
8.3. Acciones a seguir en caso de materialización de riesgos de gestión:.....	58
9. ANEXOS.....	59
10. CONTROL DE CAMBIOS.....	59

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 4 de 59

1. INTRODUCCIÓN

El Instituto Departamental de Deportes del Cauca, INDEPORTES CAUCA, define su política del Administración del Riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión, con el propósito de garantizar la adecuada prestación de sus servicios y el cumplimiento de sus objetivos institucionales, dado esto se han determinado lineamientos relativos a la administración de la gestión del riesgo, teniendo en cuenta el contexto de la Entidad y la Planeación Estratégica.

Este instrumento tiene el propósito de orientar a los servidores públicos de INDEPORTES CAUCA, responsables de los procesos del Modelo de Operación por Procesos, sobre la identificación, análisis y valoración de los riesgos, con el fin de tener un panorama general de las posibles desviaciones que pueden ocurrir y que crean incertidumbre sobre el logro de los objetivos.

Las organizaciones de todos los tipos y tamaños se enfrentan a factores e influencias externas e internas que hacen incierto si lograrán sus objetivos. La gestión del riesgo es iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas.¹

La gestión del riesgo es parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión. La gestión del riesgo es parte de todas las actividades asociadas con la organización e incluye la interacción con las partes interesadas. La gestión del riesgo considera los contextos externo e interno de la organización, incluido el comportamiento humano y los factores culturales

Este documento está formulado con base en el lineamiento Guía para la Administración del Riesgo y el Diseño de Controles en la Entidades Públicas- Riesgos de Gestión, Corrupción, fiscal y Seguridad Digital. Versión 6 – Dirección de Gestión y Desempeño Institucional. Función Pública noviembre de 2022. e involucra lineamientos de estándares nacionales e internacionales en materia de riesgos como son la norma NTC ISO 31000.

¹ Norma ISO 31000

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 5 de 59

2. OBJETIVOS

- **GENERAL**

Garantizar la gestión pública a través del logro de los objetivos y procesos institucionales, instaurando los principios básicos de la gestión del riesgo y el marco general para el control y gestión del riesgos, a través de la identificación, análisis, valoración e implementación de lo establecido en esta política, con el propósito de guiar a los servidores públicos y contratistas de INDEPORTES CAUCA responsables de los procesos, con el fin de tener un panorama general de las posibles desviaciones que pueden ocurrir y que crean incertidumbre sobre el logro de los objetivos de los procesos e institucionales.

- **ESPECIFICO**

- Establecer los parámetros necesarios para una adecuada administración de los riesgos a través de los elementos: contexto estratégico; identificación de riesgos; análisis de riesgos; valoración de riesgos; políticas de administración del riesgo, su trazabilidad, registro y monitoreo.
- Incentivar el pensamiento basado en riesgos dentro del Instituto.
- Realizar seguimientos a los riesgos identificados en los mapas de riesgos

3. NORMATIVIDAD

- Ley 87/1993: Establece normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- Ley 1474/2011: Dicta normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1753/2015: Integra en un Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulados con los Sistemas Nacional e Institucional de Control Interno.
- Ley 2195/2022: Adopta medidas en materia de transparencia, prevención y lucha contra la corrupción.
- Decreto 2145/1999: Dicta normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del Orden Nacional y Territorial.
- Decreto 1499/2017: Modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- ISO 27001/2022: Norma del Sistema de Gestión de la Seguridad de la Información.
- ISO 3100/2018: Norma de Gestión del Riesgo – Directrices
- Guía DAFP/2022: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6 - Noviembre de 2022

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 6 de 59

4. ALCANCE

La política será aplicable a los todos los procesos institucionales, así como a los planes y proyectos del Instituto, de conformidad con cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y las correspondientes a las líneas de defensa.

5. RESPONSABILIDADES

Dado que se plantea articular los niveles de autoridad y responsabilidad en el marco del esquema de líneas de defensa, a fin de facilitar la estructura para los seguimientos y monitoreos en todos los niveles organizacionales, frente a la gestión del riesgo se debe considerar el siguiente marco general para la definición de actividades o acciones propias de cada línea así:²

- **Desde la Línea Estratégica:** (Alta Dirección) se debe definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2ª línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.
- **Desde la 1ª línea de defensa:** Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo).
- **Desde la 2ª línea de defensa:** el Jefe de planeación o quien haga sus veces debe periódicamente hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los líderes de los procesos y sus equipos para la mejora de este tema.
- **Finalmente, para la 3ª línea de defensa:** Que corresponde a la Oficina de Control Interno o quien hace sus veces, a través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede

² Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6 - Noviembre de 2022

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 7 de 59

proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación o quien haga sus veces

6. TÉRMINOS Y DEFINICIONES

A continuación, se relacionan una serie de conceptos, necesarios para la comprensión de la metodología que se desarrolla a partir del paso 1 política de administración del riesgo, hasta el paso 3 valoración del riesgo. De igual forma, se consideran aquellos relacionados con el riesgo fiscal, riesgos de corrupción y de seguridad de la información respectivamente

- **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.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito del Riesgo:** 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.
- **Capacidad de riesgo:** máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Contingencia:** posible evento futuro, condición o eventualidad.
- **Control:** medida que permite reducir o mitigar un riesgo
- **Causa:** factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **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 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 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 fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial, (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 8 de 59

- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:
- **Bien de uso público:** aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.
Ejemplos: Las calles, plazas, puentes, vías, parques etc.
- **Bienes fiscales:** aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.
Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones,
- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Gestión del Riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de Frecuencia o Factibilidad.
- **Impacto:** Se entiende como las consecuencias que pueden ocasionar a la organización la materialización del riesgo.
- **Riesgo Inherente:** Es aquel riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo Residual:** Nivel de riesgo permanente luego de tomar medidas de tratamiento del riesgo.
- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Integridad:** propiedad de exactitud y completitud.
- **Tolerancia al Riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

7. DESARROLLO

La política de administración de riesgos busca el cumplimiento de la misión institucional y del plan estratégico institucional, mediante la formulación de controles efectivos y acciones de

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 9 de 59

mitigación para los riesgos identificados en el Instituto.

7.1. Beneficios de la Gestión de los Riesgos.

- **Alinea el riesgo y la estrategia:** En su evaluación de alternativas estratégicas, la gerencia considera los riesgos priorizados por la Empresa, estableciendo los objetivos correspondientes y desarrollando mecanismos para gestionar las oportunidades o amenazas asociadas.
- **Mejora las decisiones de respuesta a los riesgos:** La metodología de gestión de riesgos institucionales proporciona rigor para identificar las posibles oportunidades o amenazas que hacen parte del que hacer institucional y seleccionar entre las posibles alternativas de respuesta a las amenazas o a las oportunidades, la más viable y efectiva para alcanzar los resultados esperados.
- **Reduce las sorpresas y las pérdidas operativas:** La gestión de los riesgos mejora la capacidad de la Empresa para identificar las amenazas o vulnerabilidades que pueden afectar su gestión y establecer respuestas, reduciendo las sorpresas y las pérdidas asociadas.
- **Identifica y gestiona la diversidad de riesgos para toda la Entidad:** Cada Entidad se enfrenta a riesgos que inciden de manera negativa o positiva en el desempeño de sus procesos y en el logro de los resultados planificados; la gestión de riesgos facilita respuestas eficaces e integradas a los impactos interrelacionados de dichos riesgos.
- **Provee respuestas integradas a múltiples riesgos:** La ejecución de los procesos conllevan riesgos inherentes, para lo cual la gestión de los riesgos favorece la elaboración de soluciones integradas para administrarlos, bajo la premisa de optimizar los recursos disponibles y garantizar la coherencia en las respuestas institucionales, en el momento de abordar las posibles vulnerabilidades o amenazas, así como las oportunidades identificadas.
- **Enfoque preventivo:** la gestión del riesgo permite la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a sus grupos de valor en aspectos fundamentales frente a la generación de valor público.

7.2. Institucionalidad

El modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 10 de 59



Figura: Operatividad Institucionalidad para la Administración del Riesgo

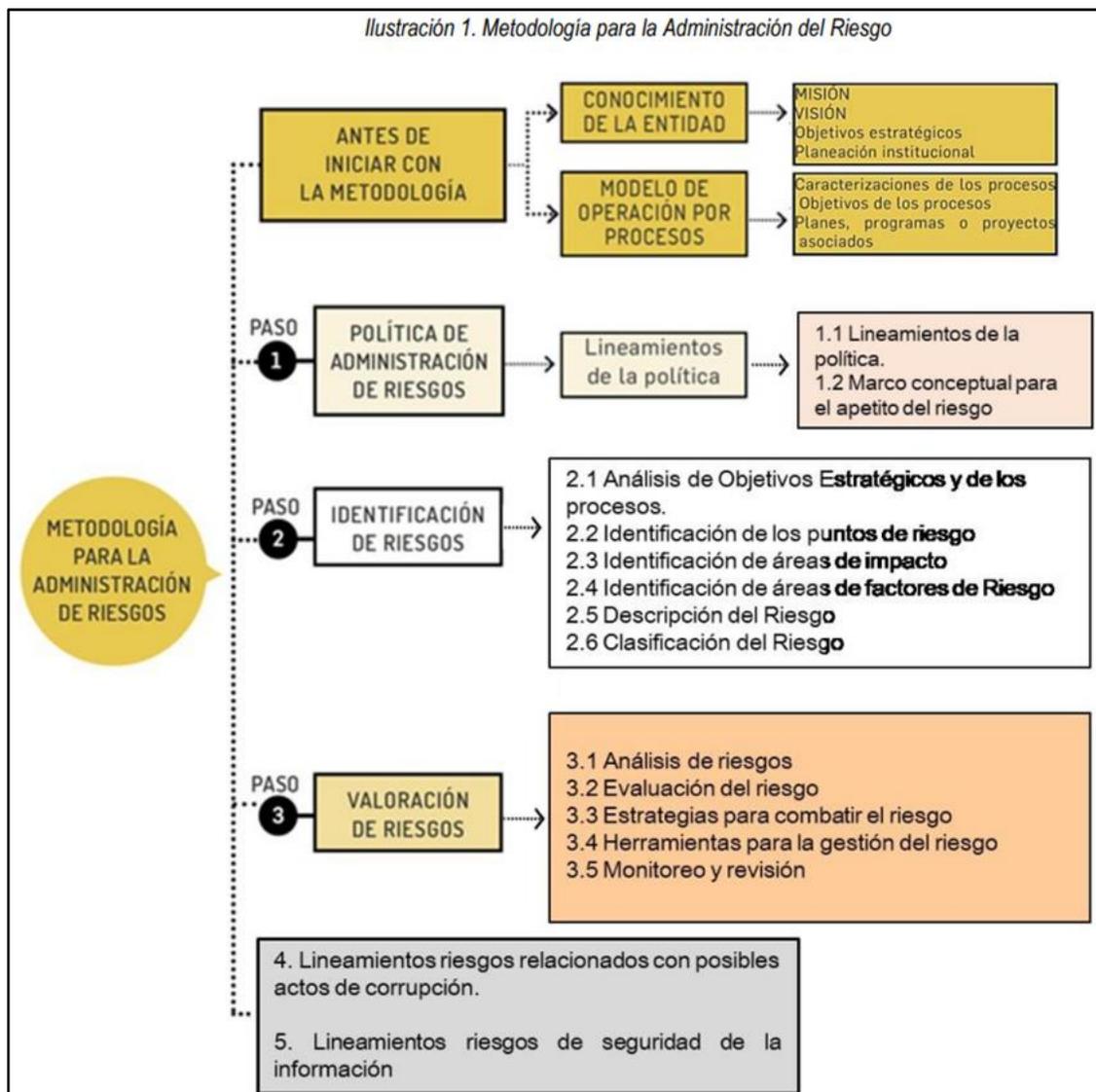
Nota: En entidades de alta complejidad se puede considerar la figura de gestores de riesgos. Se trata de personas clave en las áreas o procesos que ayudan al líder de proceso y a la 2ª línea de defensa en la gestión del riesgo, esta figura es opcional no obligatoria en su implementación.

7.3. Metodología para la administración de los riesgos en INDEPORTES CAUCA.

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada.

A continuación, se puede observar la estructura completa con sus desarrollos básicos:

 Indeportes CAUCA	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 11 de 59



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.4. Contexto Estratégico

El contexto estratégico determina las características o aspectos esenciales del entorno externo e interno en el que se opera en INDEPORTES CAUCA., A partir de este contexto se establece que para cada uno de los procesos del MIPG, de acuerdo a su naturaleza se identifiquen y se analicen de estos factores que puedan afectar el cumplimiento del objetivo del proceso.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 12 de 59

Conocimiento y análisis de la entidad³



Contexto externo

- Económicos y financieros: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
- Políticos: Cambio de Gobierno, legislación, políticas públicas, regulación.
- Sociales: Demografía, responsabilidad social, orden público.
- Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, Gobierno en línea.

³ Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6 - Noviembre de 2022

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 13 de 59

- Ambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
- Legales y reglamentarios: Normativa externa.
- Pandemia: Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

Contexto interno

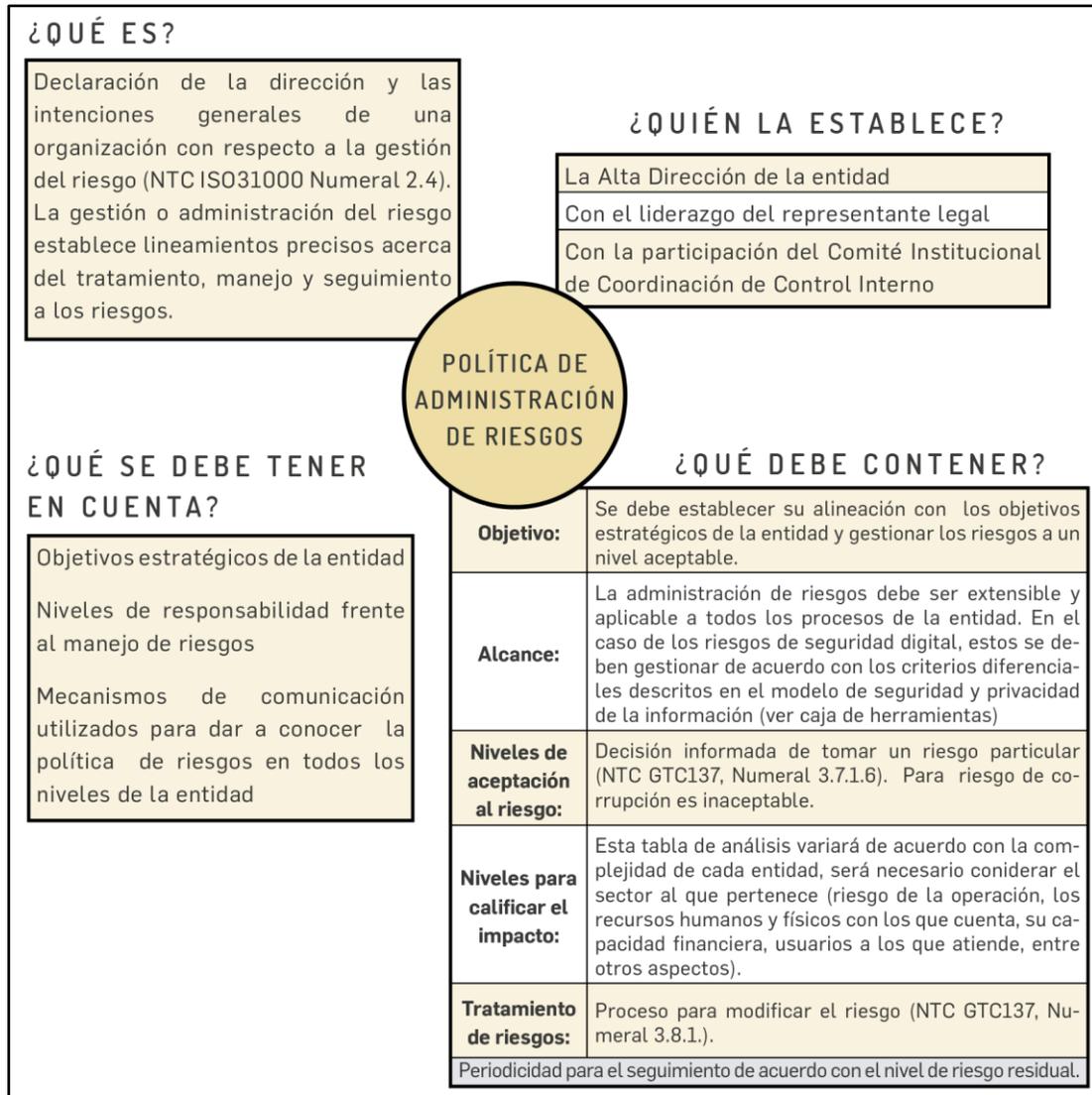
- Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
- Personal: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
- Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
- Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
- Estratégicos: Direccionamiento estratégico, planeación
- institucional, liderazgo, trabajo en equipo.
- Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

Contexto del proceso

- Diseño del Proceso: Claridad en la descripción del alcance y objetivo del proceso.
- Interacciones con otros procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios clientes.
- Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
- Procedimientos Asociados: Pertinencia en los procedimientos que desarrollan los procesos.
- Responsables del Proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- Comunicación entre los procesos: Efectividad en los flujos de información determinados.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 14 de 59

7.5. Paso 1: Política de Administración de Riesgos



El MIPG establece que esta etapa es una tarea propia del equipo directivo y se debe hacer desde el ejercicio de "Direccionamiento Estratégico y de Planeación". En este punto, se deben emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales. Adicional a los riesgos operativos, es importante identificar los riesgos de corrupción, los riesgos de contratación, los riesgos para la defensa jurídica, los riesgos de seguridad digital, entre otros.

La aceptación del riesgo puede ocurrir sin tratamiento de riesgo, los riesgos aceptados están sujetos a monitoreo, tener en cuenta que los riesgos de corrupción son inaceptables.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 15 de 59

7.6. Paso 2: Identificación del Riesgo.

En la identificación se deben establecer las fuentes o puntos de riesgo, los eventos o riesgos, sus causas e impactos. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO31000, Numeral 2.15)

El objetivo es identificar los riesgos que estén o no bajo el control de la organización, para ellos se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de los procesos que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afectan el cumplimiento de los objetivos.

Se aplican las siguientes fases:

7.6.1. Análisis de objetivos estratégicos y de los procesos:

Se deben analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características mínimas: específico, medible, alcanzable, relevante y proyectado.

Los objetivos de proceso deben ser analizados con base en las características mínimas (específico, medible, alcanzable, relevante y proyectado), pero además se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.

Fuente: Comité of Sponsoring Organizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio, p. 73. 2013.

IMPORTANTE

Los objetivos deben incluir el "qué", "cómo", "para qué", "cuándo", "cuánto".

Si no están bien definidos los objetivos, no se puede continuar con la metodología de gestión del riesgo.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 16 de 59

7.6.2. Identificación de los puntos de riesgo:

Existen actividades en las que se tienen evidencia o indicios de que pueden presentarse eventos de riesgo operativo, los cuales deben mantenerse controlados para asegurar que cada uno de los procesos cumpla con su objetivo y se garantice la cadena de valor.



7.6.3. Identificación de áreas de impacto:

Las áreas de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la Entidad en caso de materializarse un riesgo.

Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

7.6.4. Identificación de áreas de factores de riesgo:

Las causas o factores generadores de riesgos a partir de la DOFA tanto internos debilidades, como externos amenazas y del proceso, identificados en el contexto estratégico, con preguntas frente a: ¿Qué puede suceder?, ¿Cómo puede suceder? ¿Cuándo puede suceder?

Los riesgos que pueden afectar el desempeño de los procesos, para lo cual además de tener en cuenta el contexto estratégico, también se podrán identificar a través de lluvia de ideas y de acuerdo con experiencias anteriores en la entidad.

 Indeportes CAUCA	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 17 de 59

Tabla 1 Factores de riesgo

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 18 de 59

IMPORTANTE: Los factores relacionados son una guía, cada entidad puede analizar los que considere de acuerdo con la complejidad propia de cada entidad y con sector en el que se desenvuelve, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo.

7.6.5 Descripción 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:

Figura. Estructura propuesta para la redacción del riesgo



Teniendo en cuenta la anterior estructura se 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:

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

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 19 de 59

Para una mejor interpretación se tiene como ejemplo:

Proceso: Gestión de recursos

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

Alcance: Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquirentes) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:

Riesgo:



Premisas para una adecuada redacción del riesgo

- **No describir como riesgos omisiones ni desviaciones del control.**

Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

- **No describir causas como riesgos**

Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

- **No describir riesgos como la negación de un control.**

Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

- **No existen riesgos transversales, lo que pueden existir son causas transversales.**

Ejemplo: pérdida de expedientes

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 20 de 59

7.6.6. Clasificación del riesgo:

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2020

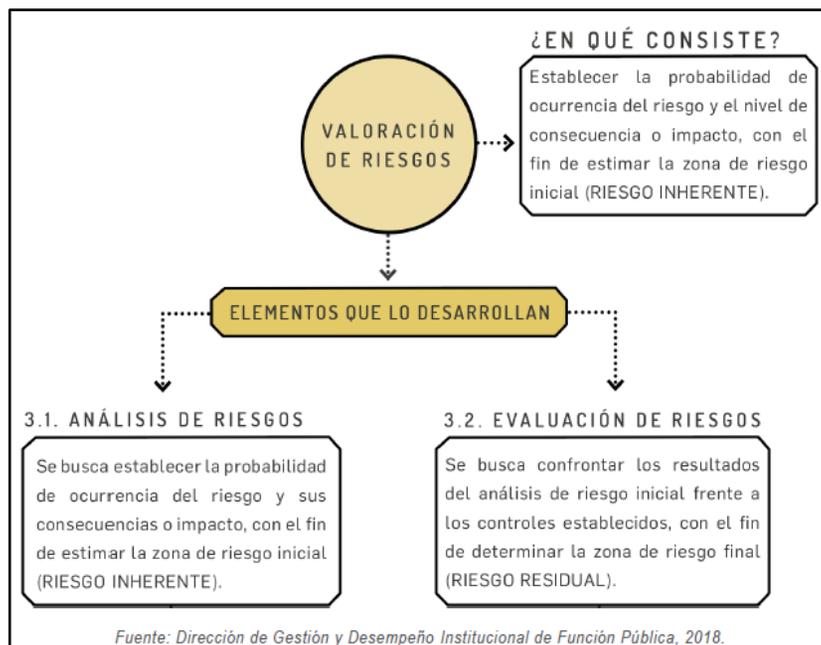
Teniendo en cuenta que en la anterior Tabla se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 21 de 59



7.7. Paso 3. Valoración del Riesgo.

La valoración del riesgo incluye dos etapas que la desarrollan, el análisis de los riesgos y la evaluación de los riesgos.



	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 22 de 59

7.7.1. Análisis de riesgos:

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

7.7.2. Determinar la probabilidad:

Se entiende como la posibilidad de ocurrencia del riesgo.

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.

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

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:

Tabla de 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
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
<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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 23 de 59

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 4 se establecen los criterios para definir el nivel de probabilidad.

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

7.7.3 Determinar el impacto:

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como

Las variables principales. 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.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 24 de 59

Nota: Dependiendo del tamaño y complejidad de los procesos en la entidad, la anterior tabla podrá ser ajustada o adaptada a sus necesidades.

IMPORTANTE: Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

Para mayor claridad, se lista el siguiente ejemplo

Proceso: Gestión de recursos

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.

N.º de veces que se ejecuta la actividad: la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.

Cálculo afectación económica: de llegar a materializarse, tendría una afectación económica de 500 SMLMV.

Aplicando las tablas de probabilidad e impacto tenemos:

Aplicando las tablas de probabilidad e impacto tenemos:

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

La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es media.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

La afectación económica se calcula en 500SMLMV, el impacto del riesgo es mayor.

Probabilidad inherente= media 60%, Impacto inherente: mayor 80%

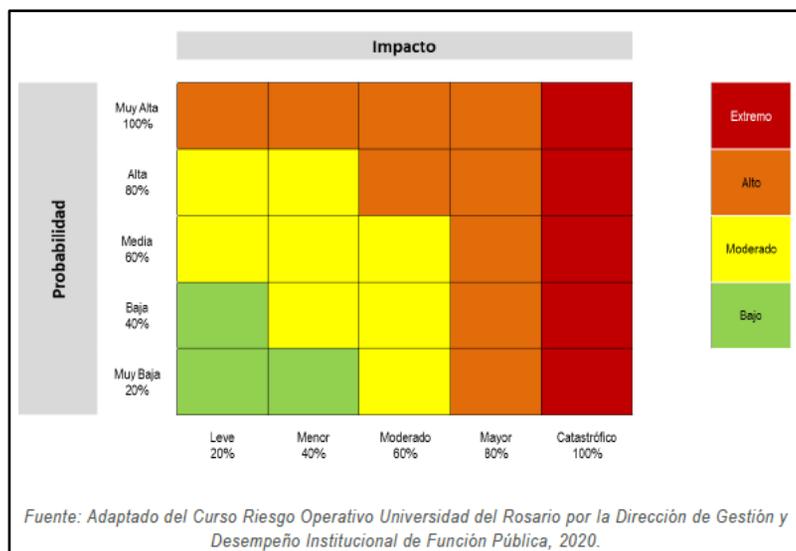
	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 25 de 59

7.7.4. Evaluación de riesgos:

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).

7.7.4.1. Análisis preliminar (riesgo inherente):

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.



7.4.4.2. Valoración de controles:

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

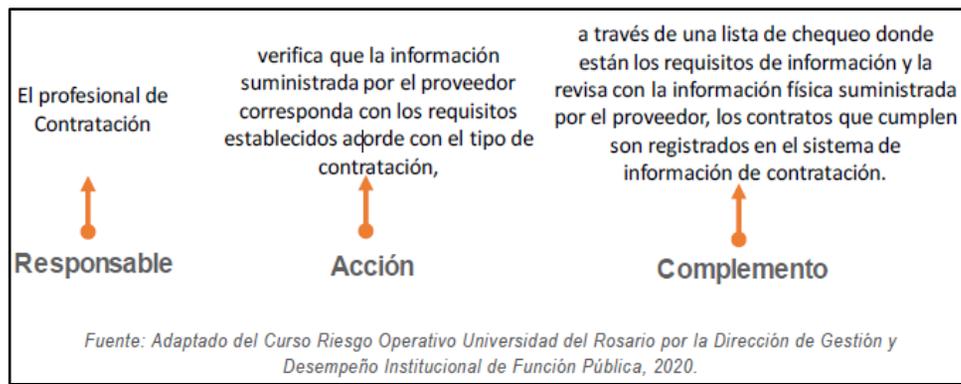
- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo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

7.4.4.3. 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:

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 26 de 59

- 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.



7.4.4.4. Tipología de controles y los procesos:

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión.

Para comprender esta estructura conceptual, se consideran 3 fases globales del ciclo de un proceso así:



	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 27 de 59

Tipologías

Tipo de control	Descripción
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.
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.

7.4.4.5. Análisis y evaluación de los controles – Atributos:

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 6 se puede observar

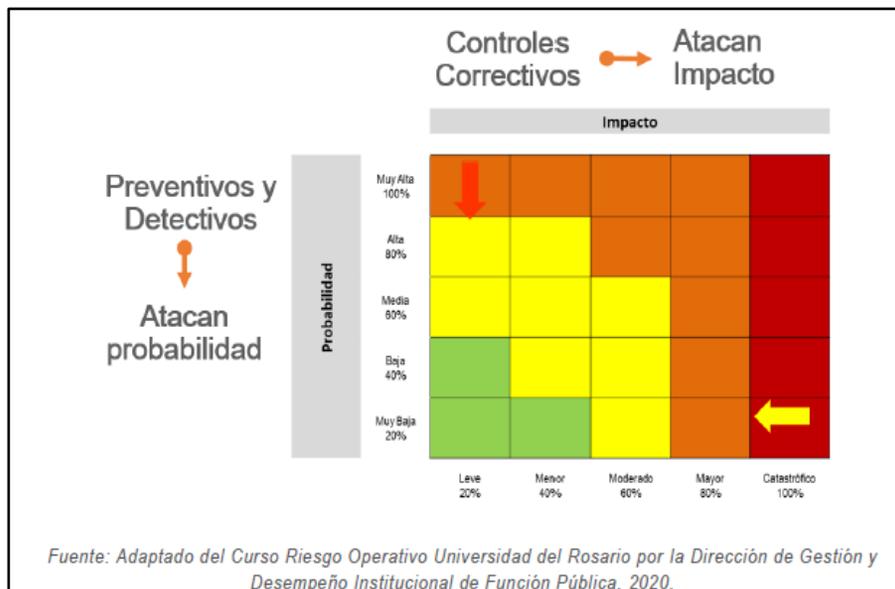
la descripción y peso asociados a cada uno así:

Características		Descripción	Peso	
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos	15%
		Correctivo	Dado que permiten 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, 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.	-

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 28 de 59

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.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde como se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



7.4.4.6. Nivel de Riesgo Residual:

En esta etapa se obtiene el riesgo residual, el cual es el resultado de aplicar la efectividad de los controles al riesgo inherente.

De acuerdo en la Guía para la administración del riesgo y el diseño de controles en Entidades públicas 2020, 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.

En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, por lo tanto, es importante señalar que no será posible su movimiento en la matriz para el impacto

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 29 de 59

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	40%	$60\% * 40\% = 24\%$ $60\% - 24\% = 36\%$
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	$36\% * 30\% = 10,8\%$ $36\% - 10,8\% = 25,2\%$
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.4.4.7. Tratamiento del Riesgo (medidas de respuesta)

La respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos.

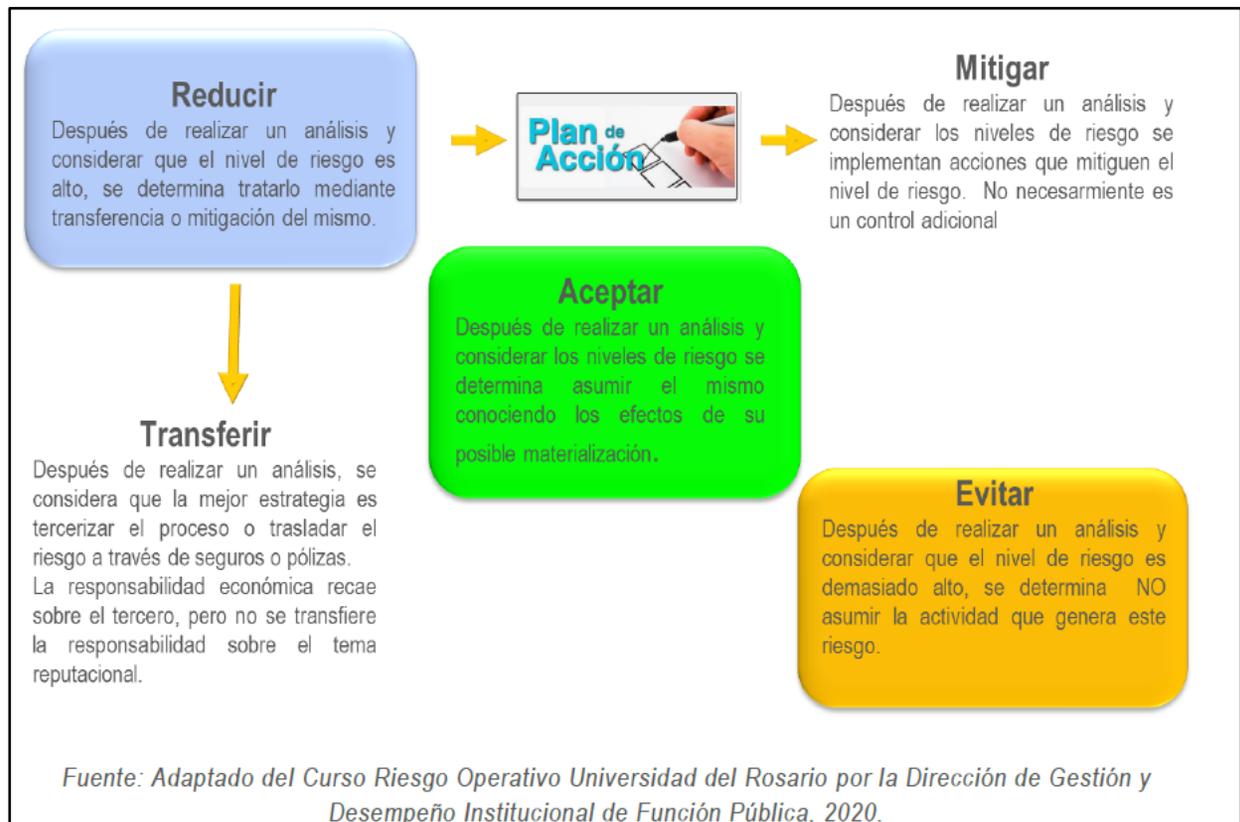
A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la Entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

El tratamiento de los riesgos involucra identificar las opciones para tratar los riesgos residuales priorizados, con el fin de optimizar los recursos disponibles y enfocar los esfuerzos institucionales; INDEPORTES CAUCA, establece como prioridad el tratamiento de los riesgos ubicados en las zonas de riesgo altas y extremas.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 30 de 59

7.5. Estrategias para combatir el Riesgo:

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.



Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

7.6. Herramientas para la gestión del riesgo:

Como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 31 de 59

7.6.1. Gestión de eventos:

Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de ayuda
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia

7.6.2. Indicadores claves de Riesgo:

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 32 de 59

7.7. Lineamientos para el riesgo fiscal

7.7.1. Control fiscal interno y prevención del riesgo fiscal:

Tiene como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

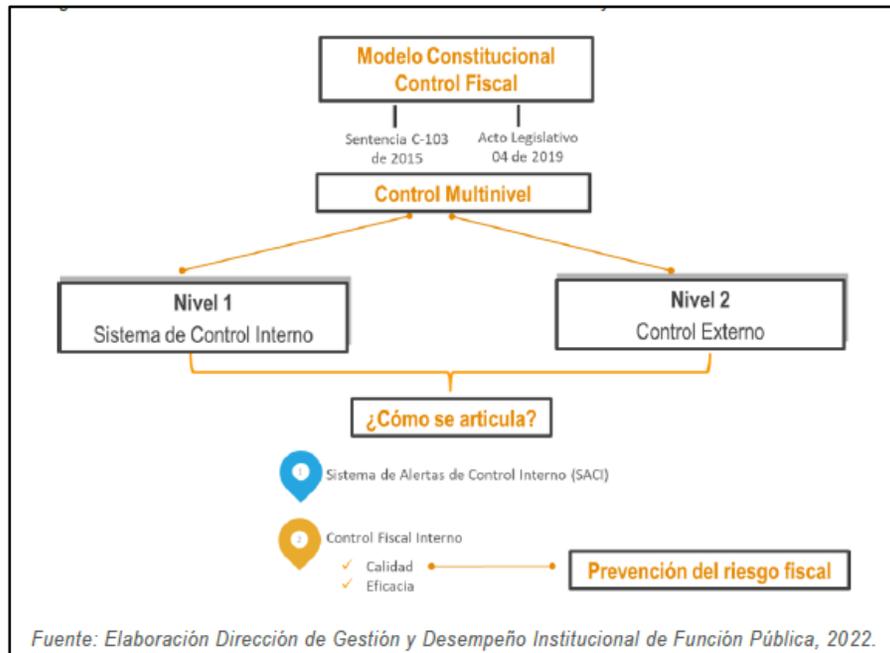
el control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante, buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, con lo cual surgen conceptos clave como:

- **Control fiscal Multinivel:** Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.
- **Control fiscal Interno (CFI):** Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

En el nuevo modelo constitucional el control externo adquiere un enfoque preventivo y a su vez el control interno potencia el enfoque preventivo, partiendo de la premisa de que el Sistema de Control Interno es fundamental para conjugar el logro de resultados, con la prevención de riesgos de gestión, corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros), a través de la prevención de responsabilidades.⁴

⁴ Guía versión 6

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 33 de 59



7.7.2. Definición y elementos el Riesgo Fiscal:

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:

*Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, |a causa de un **evento potencial**.*

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 34 de 59

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso
--

Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

7.7.3. Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales:

A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, que es fundamental para el resultado de la gestión de cada entidad y para la seguridad y prevención de responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación

7.7.3.1 Paso 1: Identificación de Riesgos Fiscales:

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.⁵

En conclusión, los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas

Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica -causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Ahora bien, para poder identificar los puntos de riesgo y las circunstancias inmediatas, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de

⁵ Artículo 3 Ley 610 de 2000.

 Indeportes CAUCA	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 35 de 59

gestión fiscal en las que potencialmente se genera riesgo fiscal) y circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal). Para este taller, puede usar las siguientes preguntas orientadoras:

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
Puntos de riesgo fiscal y circunstancias inmediatas	<p>Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-.</p> <p>Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.</p> <p>Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.</p> <p>Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañinos sobre los recursos, bienes o intereses patrimoniales del Estado.</p> <p>Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.</p>
Circunstancias inmediatas	<p>En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años?</p> <p>Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.</p>
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo1), son aplicables a la entidad?

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

- **Identificación de áreas de impacto**

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 36 de 59

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- (i) Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.
- (ii) Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el capítulo uno de conceptos básicos).

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública (consultar definiciones en el capítulo uno de conceptos básicos).

- **Identificación de la causa raíz o potencial hecho generador**

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal. Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador- causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño -efecto- (Contraloría General de la República, 2021)10.

Para tener más claridad frente a la identificación de los riesgos fiscales, se toma el siguiente ejemplo:

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 37 de 59

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por \$30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

- **¿Cuál es el daño?** El daño fiscal corresponde al monto pagado por concepto de intereses moratorios
- **¿Cuál es el hecho generador?** La omisión de pago oportuno del canon de arrendamiento.
- **Conclusión:** El hecho generador del daño no es el pago de los intereses moratorios, ya que el pago es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

Descripción del riesgo fiscal: (Ver el Ítem 7.6.5 de esta política)

7.7.3.2. Paso 2: Valoración el Riesgo Fiscal (Ver Ítem 7.4.4.2 de esta política)

- **Evaluación de riesgos:** Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.
- **La probabilidad:** Es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.
- **Impacto:** Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos, es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales, sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal

Para mayor claridad, se pone como ejemplo:

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 38 de 59

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad: Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad.

Para este ejemplo es importante tener en cuenta que los bienes muebles en cada entidad varían en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.

Aplicando las tablas de probabilidad e impacto tenemos:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 366 veces al año y máximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al año	100%

La actividad se realiza 365 veces al año, la probabilidad de ocurrencia del riesgo es media.

Para determinar el impacto es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública.

En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que para el ejemplo se determina que es de \$2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV.

De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

La afectación económica se calcula en más de 500SMLMV, el impacto del riesgo es **catastrófico**.

Probabilidad inherente= media 60%, Impacto inherente: catastrófico 100%

Zona de severidad o nivel de riesgo: De acuerdo con la tabla para la definición de zona de severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un nivel de riesgo extremo.

Probabilidad	Impacto				
	Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
Muy Alta 100%	Alto	Alto	Alto	Alto	Extremo
Alta 80%	Medio	Alto	Alto	Alto	Extremo
Media 60%	Bajo	Medio	Alto	Alto	Extremo
Baja 40%	Bajo	Bajo	Medio	Alto	Extremo
Muy Baja 20%	Bajo	Bajo	Bajo	Medio	Alto

Cruzando los datos de probabilidad e impacto definidos se tiene: **zona de riesgo extrema**.

7.7.7.3. Paso 3. Valoración de controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Tipologías de controles:

- Control Preventivo:** Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 40 de 59

Control Detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.

Control Correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos.

7.7.7.4. Nivel de riesgo (riesgo residual): (Ver ítem 4.4.4.6 de esta Política)

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 los 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.

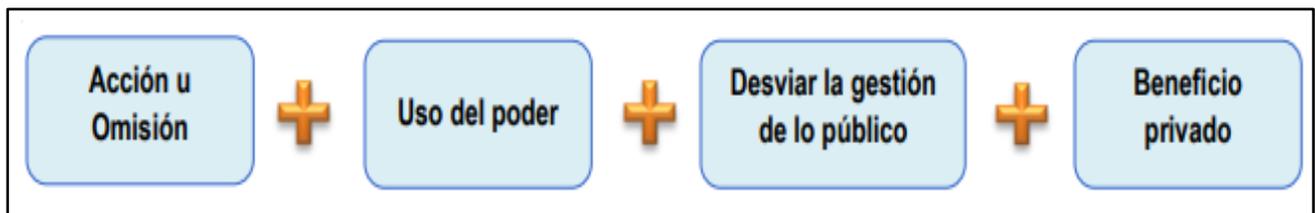
7.8. Lineamientos sobre los riesgos relacionados con posibles actos de corrupción

Para el tratamiento de los riesgos de corrupción es importante tener en cuenta que se continúa con la estructura general definida para la identificación, valoración y tratamiento de los riesgos.

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).

Para identificar un riesgo de corrupción es necesario que en la descripción del riesgo concurren los componentes de su definición, así:



Este tipo de riesgo se establece sobre los procesos y deben estar redactados de manera clara y precisa para evitar ambigüedades o confusiones con la causa generadora identificada.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 41 de 59

Así mismo, el proceso de identificación o revisión se debe llevar a cabo anualmente, por los responsables de los procesos, no obstante, están sujetos a ajustes y modificaciones después de su publicación y durante el respectivo año de vigencia, siempre y cuando esté orientado a mejorar el mapa de riesgos y se asegure el histórico de cambios y trazabilidad.

El monitoreo y evaluación los ejecuta los responsables del proceso con su equipo de trabajo, en concordancia con la cultura del autocontrol y apropiación por parte de todos.

En cuanto al seguimiento, el jefe de la oficina de control interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.⁶

Los riesgos de corrupción se establecen sobre procesos.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.

⁶ Función Pública. Guía para la administración del riesgo y el diseño en entidades públicas. V5, 2020, página 64

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 42 de 59

7.8.1. Identificación del riesgo de corrupción

La Función Pública establece algunos procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales, se podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos y se visualizan en la siguiente tabla:

Direccionamiento estratégico (alta dirección)	<ul style="list-style-type: none"> • Concentración de autoridad o exceso de poder. Extralimitación de funciones. • Ausencia de canales de comunicación. • Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto)	<ul style="list-style-type: none"> • Inclusión de gastos no autorizados. • Inversiones de dineros públicos en Entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. • Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. • Inexistencia de archivos contables. • Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	<ul style="list-style-type: none"> • Estudios previos o de factibilidad deficientes. • Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). • Pliegos de condiciones hechos a la medida de una firma en particular. • Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). • Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. • Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. • Urgencia manifiesta inexistente. • Concentrar las labores de supervisión en poco personal. • Contratar con compañías de papel que no cuentan con experiencia.
De Investigación y Sanción	<ul style="list-style-type: none"> • Inexistencia de canales de denuncia interna o externa. • Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. • Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. • Exceder las facultades legales en los fallos.
De trámites y/o servicios internos y externos	<ul style="list-style-type: none"> • Cobros asociados al trámite. • Influencia de tramitadores. • Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos)	<ul style="list-style-type: none"> • Falta de procedimientos claros para el trámite • Imposibilitar el otorgamiento de una licencia o permiso. • Tráfico de influencias: (amiguismo, persona influyente).

7.8.2. Valoración de riesgos de Corrupción

Cálculo de la probabilidad e impacto

7.8.3. Análisis de la probabilidad

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.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 43 de 59

Criterios para calificar la probabilidad

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 solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

7.8.4. Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo

Para la calificación del impacto de los riesgos de corrupción se debe tener en cuenta que la escala únicamente puede contemplar los niveles de riesgo moderado, mayor, catastrófico, pues tratándose de riesgos de corrupción el impacto siempre será negativo; en este orden de ideas, no aplica la descripción de riesgos menor y leve y no admiten aceptación del riesgo.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 44 de 59

Criterios para calificar el impacto en riesgos de corrupción

N.º	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
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 pregunta(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	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

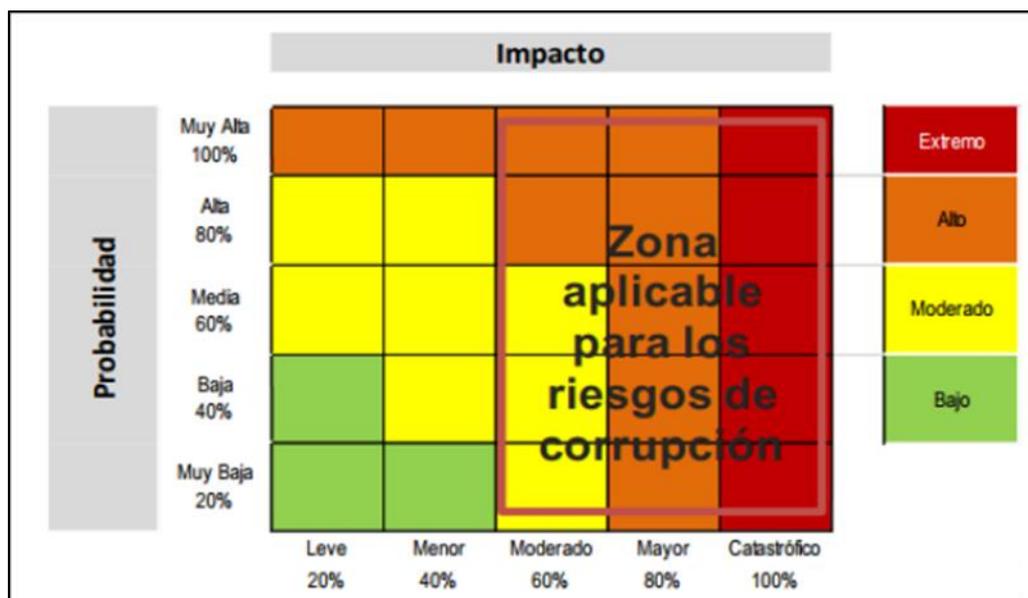
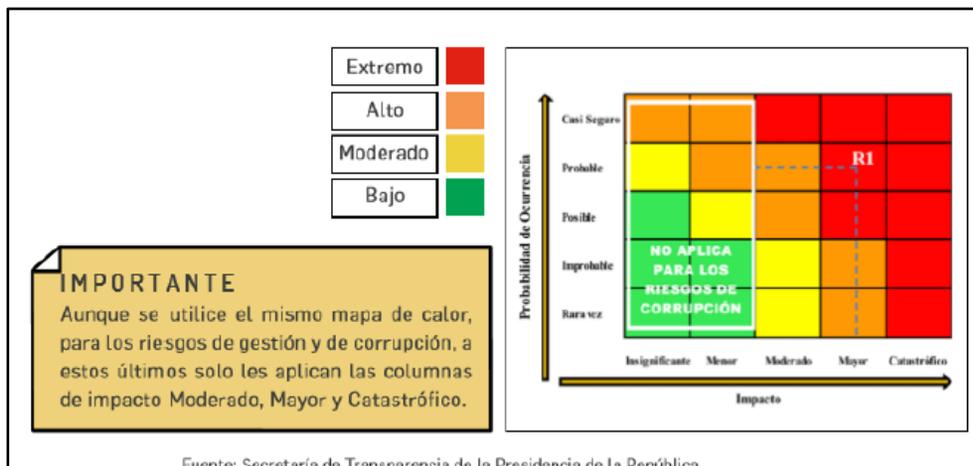
Nivel de impacto MAYOR

7.8.5. Análisis del Riesgo Inherente

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “**moderado**”, “**mayor**” y “**catastrófico**”, dado que estos riesgos siempre serán significativos; en este orden de ideas, **no aplican los niveles de impacto insignificante y menor**, que sí aplican para los demás riesgos.

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

 Indeportes CAUCA	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 45 de 59



7.8.6. Valoración de controles y tratamiento del riesgo

Para realizar la etapa de valoración de controles de los riesgos de corrupción debe aplicarse los lineamientos descritos en el ítem 7.4.2.2 de la presente política con el fin de determinar el riesgo residual sobre el cual se deben determinar las acciones de tratamiento del riesgo.

Así mismo, la formulación de las medidas de respuesta para el tratamiento del riesgo de corrupción residual debe aplicar los lineamientos descritos en el numeral 7.4.3.3 de la presente política.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 46 de 59

7.8.7. Seguimiento riesgos de corrupción

El jefe de la Oficina de Control Interno o, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es responsabilidad de esta instancia el seguimiento a la gestión del riesgo, verificando la efectividad de los controles.⁷

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

7.8.8. Monitoreo de Riesgos de Corrupción

La primera línea de defensa, como los líderes de proceso, en conjunto con su personal de apoyo, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo, la segunda línea de defensa la oficina de planeación Institucional, le corresponde adelantar el monitoreo de acuerdo a los tiempos determinados, llevando a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos.

7.8.9. Acciones a seguir en caso de materialización de Riesgos de Corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes con acciones como:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles
- Verificar que se tomaron las acciones y se actualiza el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén formulados en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles

⁷ Función Pública. Guía para la administración del riesgo y el diseño en entidades públicas. V5, 2020, página 73

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 47 de 59

- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción-
- Determinar si se adelantaron acciones de monitoreo
- Revisar las acciones del monitoreo.

7.9. Lineamientos para la Identificación de Seguridad de la Información

7.9.1. Gestión de los riesgos de seguridad digital

Para el caso de los riesgos sobre seguridad de la información, se debe realizar la incorporación del Anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en Entidades públicas”, de manera tal que los responsables analicen y establezcan, en el marco de sus procesos, los activos de información asociados y se identifiquen los riesgos correspondientes.

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”.

Para el riesgo identificado 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. Le corresponde a la primera línea de defensa identificar los activos en cada proceso.

7.9.2. Identificación de los activos de seguridad de la información

Primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

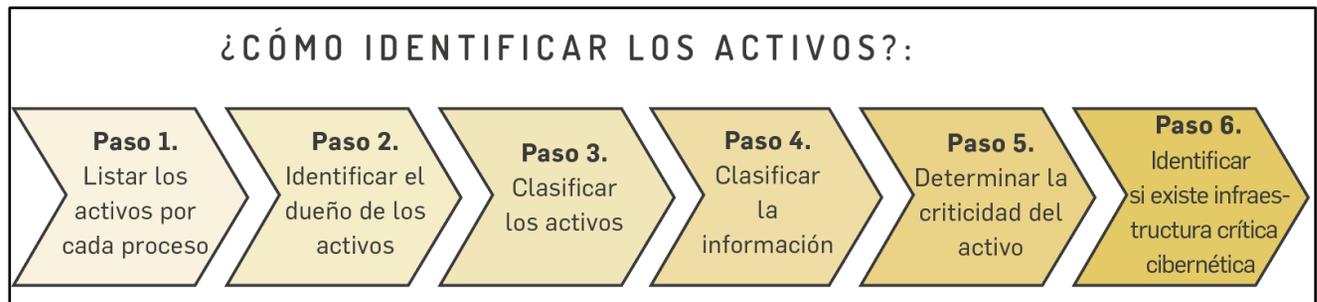
¿Qué son los activos?	¿Por qué identificar los activos?
<p>Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:</p> <p>-Aplicaciones de la organización</p>	<p>Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).</p>

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 48 de 59

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano , aumentando así su confianza en el uso del entorno digital.
Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020	

7.9.3. Como identificar los activos

Algunas amenazas pueden afectar a más de un activo y pueden causar diferentes impactos dependiendo de los activos que se vean afectados.



Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el front office de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 49 de 59

7.9.4. Identificación del Riesgo de Seguridad de la Información

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

1. Pérdida de la confidencialidad
2. Pérdida de la integridad
3. 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.

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.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 50 de 59

IMPORTANTE

- * Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- * Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo “Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas”**, el cual hace parte de la presente guía.
- * **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
- * **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 51 de 59

7.9.5 Valoración del riesgo de seguridad de la información

Para esta etapa se deben aplicar los lineamientos de medición de la probabilidad e impacto definidos en la presente política.

Tener presente:

IMPORTANTE

Cada entidad deberá adaptar los criterios a su realidad.

El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 52 de 59

RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confidencialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Extremo	
Alto	
Moderado	
Bajo	

IMPORTANTE:
La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

7.9.6. Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

 Indeportes CAUCA	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 53 de 59

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la pérdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del <i>software</i> y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

 Indeportes CAUCA	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 54 de 59

Formato mapa riesgos seguridad de la información

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	Pérdida de la integridad	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	Probable	Menor	Moderado	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	EFICACIA: Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 EFFECTIVIDAD: Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

*En este ejemplo el responsable de las actividades de control fue La Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 55 de 59

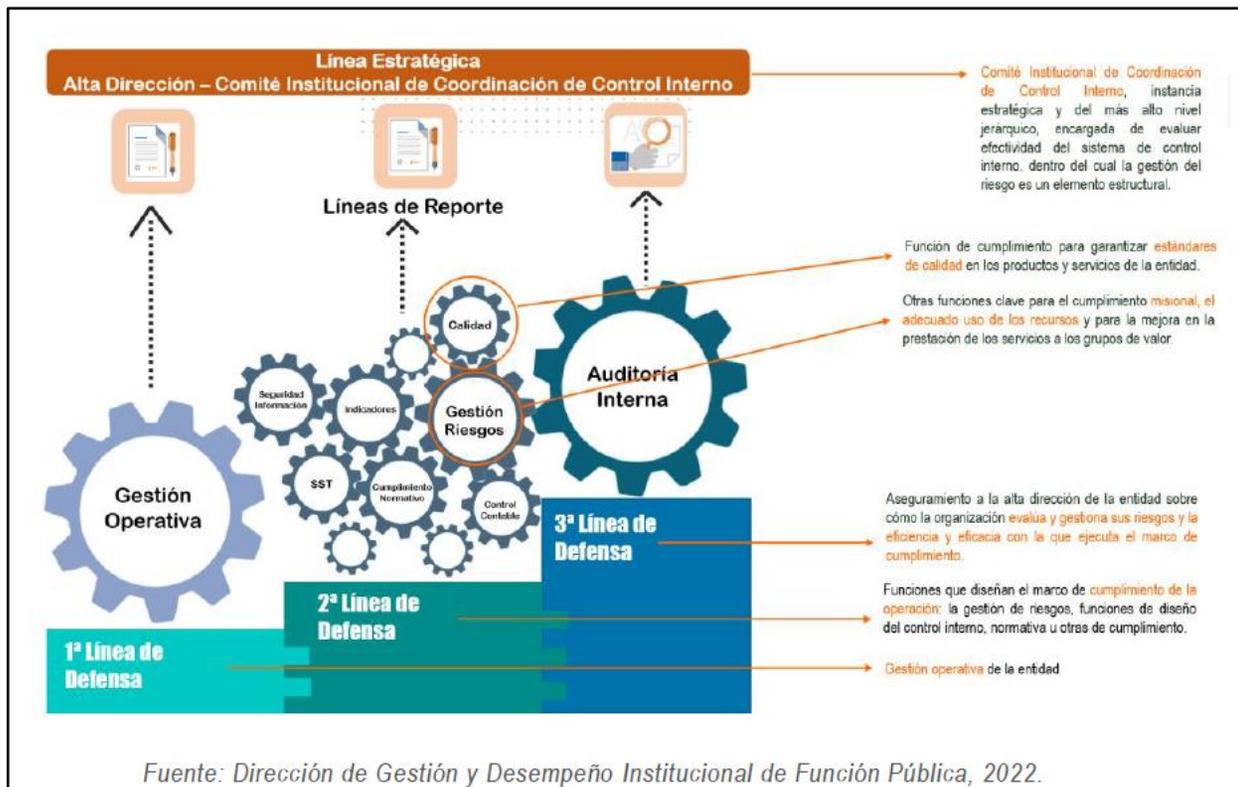
8. SEGUIMIENTO Y EVALUACIÓN

8.1. Monitoreo y revisión:

El modelo integrado de planeación y gestión (MIPG) desarrolla en la dimensión 7 el Modelo Estándar de Control Interno (MECI) y las líneas de defensa como eje articulador para identificar la responsabilidad de la gestión del riesgo y control. que está distribuida en diversos servidores de la entidad.

La estructura del MECI busca una alineación a las buenas prácticas de control referenciadas desde el Modelo COSO, razón por la cual la estructura del MECI se fundamenta en cinco componentes, a saber: (i) ambiente de control, (ii) Evaluación del riesgo, actividades de control, (iv) información y comunicación y (v) actividades de monitoreo.

8.2. Líneas de Defensa



Línea Estratégica: Define el marco general para la gestión del riesgo y el control, supervisa su cumplimiento. Esta línea está a cargo de la Alta Dirección y del Comité Institucional de Coordinación de Control Interno.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 56 de 59

A través de sus Comités deben revisar el cumplimiento de los objetivos mediante una adecuada gestión de riesgos teniendo en cuenta:

1. Revisar los cambios en el “Direccionamiento Estratégico” y como estos pueden generar nuevos riesgos o modificar los que ya tienen identificados.
2. Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de proceso, que han sido la base para llevar a cabo la identificación de los riesgos.
3. Hacer seguimiento en el Comité Institucional de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.
4. Revisar el cumplimiento a los objetivos institucionales, de procesos y sus indicadores e identificar en caso de que no estén cumpliendo los posibles riesgos que se estén materializando en el cumplimiento de los objetivos.
5. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

1° Línea de Defensa: Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Esta línea está a cargo de los líderes de los procesos, programas y proyectos de la Entidad, donde su principal rol es el de diseñar, implementar y monitorear los controles, además de gestionar día a día los riesgos.

Los líderes de Proceso: Deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos incluyendo los riesgos de corrupción:

1. Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos pueden generar nuevos riesgos o modificar los que se tienen identificados en cada uno de sus procesos.
2. Revisión como parte de sus procedimientos de supervisión, la revisión de su adecuado diseño y ejecución de los controles establecidos para la mitigación del riesgo.
3. Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
4. Revisar el cumplimiento de sus objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se estén materializando en el cumplimiento de los objetivos.
5. Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la Entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a la materialización de los mismos.
6. Revisar los planes de acción establecido para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento de los objetivos.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 57 de 59

7. Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

2° Línea de Defensa: Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen eficientemente.

Esta línea de defensa está a cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefe de Oficina de Planeación, Supervisores e Interventores de contratos o proyectos, coordinadores de sistemas de gestión.

1. Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que se tienen identificados en cada uno de sus procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
2. Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos y realizar las recomendaciones a que haya lugar.
3. Revisar el adecuado diseño de los controles para la mitigación de riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
4. Revisar el perfil del riesgo inherente y residual para cada proceso y consolidarlo y pronunciarse sobre cualquier riesgo que este fuera del perfil de riesgo de la entidad.
5. Hacer seguimiento a que las actividades de control establecidas para mitigar el riesgo de los procesos se encuentren documentadas y actualizadas en los procedimientos.
6. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

3° Línea de Defensa: Proporciona información sobre la efectividad del Sistema de Control Interno a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

Esta línea de defensa está a cargo de la Oficina de Control Interno, auditoría interna o quien haga sus veces buscando proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno.

1. Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que se tienen identificados en cada uno de sus procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 58 de 59

2. Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos y realizar las recomendaciones a que haya lugar.
3. Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
4. Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgos de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
5. Revisión de los planes de mejoramiento como resultado de las auditorias efectuadas, que se lleven a cabo de manera oportuna, se establezca la causa raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

8.3. Acciones a seguir en caso de materialización de riesgos de gestión:

En el evento de materialización de un riesgo, las líneas de defensa deberán emprender acciones en el marco de sus responsabilidades, así:

1° Línea de Defensa:

1. Informar a la segunda línea de defensa sobre la materialización detectada, remitiendo el respectivo plan de restablecimiento que incluya la ejecución de la corrección que permitió restablecer la situación y las acciones a adelantar para la actualización del mapa de riesgos.
2. Implementar el plan de acción para el tratamiento de riesgo definido.

2° línea de defensa:

1. Consolidar y comunicar a la tercera línea de defensa sobre las materializaciones informadas por los líderes de proceso.
2. Verificar el cumplimiento de los planes de restablecimiento definidos.
3. Orientar a los líderes de proceso en la actualización del mapa de riesgos.
4. En articulación con la tercera línea de defensa, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados.

3° línea de defensa:

1. En el marco de un ejercicio de evaluación independiente o seguimiento, la Oficina de Control Interno identifique la materialización de un riesgo, deberá informar a los líderes de proceso sobre el hecho detectado, los cuales emprenderán las acciones descritas para la

	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO		 Gobernación del Cauca
	PLANEACIÓN INSTITUCIONAL		
FECHA: 2024/05/10	CÓDIGO: DE-PL- PP- 002	VERSIÓN: 02	PÁGINA: 59 de 59

primera línea de defensa en este numeral.

2. Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso para revisar el mapa de riesgos.
3. En articulación con la segunda línea de defensa, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados.

El seguimiento al documento tiene como propósito monitorear permanentemente el avance o cumplimiento de los entregables y productos propuestos, de acuerdo con las fechas establecidas

9. ANEXOS

Mapas de Riegos de los procesos.

10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
01	2021/06/22	Elaboración de la Política de Operación de Riesgos
02	2024/03/18	Actualización del contenido de la política, nombre del documento, teniendo en cuenta la guía versión 6 del 2022,

ELABORÓ		REVISÓ		APROBO	
Wilder F Patiño M. Contratista de Planeación Institucional		Mónica Mera Jefe de Planeación Institucional Giovany Beltrán Jefe de Oficina de Control Interno		Acta No 3 Comité de Gestión y Desempeño Resolución 118 del 27 junio 2024	
Fecha	2024/05/10	Fecha	2024/05/10	Fecha	2024/05/10