SISTEMA INTEGRADO DE GESTIÓN

RENTAN EICE

PROCESO

EVALUACIÓN INDEPENDIENTE

PROCEDIMIENTO

GESTIÓN DEL RIESGO

POLÍTICA INTEGRAL DE ADMINISTRACIÓN DEL RIESGO

DICIEMBRE 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La gestión de riesgo, es una herramienta clave para que las entidades públicas puedan alcanzar los objetivos en forma eficiente y transparente, disponer de procesos claros y efectivos que identifiquen, prevengan y mitiguen riesgos. Esta, no solo fortalece la confianza ciudadana, sino que también impulsa una cultura de mejora continua y buen gobierno, más aún, en un contexto donde la administración de los recursos públicos enfrenta grandes retos.

En el marco del Modelo Integrado de Planeación y Gestión MIPG decreo 1499 de 2017, guía que no solo presenta herramientas técnicas, sino que también promueve la construcción de una cultura organizacional basada en el autocontrol, la transparencia y la rendición de cuentas, somos conscientes que gestionar riesgos no es tarea de unos pocos, sino un compromiso que involucra a todos los servidores públicos, independientemente de su rol dentro de la entidad.

La Alta Dirección de las organizaciones debe asegurar que la gestión del riesgo se vincule a todas las actividades de la operación, para lo cual debe definir una política que establezca las líneas de acción o enfoque para la gestión del riesgo que incluya, la adopción de un marco de referencia, la disposición de recursos necesarios y la asignación de responsabilidades en los niveles adecuados, atendiendo la autoridad y responsabilidad, con el fin de hacer seguimiento y monitoreo integral a los riesgos.

La estructuración del presente documento para **RENTING DE ANTIOQUIA, RENTAN EICE,** está basada en la guía para la administración del riesgo versión 7, emitida por el Departamento Administrativo de la Función Pública, esta versión, actualiza el enfoque para unificar la gestión de diferentes tipos de riesgos y se alinea con el Modelo Integrado de Planeación y Gestión.

Los pasos clave son la identificación, análisis inherente, diseño de controles y valoración del riesgo vigente y se establece para asegurar el cumplimiento de la misión institucional y los objetivos estratégicos y de proceso.

La Implementación y cumplimiento de la presente Política, contribuye a que la entidad consolide su Sistema de Control Interno y genere una cultura de Autocontrol y autoevaluación al interior de esta.

2. DECLARACIÓN DE LA POLÍTICA INTEGRAL DE ADMINISTRACIÓN DEL RIESGO

La Alta Dirección y el equipo de trabajo de RENTING DE ANTIOQUIA RENTAN EICE, están comprometidos con la gestión integral de los riesgos, mediante la adopción de diferentes lineamientos, como es la identificación, valoración, tratamiento, monitoreo y seguimiento, comunicación, consulta, y consideración de riesgos emergentes con el fin de prevenir su materialización y la adopción de controles efectivos

3. OBJETIVOS

3.1 Objetivo Principal

Disminuir la vulnerabilidad de la entidad, frente a situaciones que puedan interferir en el cumplimiento de los objetivos, mediante la formulación de controles efectivos y acciones de mitigación para los riesgos identificados en la entidad, contribuyendo a la creación y protección de valor público, así como al fortalecimiento del control interno institucional.

3.2 Objetivos Especificos

- Diseñar e implementar un conjunto de controles para prevenir y mitigar los riesgos identificados, con un enfoque de mejora continua, garantizando la protección de los recursos públicos y el fortalecimiento de la cultura de control interno en la entidad.
- Promover una cultura organizacional de gestión de riesgos en RENTAN EICE , a través de la capacitación continua del personal y la sensibilización sobre la importancia del control interno, con el fin de fortalecer la capacidad institucional para cumplir con los compromisos de gobierno y los fines estratégicos de la entidad

4. ALCANCE

Da cobertura a todos los procesos, programas y proyectos. De acuerdo a la naturaleza y misionalidad de cada entidad, será necesario analizar dentro del alcance unidades desconcentradas o temas tercerizados, operados por privados u otras entidades públicas a través de convenios, con el fin de establecer acciones de

seguimiento, dado que estas organizaciones que son externas a la entidad pueden generar riesgos críticos que deben considerarse para su control.

Aplica para todos los procesos, programas y proyectos, servidores públicos, trabajadores oficiales y contratistas de prestación de en todas las áreas, programas y proyectos institucionales de **RENTAN EICE**.

Inicia desde las directrices que se toman desde la línea estratégica y termina con el seguimiento, control y reporte de la tercera línea de defensa.

5. DEFINICIÓN DEL CONTEXTO ESTRATÉGICO

Con el fin de identificar los factores externos e internos del riesgo, que inciden en el desempeño de los procesos y en el logro de las metas y objetivos establecidos en la planeación estratégica, se debe identificar el contexto externo, interno y del proceso.

CONTEXTO EXTERNO	CONTEXTO INTERNO	CONTEXTO DE PROCESO
Determina las características o aspectos esenciales del entorno en el cual opera la entidad, retoma los siguientes factores:	Determina las características del ambiente en el cual la organización busca alcanzar sus objetivos, se analizan aspectos como:	Lo relacionado con la gestión implementación y desarrollo del proceso
Económicos: Disponibilidad de recursos financieros, liquidez, mercados financieros, desempleo, competencia	**Financieros**: Presupuesto funcionamiento, recursos de inversión, infraestructura, capacidad instalada.	Diseño del proceso: Claridad en la descripción del alcance y objeto del proceso
Político: cambios de gobierno, legislación, políticas públicas, regulación	**Personal**: Competencia y disponibilidad de personal, seguridad y salud laboral	Interrelación con otros procesos: Claridad en la descripción del alcance y objetivo del Proceso
Medioambientales: Condiciones ambientales, residuos, energía, agua, catástrofes naturales, desarrollo sostenible	**Procesos**: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento, interacción, transversalidad, responsables, lineamientos internos definidos, registros.	Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad

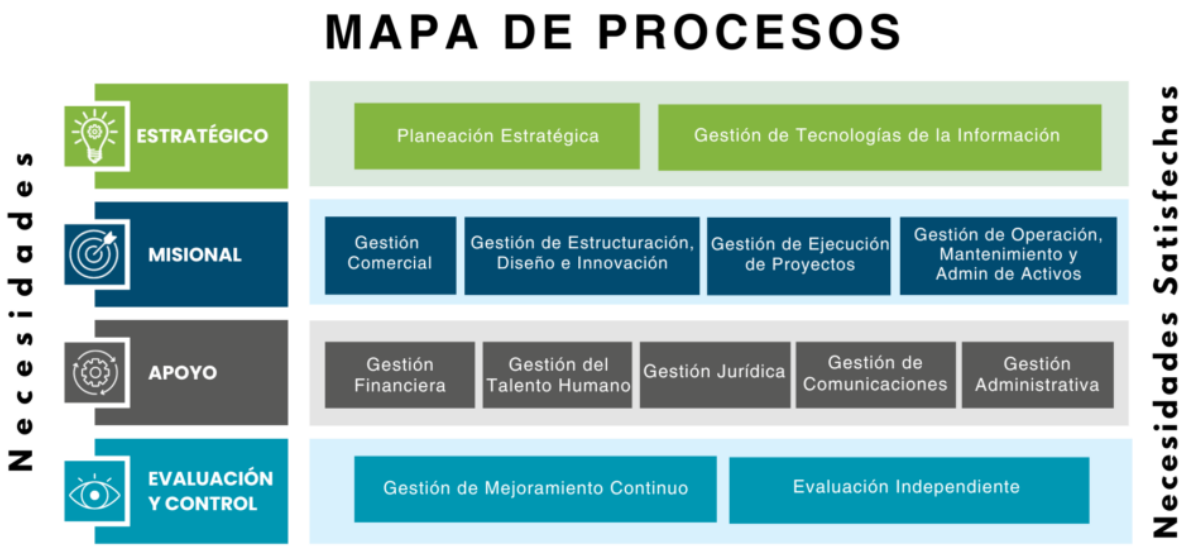
CONTEXTO EXTERNO	CONTEXTO INTERNO	CONTEXTO DE PROCESO
Seguridad y Salud en el Trabajo: Condiciones de Seguridad y salud en el trabajo externas, emergencias, eventos catastróficos, residuos peligrosos.	**Seguridad y Salud en el Trabajo**: Condiciones de Salud, condiciones de trabajo, presupuesto, recursos, infraestructura, comunicación, responsabilidades.	Procedimientos asociados: pertinencia en los procedimientos que desarrolla el proceso
Sociales y Culturales: Demografía, responsabilidad social, orden público	**Estructura organizacional**: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo	Responsables del proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso
Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, interrupciones, tecnología emergente, gobierno en línea.	**Tecnología**: avances tecnología, acceso al sistema de información externo, gobierno en línea.	Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos
Comunicación Externa: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad	**Comunicación Interna**: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	Cumplimiento del plan de comunicaciones y publicación en página web.

6. VALORES Y PRINCIPIOS

7. PRINCIPIOS RECTORES

- **Proactividad**: En RENTAN EICE; se priorizará la prevención y detección temprana de riesgos.
- **Responsabilidad Compartida**: La administración de riesgos es una tarea compartida en toda la entidad, bajo el esquema de las tres líneas de defensa.
- **Mejora Continua**: Implementación de controles y acciones correctivas adaptadas al contexto y evolución de los riesgos

8. PROCESOS DE LA ENTIDAD



9. RESPONSABILIDADES Y ROLES

Niveles de Responsabilidad frente a la Gestión del Riesgo y de acuerdo a las líneas de Defensa

Línea de Defensa	Responsable	Responsabilidad frente al Monitoreo del Riesgo
Línea Estratégica 	Alta Dirección y Comité Institucional de Gestión y Desempeño	Aprobar la política integral de administración del riesgo previamente estructurada por parte de la Oficina Asesora de Planeación, como segunda línea de defensa en la entidad. Generar recomendaciones de mejora a la política integral de administración del riesgo para su análisis y actualización. Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento del Plan Estratégico Institucional, para la toma de decisiones.
Primera Línea de Defensa 	Líderes de proceso en todos los niveles	Conocer y apropiar la política integral de administración de riesgos y el procedimiento Gestión Integral del Riesgo", con el propósito de tomar acciones para el autocontrol en sus procesos y promoverlo al interior de su equipo de trabajo. Identificar, valorar, evaluar, actualizar los riesgos, establecer los controles y garantizar su implementación, para evitar su materialización. Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. En caso de la materialización de un riesgo realizar su comunicación y respectivo tratamiento Solicitar a la Oficina Asesora de Planeación la eliminación de un riesgo con la debida justificación, para evaluar su pertinencia. Comunicar a la Oficina Asesora de Planeación la necesidad de la actualización de un riesgo, para realizar su debido acompañamiento.

Línea de Defensa	Responsable	Responsabilidad frente al Monitoreo del Riesgo
		Participar en el diseño de los controles que tienen a cargo. Ejecutar los controles a su cargo de la forma como están diseñados. Proponer mejoras a los controles existentes
Segunda Línea de Defensa 	Dirección de Planeación	Estructurar la política integral de administración de riesgos. Consolidad el Mapa de riesgos institucional con enfoque en los riesgos de mayor criticidad y establecer la periodicidad de análisis y seguimiento. Informar a Control Interno sobre las actualizaciones de riesgos o la eliminación justificada de riesgos. Acompañar, orientar y entrenar a los Líderes de Procesos y sus equipos en la identificación, análisis, valoración y evaluación del riesgo. Asesorar el adecuado diseño de los controles de acuerdo con lo indicado en la guía del DAFP. Evaluar la implementación del cumplimiento de la política integral de administración de riesgos y presentar la respectiva información consolidada.
Tercera Línea de Defensa 	Proceso: Evaluación independiente -Jefe de Control interno	Asesorar y orientar técnicamente y realizar recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación, para garantizar el cumplimento efectivo de los objetivos. Monitorear la exposición de la entidad al riesgo y realizar recomendaciones con alcance preventivo. Informar los hallazgos en materias de riesgos y proporcionar recomendaciones en el ejercicio de la auditoría independiente. Hacer seguimiento a las acciones complementarias que apoyan el tratamiento de los riesgos.

Línea de Defensa	Responsable	Responsabilidad frente al Monitoreo del Riesgo
		Realizar evaluación independiente de la gestión de los riesgos. Evaluar fallas en los controles (diseño y ejecución) para definir las acciones apropiados para su mejora. Identificar y alertar al Comité Institucional de Coordinación de Control Interno de posibles cambios que pueden afectar la evaluación y el tratamiento del riesgo. Alertar sobre la probabilidad de riesgo de gestión, riesgos de posibles actos de corrupción, riesgos de seguridad de la información, riesgos de integridad y riesgos fiscales.

9.1 Liderazgo y Compromiso

ISO31000:2018, en el numeral 5.2	Modelo Integrado de Planeación y Gestión MIPG, Dimensión de Direccionamiento Estratégico y Planeación
La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización y deberían demostrar el liderazgo y compromiso. adaptando e implementando todos los componentes del marco de referencia; publicando una declaración o una política que establezca un enfoque, un plan o una línea de acción para la gestión del riesgo: asegurando que los recursos necesarios se asignan para gestionar los riesgos;	Esta 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 (…)" (Función Pública, Manual Operativo MIPG v6, 2024, p.36)

asignando autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la organización	

10. PROCEDIMIENTOS Y DIRECTRICES

Alineación Estratégica con el Modelo Integrado de Planeación y Gestión (MIPG)

La gestión del riesgo se presenta como un pilar fundamental para el buen gobierno y el control institucional, y debe integrarse en todas las actividades de las entidades. El MIPG, un marco de referencia para la dirección y el control de organismos públicos, articula la gestión de riesgos a través de sus siete dimensiones. La guía destaca al menos diez políticas del MIPG que tienen una relación directa con la administración de riesgos, incluyendo:

- **Planeación institucional**: La gestión del riesgo contribuye a definir objetivos y estrategias para el logro de la misión, considerando los factores del entorno.
- **Gestión presupuestal y eficiencia del gasto público**: La gestión de riesgos Fiscales es clave para asegurar un uso apropiado, eficiente y transparente de los recursos.
- **Fortalecimiento organizacional y simplificación de procesos: La** identificación de riesgos se vincula directamente a la definición de procesos, procedimientos y controles para cumplir con los objetivos.
- **Seguridad digital**: Requiere asegurar la integridad, disponibilidad y confidencialidad de la información.
- **Transparencia y lucha contra la corrupción**: El Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) se alinea con los Programas de Transparencia y Ética Pública (PTEP).

11. BENEFICIOS DE LA GESTION DEL RIESGO

- **Alinea el riesgo y la estrategia:** En su evaluación de alternativas estratégicas, la dirección considera los riesgos priorizados por la entidad, estableciendo los

objetivos correspondientes y desarrollando mecanismos para gestionar las oportunidades o amenazas asociadas.

- **Mejora las decisiones de respuesta a los riesgos:** La 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 mejorar la capacidad de la Entidad 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
- **Permite aprovechar las oportunidades:** mediante la consideración de una amplia gama de potenciales eventos, la Entidad está en posición de identificar y aprovechar las oportunidades de modo proactivo, a fin de potencializar los efectos deseables.

12. GESTIÓN DEL RIESGO GUÍA 7 FUNCIÓN PÚBLICA

12.1 Diagnostico de la Madurez del Riesgo

Para fortalecer una cultura organizacional consciente del riesgo, inicialmente se parte de la evaluación del nivel de madurez de la gestión del riesgo, basada en los cinco componentes del marco COSO-ERM:

- Gobierno y Cultura
- Establecimiento de la Estrategia y Objetivos,
- Desempeño, Revisión y Monitorización, e
- Información, Comunicación
- Reporte.

Estos cinco (5) componentes hacen parte del **INSTRUMENTO DE AUTODIAGNÓSTICO PARA DETERMINAR EL NIVEL DE MADUREZ DE LA GESTIÓN INTEGRAL DEL RIESGO**, emitido por funcion publica, el cual se diligencia para conocer el puntaje de la madurez del riesgo en el proceso en una escala de 1-5 que se muestra a continuacion en cada nivel.

12.2 Tipos de Riesgos

Riesgos de Gestión: Incluyen los tradicionales (estratégicos, operativos, financieros, de talento humano, administrativos), buscando la integralidad en su manejo.

Riesgo Fiscal: Afecta los recursos públicos y patrimonios de la entidad

Riesgo de Seguridad de la Información: Protege activos de información, incluyendo seguridad digital y ciberseguridad.

Riesgo de corrupción: La P**osibilidad** de usar el poder público para beneficio privado (soborno, malversación)

Riesgo de integridad pública: La posibilidad de que se transgredan los principios, deberes y normas éticas de la función pública por acción u omisión, afectando la ética y la confianza en el Estado.

12.3 Metodología para Riesgos Generales de la Gestión

Los riesgos generales de la Gestion son aqueloos riesgos asociados a la operación de la entidad, que en el lenguaje de marcos de referencia internacional podrían llamarse operativos, al ser propios o intrínsecos a las procesos, funciones y misionalidad de cada entidad.

A continuación, se describe una metodología aplicable a todos los tipos de riesgos:

a) **Identificación y Descripción del Riesgo**: Se inicia con el evento no deseado y sus consecuencias (Impacto) y se profundiza en la **causa inmediata** y la **causa raíz**. Un riesgo debe describirse en términos de qué podría pasar, por qué puede pasar y qué condición aumenta su probabilidad.

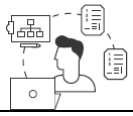
b) **Identificación de áreas de impacto:** El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

c) **Identificación de áreas de factores de riesgo:**Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

Factores del Riesgo desde diferentes perspectivas

Factor	Definición	Grafico	Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en		Falta de aplicación de los procedimientos
			Falta segregación de funciones

Factor	Definición	Grafico	Descriptores
	las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional		Errores de grabación, autorización
			Falta de supervisión o interventoría
			Errores en cálculos para pagos internos y externos
			Alta rotación o insuficiencia de personal
			Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
			Acciones contrarias a las leyes o acuerdos contractuales
			Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.		Contrapartes de la entidad (naturales o jurídicas)
			Productos (bienes o servicios) que oferta/requiere
			Canales utilizados para la operación
			Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.		Fraude Interno
			Soborno
			Gestión inadecuada de conflicto de Intereses

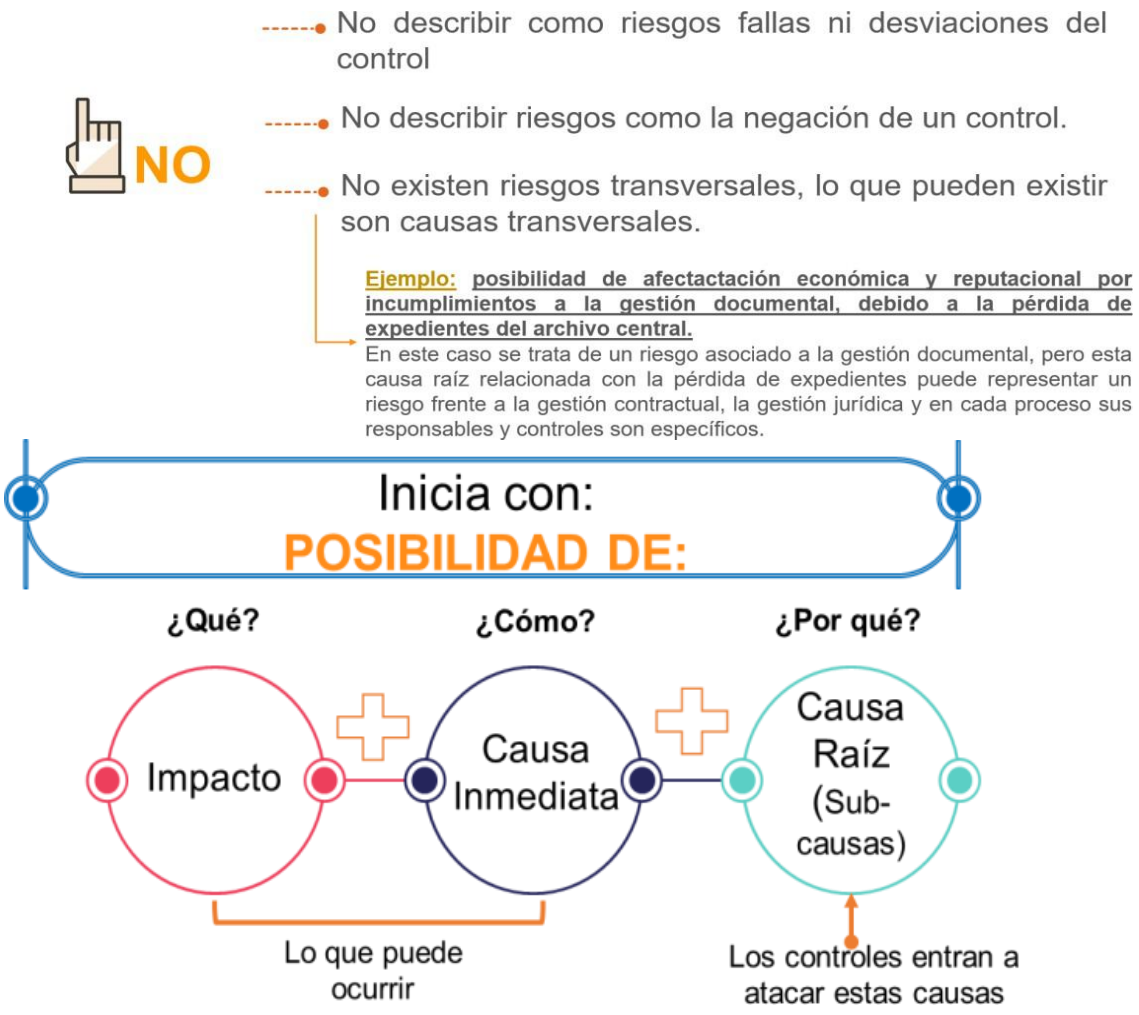
Factor	Definición	Grafico	Descriptores
			Corrupción
			Hurto activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de sistemas de información y aplicaciones
			Caída de redes
			Errores en hardware o software
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.		Fraude Externo
			Suplantación de identidad

Factor	Definición	Grafico	Descriptores
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional -Función Pública y ecretaría de Transparencia, 2025.

Descripción del riesgo:

Despues de realizar los pasos anterios se procede a la descripción del riesgo, teniendo presente una decuada redacción según la siguiente estructura



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

Se debe tener presente las siguientes premisas

d) Análisis de Riesgo Inherente: Se determina la **probabilidad** (posibilidad de ocurrencia del riesgo, medida por la frecuencia de la actividad) y el **impacto** (consecuencias económicas y/o reputacionales). La combinación de estos dos factores se visualiza en una matriz de severidad o mapa de calor.

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**

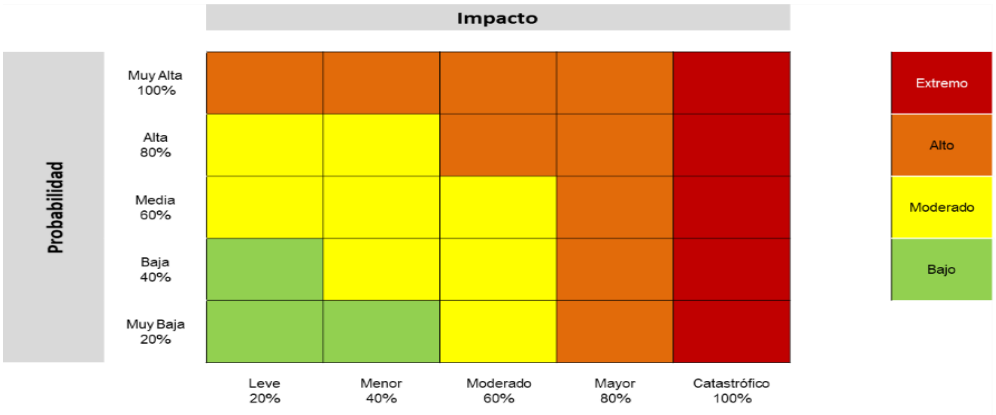
Criterios para definir el nivel de probabilidad

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

e) **Determinar el impacto**: se definen los impactos económicos y reputacionales como las variables principales. así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se hace necesario agruparlos en impacto económico y reputacional, con el fin de facilitar el análisis y evitar la subjetividad en los análisis por parte de los líderes internos.

Criterios para definir el nivel de impacto

Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 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

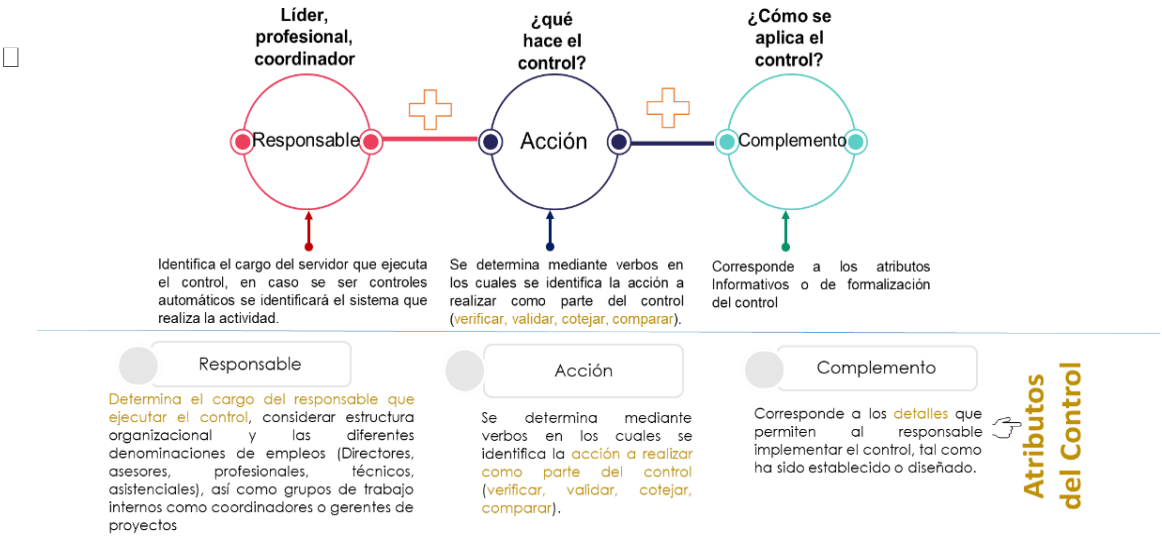
Análisis de severidad:

Consiste en 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 **Matriz de calor (niveles de severidad del riesgo)**

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar el nivel de **RIESGO INHERENTE**.

f) Diseño y Análisis de Controles: Se definen acciones para prevenir, detectar o corregir los riesgos, para su redacción que agrupa los atributos necesarios para garantizar su implementación de forma efectiva por parte del responsable.



Los atributos asociados al control se constituyen en una herramienta de control efectiva, los cuales se agrupan a través de la estructura para la redacción del control **Atributos Informativos o de formalización del control:**

- **Documentación**: se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.

- **Frecuencia**: corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).

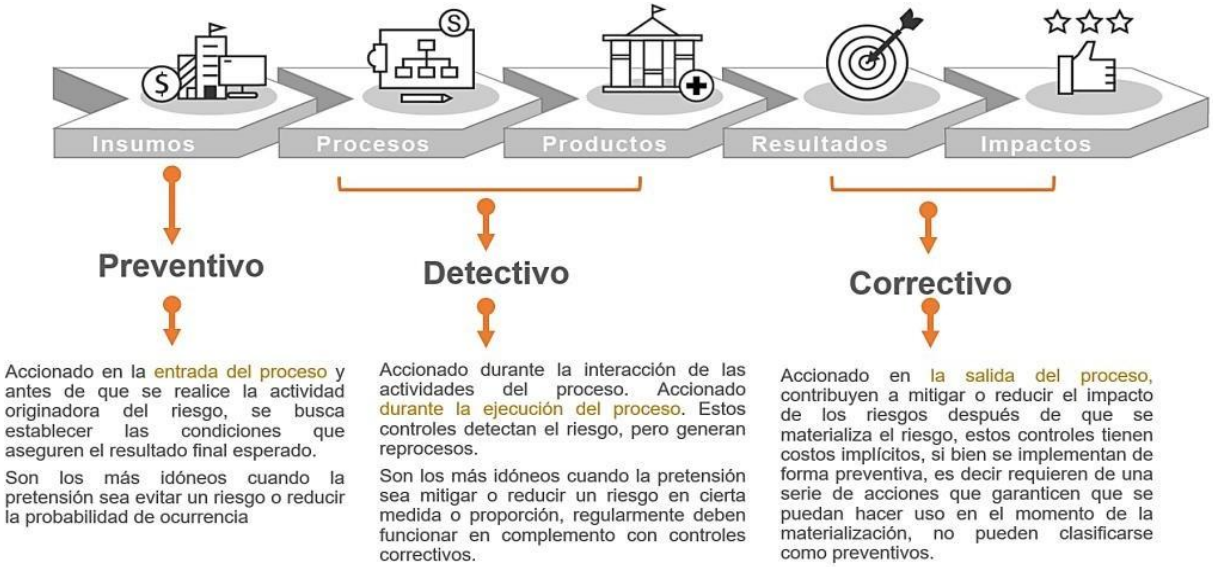
- **Evidencia**: permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.

- **Ejecución**: permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten. Puede darse a través de la comparación con información interna, externa o mixta.

Tipos de controles

- **Control preventivo:** 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:** accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Se debe tener en cuenta que los controles que se contemplan en esta tipología usualmente tienen que ver con pólizas de seguro, copias de seguridad (*backup*), bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez materializado, los cuales se implementan de forma preventiva, es decir requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización pero no pueden clasificarse como preventivos, ya que sería una sobrevaloración de control que podría generar análisis errados en los niveles de severidad.

Desde la cadena de valor de los procesos, se defien el tipo de control, de acuerdo al momento en que se debe activar en función de las actividades clave del proceso.



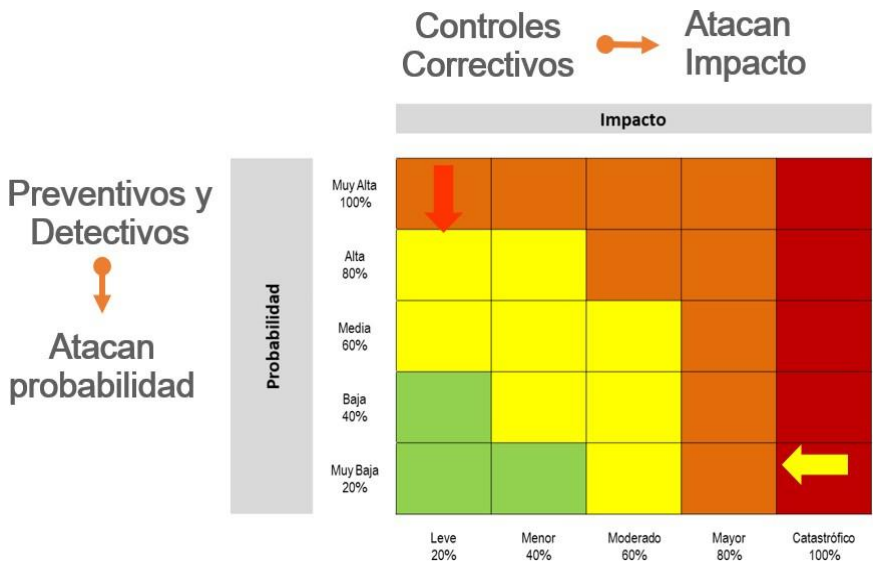
De acuerdo a la ejecución, se tienen dos (2) tipo de controles:

- **Control manual**: ejecutados por personas.
- **Control automático**: ejecutados por un sistema o software previamente programado o diseñado

Valoración de Controles

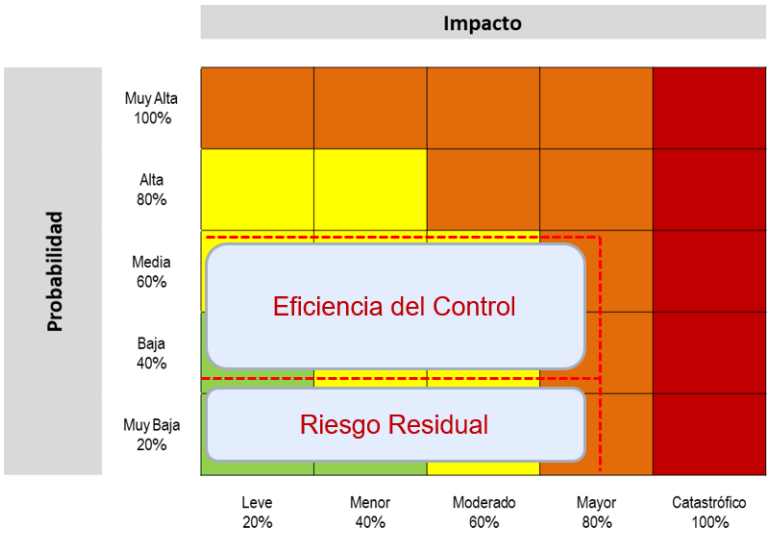
Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Aplicación de Controles en la matriz de severidad: Movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles



g) Valoracion del Riesgo Residual

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



Consolidación Mapa de Riesgos Integral

A partir de la aplicación de cada uno de los pasos metodológicos ya explicados se procede con la elaboración y consolidación del mapa integral de riesgos por proceso.

Gestión Específica de Riesgos

Se tienen tres (3) categorías de riesgo, aplicando la metodología general con particularidades:

12.3.1 Riesgos Fiscales:

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

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

Estos son los riesgos que puedan provocar un **daño patrimonial al Estado**, el cual en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado.

Componentes de la Gestion Fiscal, para determinar los riesgos fiscales

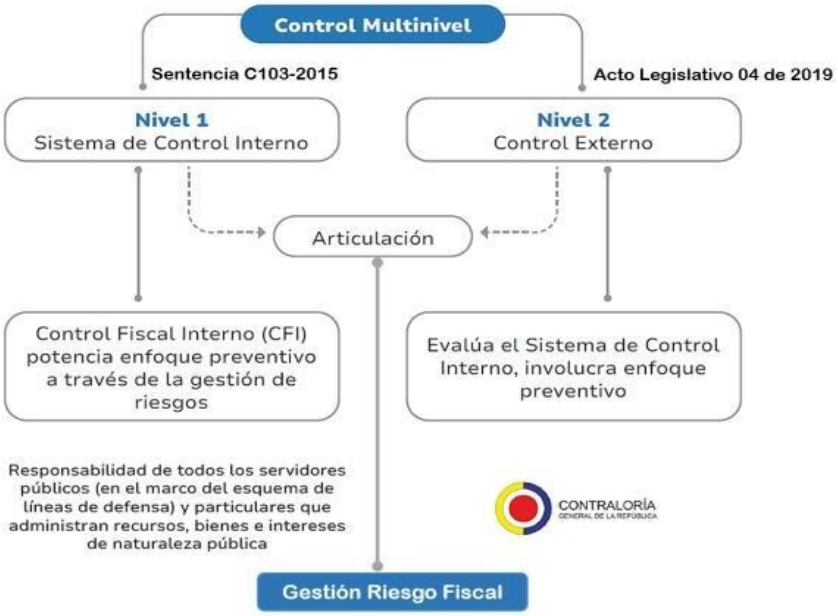
¿Qué es?	¿Quién la realiza?	¿Qué comprende?	¿Para qué?
El conjunto de actividades económicas, jurídicas y tecnológicas	Los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos	La adecuada y correcta • adquisición • planeación • conservación • administración • custodia • explotación • enajenación • consumo • adjudicación • gasto • inversión • disposición • recaudación • manejo • inversión	En orden a cumplir los fines esenciales del Estado, con sujeción a los principios establecidos en artículo 3 de la Ley 610 de 2000

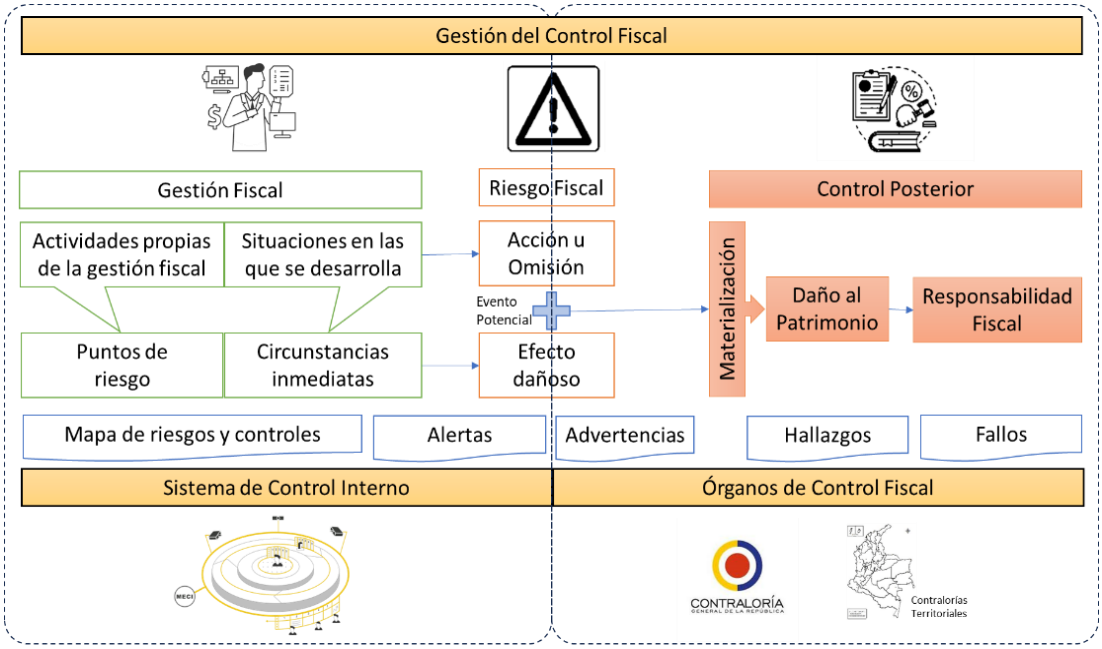
En el nuevo modelo constitucional, el control fiscal adquiere un enfoque preventivo que se potencia con el control interno, a partir de la premisa que el Sistema de Control Interno es el conjunto de mecanismos y medidas que toma una administración para proveer una seguridad razonable respecto al logro de los resultados, con lo cual se brinda también seguridad razonable al gestor fiscal, de haber tomado todas las medidas posibles para evitar daños al patrimonio del Estado.

12.3.1.1 Gestor fiscal

Comprende los jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores de proyectos, responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros roles cuyas funciones u obligaciones incidan en la gestión fiscal.

Articulación modelo constitucional control fiscal y sistema de control interno





Metodología para el levantamiento del mapa de riesgos fiscales

a) Identificación de riesgos fiscales

Pasos para la identificacion de los riesgos fiscales

1. Identificar puntos de riesgo y circunstancias inmediatas	Los **puntos de riesgo fiscal** son eventos en los que potencialmente se genera riesgo fiscal, es decir, son las actividades propias de la gestión fiscal. para lo cual es pertinente prestar especial atención a aquellas en las cuales se han generado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal. En cuanto a las **circunstancias inmediatas** son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo.
2. Identificar el área de impacto	Corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

	Para definir de manera correcta el área de impacto, al momento de identificar y redactar riesgos fiscales se debe tener claro el concepto de: • **Bienes públicos** • **Recursos públicos** • **Intereses patrimoniales de naturaleza pública**
3. Identificar el efecto económico	Es el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público.
4.Indentificar la causa raíz	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).
5. Describir el Riesgo Fiscal	Para redactar un riesgo fiscal, se debe tener en cuenta: Iniciar con la expresión: ***Posibilidad de***, dado que nos estamos refiriendo al evento potencial **Impacto:** corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre el área de impacto (recursos públicos, bienes o intereses patrimoniales de naturaleza pública). **Circunstancia inmediata**: corresponde al cómo. Se refiere a aquella situación en la que se presenta el riesgo; pero no constituye la causa principal que lo genera. **Causa Raíz:** corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño. Es la condición necesaria del riesgo, de tal forma que, si ese hecho no se produce, el daño no se genera.

Estructura de la Descripción del riesgo Fiscal :

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efecto dañoso sobre los **recursos de la entidad**	por la generación de intereses moratorios en contrato de arrendamiento	a causa de la omisión en el pago oportuno del canon pactado.

Nota: 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

Ejemplos de daños económicos

- Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.
- Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, 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
- Multas impuestas por hechos que no comportan gestión fiscal
- Existencia de actuación de cobro coactivo por parte de la entidad.
- Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.
- Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su “normal uso” (máquinas eléctricas, computadores, celulares, etc.). (Contraloría General de la República, 2023, p. 12).

b) Valoracion del Riesgo Fiscal

En esta etapa se realiza la **Evaluación de riesgos** que busca establecer el nivel de riesgo inherente, entendido como la probabilidad de ocurrencia del riesgo, así como su impacto en la gestión fiscal.

c) 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. Se debe tener en cuenta los tipos de control y sus atributos y conocer el riesgo residual

12.3.2 Riesgos de Seguridad de la Información

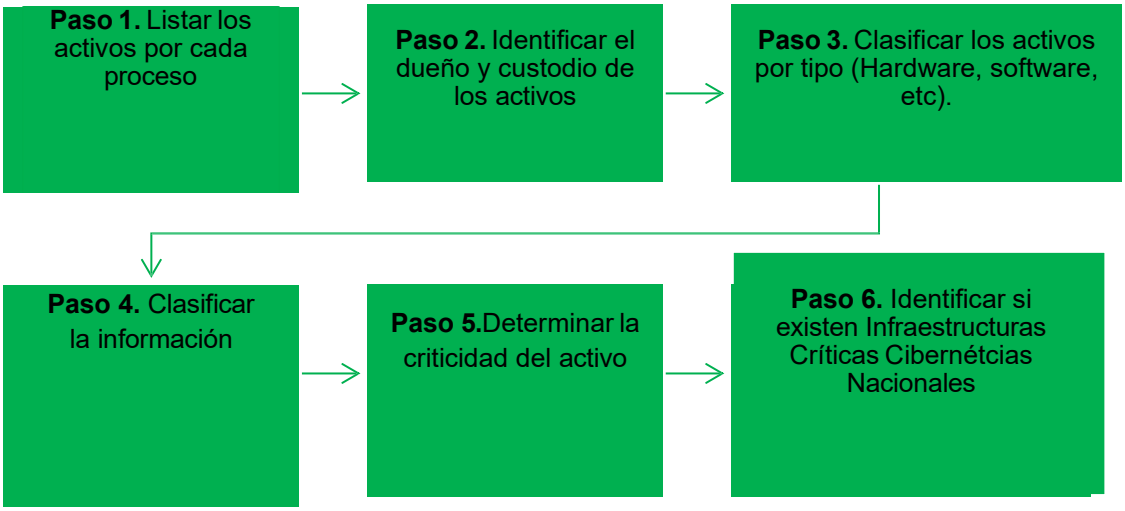
Su objetivo es asegurar los activos de información y fortalecer la confianza en el entorno digital.

El Modelo de Seguridad y Privacidad de la Información es un instrumento desarrollado por el Ministerio de las Tecnologías de la Información y de las Comunicaciones que imparte los lineamientos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información basado en las normas y estándares de mejores prácticas en materia de seguridad de la información

a) Identificación y descripción de riesgos de seguridad de la información

En primer lugar, se deben identificar los activos de Información

Pasos para la identificación y valoración de activos



Se deben listar cada uno de los activos de información de la entidad que corresponden al alcance del proyecto, luego, para cada activo se deben registrar los siguientes datos:

- **Macroproceso**: Macroproceso de la Entidad al que pertenece el activo de información (En caso de que existan).
- **Proceso**: Proceso de la Entidad al que pertenece el activo de información.
- **Identificador**: Se sugiere que el identificador sea una concatenación del código de la dependencia según la Tabla de Retención Documental (TRD) + número consecutivo.
- **Tipo**: Define el tipo de Activo de Información asi:
  - **Información y datos de la entidad**: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros
  - **Sistemas de información y aplicaciones de Software**: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.

- **Dispositivos de Tecnologías de información- Hardware**: Equipos de cómputo que por su criticidad son considerados activos de información, no sólo activos fijos.
- **Soporte para almacenamiento de información**: Equipo para almacenamiento de información como USB, Discos Duros, CDs, SAN, NAS.
- **Servicios**: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- **Recursos Humanos**
- **Instalaciones**
- **Redes**

Clasificación de Activos de Información de acuerdo con la propiedad correspondiente: Disponibilidad, Integridad y Confidencialidad

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Clasificación de Activos

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)						
Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	Es Infraestructura Critica cibernética	Información publicada	Lugar de consulta o ubicación

Índice de Información Clasificada y Reservada

ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA (DECRETO 103 DE 2015)					
Objeto legítimo de la excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción total o parcial	Fecha de clasificación (DD/MM/AAAA)	Tiempo de clasificación

Datos Personales

DATOS PERSONALES (LEY 1581 DE 2012)				
¿Contiene datos personales?	¿Contiene datos personales de niños, niñas o adolescentes?	Tipos de datos personales	Finalidad de la recolección de los datos personales	Existe la autorización para el tratamiento de los datos personales

Matriz de Riesgos de Seguridad de la Información: Con base en la criticidad se realiza el proceso de gestión de riesgos, la cual registra en la Matriz de Riesgos de Seguridad de la Información, con respecto al activo de información se registran los siguientes datos

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN			
Proceso	Referencia	Activo de Información	Tipo de Activo

b) Identificación de áreas de impacto

El área de impacto es la consecuencia negativa en los objetivos de la organización en caso de materializarse un riesgo o las que por causa de incidentes de seguridad de la información tenga consecuencias en la gestión de la entidad.

c) Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos asi:.

Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raíz)

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022) y pueden ser

- Deliberadas (D)
- fortuitas (F)
- Ambientales (A)

Amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F

	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

Tabla de Vulnerabilidades Comunes

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla

Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como usoaceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

d) Descripción del riesgo

Se debe tener en cuenta:

Tipo de Riesgo: Este campo solo admite uno de estos 3 valores:

- Pérdida de Disponibilidad
- Pérdida de Integridad
- Pérdida de Confidencialidad

Descripción del Riesgo: En este campo se describe la situación específica que da como resultado el correspondiente riesgo.

Clasificación del Riesgo: Este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad.

e) **Análisis de Riesgo Inherente: Se** desarrolla con los lineamientos para los riesgos generales de la gestión.

f) Determinar la probabilidad con base en :

- **Frecuencia**: Este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.

- **% Probabilidad Inherente**: Este campo corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa.
- **Probabilidad inherente**: Este campo corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa.

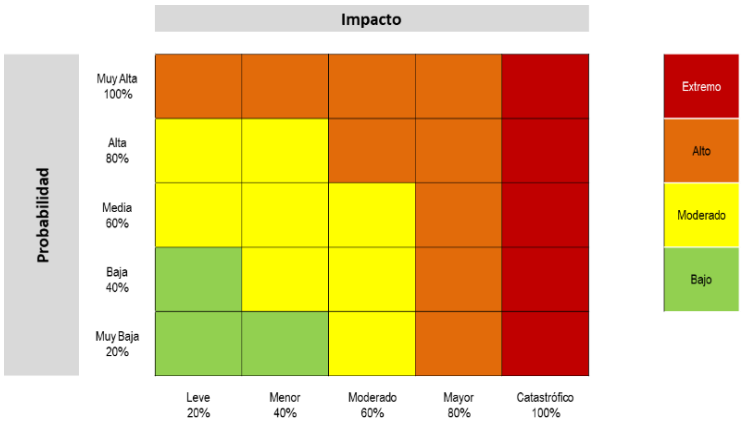
Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

g) Determinar el impacto

- **% Impacto Inherente**: Este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa
- **Impacto Inherente**: Este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa.

Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 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

h) Análisis de la Severidad: Zona de riesgo inherente: En este campo se determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto.



i) Diseño y análisis de controles

Control Anexo A: Este campo corresponde al control seleccionado del Anexo A de la norma 27001:2022.

Valoracion de los controles

En esta actividad se establece la afectación que tendrá la implementación del control sobre la Probabilidad o el Impacto del riesgo **.**

Probabilidad: En este campo se especifica si el control pretende modificar la probabilidad de ocurrencia de riesgo.

Impacto: En este campo se especifica si el control pretende modificar el impacto de ocurrencia de riesgo.

Atributos. En esta actividad se establecen los Atributos de la implementación del control, donde se consideran atributos de eficiencia y los de formalización del control.

j) **Valoración del Riesgo Residual:** En esta etapa se revisa la efectividad de los controles

Valoración del Riesgo Residual

VALORACIÓN DEL RIESGO RESIDUAL				
Probabilidad Residual	% de Probabilidad Residual	Impacto Residual	% Impacto Residual	Zona de Riesgo Final

Plan de implementación de controles

En esta actividad se establece un plan para implementar los controles y poder realizar el correspondiente seguimiento:

PLAN DE IMPLEMENTACIÓN DE CONTROLES					
Tratamiento	Plan de Acción	Responsable	Fecha de Implementación	Seguimiento	Estado

12.3.3.Riesgos para la Integridad Pública (SIGRIP):

Las amenazas clave para la integridad publica son:

- **Soborno**: El Soborno puede ser entendido como "ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]"[9]. Y opera en dos niveles: Soborno Entrante y Saliente. Se entiende como Entrante el soborno al servidor de la Entidad, y como Saliente el soborno por parte de servidores a otros en nombre de la Entidad.

- **Fraude**: El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros[10]. Este puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima

- **Inadecuada gestión del conflicto de intereses** : Un conflicto de intereses[11] surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.

- **corrupción**. La Corrupción es "todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas

punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios *personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral"*[12].

- **Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP:** La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la capacidad del Estado para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento

  El Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP contempla que la entidad adopte una serie de instrumentos de gestión del riesgo, que actúe con diligencia en el conocimiento de sus contrapartes y que integre en su operación una función de cumplimiento, todo esto además de la identificación y valoración de los riesgos según la metodología definida en la Política para la Gestión Integral de Riesgos que adopte. Todos estos elementos interactúan para asegurar que la gestión pública se realice de forma íntegra, es decir, con el pleno cumplimiento de la ley en toda la gestión institucional.

  El SIGRIP, además, permite a las entidades dar cumplimiento a los lineamientos establecidos para la gestión de riesgos en los Programas de Transparencia y Ética Pública, según lo dispuesto por la Secretaría de Transparencia de la Presidencia de la República. En la medida que se implemente plenamente el Sistema, la entidad estará acreditando la gestión de riesgos para la integridad pública, de riesgos LA/FT/FP, canales de denuncia y debida diligencia.

  Roles y Responsabilidades SGIRIP

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	Auditor del Programa	Administrador del Programa	Ejecutores del Programa
Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno	Oficina de Control Interno, Auditoría Interno o quien haga sus veces	Dependencia o persona designada por la Alta Dirección	Directivos, líderes de proceso, servidores y colaboradores
Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP, con el propósito de asesorar y recomendar mejoras.	En el marco del Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP asume la función de cumplimiento que se desarrolla en el numeral 6.3.7.3	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP.

Sistema de Gestión de Riesgos para la Integridad Pública

Componentes de SGRIP

Debida Diligencia

Las entidades deben contar con lineamientos y procedimientos internos sobre la debida diligencia con que deben llevar a cabo el conocimiento de sus contrapartes. Así lo establece la Ley 2195 de 2022, que dispone:

ARTÍCULO 12. PRINCIPIO DE DEBIDA DILIGENCIA. *La Entidad del Estado y la persona natural, persona jurídica o estructura sin personería jurídica o similar, que tenga la obligación de implementar un sistema de prevención, gestión o administración del riesgo de lavado de activos, financiación del terrorismo y proliferación de armas o que tengan la obligación de entregar información al Registro Único de Beneficiarios Finales (RUB), debe llevar a cabo medidas de debida diligencia que permitan entre otras finalidades identificar el/los beneficiario(s) final(es), teniendo en cuenta como mínimo los siguientes criterios:*

- Identificar la persona natural, persona jurídica, estructura in personería jurídica o similar con la que se celebre el negocio jurídico o el contrato estatal.
- Identificar el/los beneficiario(s) final(es) y la estructura de titularidad y control de la persona jurídica, estructura sin personería jurídica o similar con la que se celebre el

negocio jurídico o el contrato estatal, y tomar medidas razonables para verificar la información reportada.

- Solicitar y obtener información que permita conocer el objetivo que se pretende con el negocio jurídico o el contrato estatal. Cuando la entidad estatal sea la contratante debe obtener la información que permita entender el objeto social del contratista.
- Realizar una debida diligencia de manera continua del negocio jurídico o el contrato estatal, examinando las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones sean consistentes con el conocimiento de la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se realiza el negocio jurídico o el contrato estatal, su actividad comercial, perfil de riesgo y fuente de los fondos.

  El obligado a cumplir con el principio de debida diligencia del presente artículo, debe mantener actualizada la información suministrada por la otra parte.

Caracteristicas de la Debida Diligencia

- Identificar el/los beneficiario(s) final(es) y la estructura de titularidad y control de la persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico o el contrato estatal, y tomar medidas razonables para verificar la información reportada.
- Solicitar y obtener información que permita conocer el objetivo que se pretende con el negocio jurídico o el contrato estatal. Cuando la entidad estatal sea la contratante debe obtener la información que permita entender el objeto social del contratista.
- Realizar una debida diligencia de manera continua del negocio jurídico o el contrato estatal, examinando las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones sean consistentes con el conocimiento de la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se realiza el negocio jurídico o el contrato estatal, su actividad comercial, perfil de riesgo y fuente de los fondos.
- El obligado a cumplir con el principio de debida diligencia del presente artículo, debe mantener actualizada la información suministrada por la otra parte.

- contener una evaluación sobre la viabilidad de la vinculación o relación con base en los hallazgos; (3) el informe debe incluir recomendaciones para mitigar o gestionar los riesgos encontrados

A) Establecer un procedimiento y lista de verificación, para la consulta en los siguientes listados:

- Sistema de Información del Boletín de Responsables Fiscales – SIBOR, de la Contraloría General de la República.
- Sistema de Información de Registro de Sanciones e Inhabilidades – SIRI, de la Procuraduría General de la Nación.
- Antecedentes Penales y Requerimientos Judiciales, de la Policía Nacional de Colombia.
- Sistema Registro Nacional de Medidas Correctivas — RNMC, de la Policía Nacional de Colombia.
- Registro de Deudores Alimentarios Morosos — REDAM, del Ministerio de Tecnologías de la Información y las Comunicaciones.
- Lista consolidada del Consejo de Seguridad de las Naciones Unidas, que incluye, pero sin limitarse, las Resoluciones 1267 de 1999, 1988 de 2011,
- 1373 de 2001, 1718 y 1737 de 2006 y 2178 de 2014 del Consejo de Seguridad de las Naciones Unidas, y todas aquellas que le sucedan, relacionen y complementen, y cualquiera otra lista que se adopte formalmente por el país.
- Lista vigente de terroristas de Estados Unidos de América.
- Lista vigente de la Unión Europea de Organizaciones Terroristas.
- Lista vigente de la Unión Europea de Personas Catalogadas como Terroristas.

La consulta deberá hacerse respecto de las contrapartes que sean personas naturales y del representante legal y suplente, revisor fiscal y beneficiarios finales de las contrapartes que sean personas jurídicas u otras estructuras.

B) Establecer un procedimiento para la verificación de la identidad de las contrapartes y evaluación de su historial, lo cual es fundamental para detectar cualquier vinculación con actividades sospechosas. Para lo cual se deberá:

- Identificar el nombre o razón social la contraparte.
- Determinar la existencia y representación legal. Las personas naturales lo acreditan con su cédula; las personas jurídicas con los certificados expedidos por las cámaras de comercio; otras estructuras con su acto de creación y Registro Único Tributario, si aplica.
- En el caso de personas jurídicas u otras estructuras, identificar la estructura de propiedad y existencia de situaciones de control[16].
- En el caso de personas jurídicas u otras estructuras, identificar los beneficiarios finales[17].
- Evaluar las relaciones que ha tenido la contraparte con entidades similares en un período de dos (2) años anteriores al relacionamiento, siempre y cuando la contraparte tenga dos o más años de existencia. Para estos efectos, la entidad podrá solicitar referencias de, al menos, dos entidades similares con que la contraparte haya estado relacionada.
- Determinar si la contraparte cuenta con un Programa de Transparencia y Ética Pública o Empresarial, o con políticas Antilavado de Activos, Antisoborno o Anticorrupción.
- Verificar la documentación aportada para acreditar cualquier hecho en el marco de la relación, como formación, experiencia, capacidad financiera y organizacional, etc.
- Verificar, por los medios disponibles, la reputación de la contraparte. Para esto, la entidad podrá revisar noticias e información pública que esté disponible en internet y hacer uso de herramientas de inteligencia artificial.
- Requerir declaraciones sobre la fuente de los recursos que utilizará en el marco de la relación que mantenga con la entidad, con sus debidos soportes.
- Verificar si la contraparte tiene procesos administrativos sancionatorios, disciplinarios, de responsabilidad fiscal, penales o judiciales, que estén activos o en curso ante las autoridades colombianas

C) Establecer un lineamiento respecto de los casos en que se identifique que una de las contrapartes es una Persona Expuesta Políticamente, según la definición del artículo 2.1.4.2.3 del Decreto 1081 de 2015. Sobre este punto se debe resaltar que la calidad de Persona Expuesta Políticamente (PEP) se mantendrá en el tiempo durante el ejercicio del cargo y por dos (2) años más desde la dejación, renuncia, despido o declaración de insubsistencia del nombramiento, o de cualquier otra forma de desvinculación, o terminación del contrato. La debida diligencia debe incluir una investigación más profunda sobre estas contrapartes, ya que pueden estar expuestos a mayores riesgos para la integridad pública.

D) Establecer lineamientos para la toma de decisiones basada en los resultados de la debida diligencia:

- El Manual debe identificar los procesos en que se deben aplicar los mecanismos de conocimiento de la contraparte. Deben incluirse todos aquellos en que se ha identificado riesgos para la integridad pública. En cada proceso, se deben identificar, además, las operaciones, vinculaciones o relaciones que tienen exposición a riesgos para la integridad pública.
- El Manual debe establecer como una política institucional incluir en todos los procesos donde se identifiquen operaciones, vinculaciones o relaciones expuestas a riesgos, la adopción de un punto de control relacionado con la aplicación de mecanismos de conocimiento de las contrapartes.
- La política, además, debe indicar cómo se realizará la discusión de los hallazgos, y cómo se tomarán decisiones sobre si proceder, modificar o cancelar la operación, vinculación o relación.

E) Establecer un lineamiento para el tratamiento de los hallazgos y las "posdebida diligencia"

- En el Manual la entidad debe incluir una política que establezca el margen de acción posible ante eventuales hallazgos, contemplando los ajustes que puede realizar la entidad en los términos del acuerdo para mitigar riesgos.
- Es fundamental resaltar que no en todos los casos la debida diligencia deriva en una inhabilidad, sin embargo, los hallazgos deben ser objeto de tratamiento.
- El tratamiento de los hallazgos puede ir desde cambios en los términos del acuerdo; supervisión especial a la operación, vinculación o relacionamiento; la transferencia

del riesgo; solicitar garantías adicionales de cumplimiento o requisitos complementarios; el reporte a autoridades; etc. Los posibles

F) Tratamientos los define cada entidad y se pueden ir ajustando conforme la experiencia institucional en gestión del riesgo se haga más compleja.

- En la política debe quedar contemplada la obligación de la entidad de examinar continuamente, a lo largo de la vinculación o relación, las operaciones llevadas a cabo por la contraparte relacionada con los hallazgos, para asegurar que sean consistentes con el conocimiento que se tiene de la contraparte, su actividad económica y su perfil de riesgo.
- Se consideran como alertas que pueden derivar en potenciales hallazgos que requieren tratamiento:
- No haber identificado plenamente a la contraparte, incluyendo, no conocer sus beneficiarios finales.
- La existencia de procesos activos o en curso que involucren a la contraparte, haber obtenido referencias negativas o malos antecedentes en la revisión de la reputación. En el caso de las personas jurídicas u otras estructuras, aplicará respecto del representante legal principal y suplente, el revisor fiscal y los miembros de junta directiva, los controlantes y el beneficiario final.
- Los precios son considerablemente distintos a los normales del mercado, aun cuando no fueron considerados artificiales.
- La contraparte se financia con recursos internacionales que se originan en países no cooperantes o jurisdicciones de riesgo, según lo defina la normativa nacional.
- La relación implica que la contraparte deberá contar con subcontratistas.
- La contraparte está registrada en los listados internacionales vinculantes para el país de personas y entidades asociadas con organizaciones terroristas. En el caso de las personas jurídicas u otras estructuras, aplicará respecto del representante legal principal y suplente, el revisor fiscal y los miembros de junta directiva, los controlantes y el beneficiario final.

G) Establecer un lineamiento para informar a las autoridades de los hallazgos.

Si se detecta alguna actividad intentada o sospechosa de lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva, la entidad está obligada a informar a las autoridades competentes, como la Unidad de Información y Análisis Financiero (UIAF) o Fiscalía General de la Nación. Esto es parte del cumplimiento con las leyes. la entidad debe contemplar un procedimiento para la identificación de estas operaciones sospechosas, por lo que en el Manual solo debe quedar contemplada la política de informar este tipo de hallazgos, así como cualquier otro que se configure como un potencial delito o falta a las autoridades competentes.

Función de cumplimiento

La función de cumplimiento implica, entre otros aspectos:

- Velar por el efectivo, eficiente y oportuno funcionamiento del SIGRIP en su conjunto, y cada uno de sus elementos, promoviendo el cumplimiento de sus disposiciones y apoyando a los líderes de procesos y gestores de riesgo, en la gestión de los riesgos identificados. Para estos efectos, se podrán generar políticas o procedimientos internos, vinculantes para la organización.
- Evaluar el SIGRIP y presentar, en la periodicidad que se establezca, los resultados de la evaluación a la Alta Dirección. Las evaluaciones deberán contemplar, además:

  Los resultados de la gestión desarrollada en el marco de la función de cumplimiento.

  Los reportes de operaciones generados en el marco de la gestión del riesgo.

  Los planes de mejoramiento del SIGRIP implementados, en el marco del proceso de mejora continua.
- Revisar y recomendar la implementación de los lineamientos que el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la
- Presidencia de la República, la Unidad de Información y Análisis Financiero, y las entidades de control, expidan en temas relacionados con la gestión del riesgo.
- Promover la adopción de correctivos del SIGRIP y adoptar aquellos que estén dentro de su competencia.

- Articular con las dependencias correspondientes las gestiones pertinentes para la operatividad del SIGRIP, así como el desarrollo de programas internos de capacitación en materia de cumplimiento y gestión del riesgo.
- Proponer a la Alta Dirección la actualización de los elementos del SIGRIP y velar por su comunicación oportuna a todas las partes interesadas.
- Colaborar con el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos que requiera el SIGRIP y aplicarlos según corresponda.
- Establecer los lineamientos institucionales para la aplicación proporcional basada en riesgos de los mecanismos de debida diligencia en el conocimiento de las contrapartes.
- Elaborar y someter a aprobación de la Alta Dirección, los criterios objetivos para la determinación de las operaciones inusuales y sospechosas.
- Reportar a la Unidad de Información y Análisis Financiero, a la Fiscalía General de la Nación o a la autoridad que corresponda, las operaciones intentadas o sospechosas que se hayan identificado conforme a los criterios definidos y el procedimiento institucional adoptado.

La función de cumplimiento puede ser asignada dentro de las plantas de personal existentes en la mayoría de las entidades públicas y deberán tenerse en cuenta los siguientes aspectos:

- La función puede ser asignada a una persona, grupo o dependencia, según las capacidades de la entidad. Se recomienda tener en cuenta: la estructura organizacional, la planta y cargas de trabajo, la complejidad de las operaciones y el nivel de exposición a los riesgos para la integridad pública, para determinar la capacidad que debe tener la persona, grupo o dependencia que tendrá la función de cumplimiento.
- La función debe estar asignada dentro del segundo nivel jerárquico de la entidad. Es decir, la persona, grupo o dependencia debe responder directa y exclusivamente a la Alta Dirección.
- La persona, grupo o dependencia, preferiblemente, debe dedicarse exclusivamente a desarrollar la función de cumplimiento. Sin embargo, en el evento en que la función se asigne a una persona, grupo o dependencia que no tenga dedicación exclusiva y

desempeñe funciones adicionales, la Entidad debe contar con mecanismos para prevenir y gestionar los conflictos de intereses que puedan surgir producto del ejercicio de otras funciones que podrían ser objeto de evaluación.

- La entidad debe asegurar que la persona, grupo o dependencia se capacite de forma permanente en temas de gestión de riesgos, transparencia, integridad, sistemas de gestión antisoborno, antifraude y de cumplimiento; además deben estar actualizados en los lineamientos de la Política Nacional Antilavado de Activos, contra la Financiación del Terrorismo y contra la Financiación de la Proliferación de Armas de Destrucción Masiva.

- A quien se asigne la función de cumplimiento o quienes integren el grupo de trabajo o dependencia, deberán ser personas reconocidas dentro de la organización por su probidad, ética y que cumplan diligentemente con sus obligaciones, en consecuencia: no podrá haber investigaciones de ningún tipo en su contra; los resultados de sus evaluaciones de desempeño deben ser satisfactorios; deberá haber realizado las declaraciones de bienes y rentas, y de conflictos de interés, de forma oportuna y mantenerlas actualizadas según la normativa vigente.

- Quien asuma la función de cumplimiento podrá asumir, también, el rol de administrador del Programa de Transparencia y Ética Pública de la entidad.

  Además de contar con una Política para la Gestión Integral de Riesgos, un Mapa de Riesgos, un Manual de Debida Diligencia en el Conocimiento de las Contrapartes y una función de cumplimiento distribuida dentro de la organización, la gestión de riesgos para la integridad pública requiere que la organización implemente una serie de políticas, procedimientos y códigos de conducta, que contribuyen a la integralidad del sistema.

- Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP).

- Política Antisoborno

- Política Antifraude

- Procedimiento para la gestión de los conflictos de intereses

- Procedimiento para el reporte de operaciones sospechosas

- Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético

Indicadores Clave de Proceso *(KPI)*	Indicadores Clave de Riesgo (KRI)
Permiten medir periódicamente el desempeño general de la entidad y sus principales unidades operativas.	Complementan el seguimiento a los resultados de la entidad.
Se definen tomando como referencia las metas establecidas, por procesos, unidades u operaciones clave.	Proporcionan una señal temprana y oportuna de una exposición al riesgo en diversas áreas de la entidad.

El Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP debe ser objeto de auditoría, la cual estará a cargo de control interno o quien ejerza la tercera línea de defensa

la mejora del Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP corresponde a la Alta Dirección o línea estratégica, quien lleva a cabo la revisión integral del Sistema

13. SEGUIMIENTO, MONITOREO Y REVISIÓN EN EL MARCO DEL ESQUEMA DE LÍNEAS DEL MODELO ESTÁNDAR DE CONTROL INTERNO MECI

Teniendo en cuenta lo expresado en el capítulo II que desarrolla la alineación estratégica de la gestión del riesgo y el Modelo Integrado de Planeación y Gestión (MIPG), el cual a través de la Dimensión 7 despliega los componentes de evaluación del riesgo y actividades de control en articulación con el esquema de líneas, se precisa que dicho esquema atiende de manera íntegra la gestión del riesgo al interior de la entidad, comprometiendo todos los niveles de la organización, al definir los niveles de autoridad y responsabilidad en la aplicación de controles como eje para materializar el seguimiento y monitoreo a los riesgos que enfrenta la entidad, por lo que, se hace relevante definir adecuados mecanismos para la medición del riesgo como una herramienta estratégica que permite establecer la efectividad de los controles, validar el cumplimiento de metas, analizar comportamientos y tendencias, así como identificar posibles desviaciones que puedan afectar la gestión institucional.

Indicadores Clave de Riesgo (*Key Risk Indicators* — KRI

Articulación entre los indicadores claves del Riesgo y los Indicadores clave del proceso

Mide el rendimiento pasado, proporcionando información sobre qué tan bien se están logrando los objetivos estratégicos y operativos.	Proporcionan información útil sobre los riesgos emergentes y potenciales que pueden impactar en los objetivos estratégicos de la organización.

Ofrecen información sobre aquellos aspectos críticos de la operación que requieren mayores recursos y atención.	Ayudan a identificar y anticipar problemas que se pueden presentar interna o externamente, así como oportunidades futuras.
Permiten medir los resultados que se obtienen de la ejecución de los programas, planes y proyectos, en los diferentes momentos o etapas de su desarrollo.	Permiten realizar un monitoreo constante y mitigar los posibles eventos de riesgo que se presenten al aplicar medidas oportunas para disminuir su impacto.
Permiten mejorar la planificación, entender con mayor precisión las oportunidades de mejora de determinados procesos y analizar el desempeño de las acciones, logrando tomar decisiones con mayor certeza y confiabilidad.	Facilitan el proceso de generación de informes y el escalamiento de los riesgos.

14. SEGUIMIENTO Y MONITOREO INDICADORES CLAVE DE RIESGO (KRI)EN EL MARCO DEL ESQUEMA DE LÍNEAS DE ASEGURAMIENTO

LÍNEAS DE ASEGURAMIENTO	RESPONSABLE	RESPONSABILIDAD FRENTE A LOS INDICADORES CLAVE DE RIESGO (KRI)
Línea Estratégica	Alta Dirección Comité institucional de coordinación de control interno / instancia similar del mismo nivel	• Incorporar en la política para la gestión integral de riesgos lineamientos sobre los Indicadores Clave de Riesgo (KRI) • Realizar seguimiento y análisis periódico a los indicadores claves de riesgos institucionales y proponer mejoras a su estructura. • Analizar los umbrales definidos para los Indicadores Clave de Riesgo (KRI) y sugerir ajustes de ser necesario, de tal forma que estos se alineen con los niveles aceptables para la entidad. • Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a los indicadores claves de riesgo, así como a los indicadores clave de proceso asociados.
	Comité de Gestión y Desempeño Institucional	• Realizar seguimiento y análisis periódico a los indicadores claves de desempeño de manera articulada con los indicadores clave de riesgo. • Generar las alertas que correspondan, de acuerdo con los umbrales definidos para los Indicadores Clave de Riesgo (KRI)
1ª Línea de Aseguramiento	Líderes de Procesos Responsable del proyecto Servidores en general	• Identificar y formular los indicadores clave de riesgos que pueden alertar sobre la exposición al riesgo para los procesos, programas o proyectos bajo su responsabilidad. • Aplicar, medir y hacer seguimiento a los indicadores clave de riesgos, alineados con los indicadores clave de proceso. • Reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos de acuerdo con los indicadores claves de riesgo dentro de los plazos establecidos. • Informar a la Oficina Asesora de Planeación o quien haga sus veces (como 2ª línea de defensa) sobre las alertas críticas resultado de la medición de los indicadores claves de riesgo bajo su responsabilidad. • Si se identifica que un indicador claves de riesgo está fuera

LÍNEAS DE ASEGURAMIENTO	RESPONSABLE	RESPONSABILIDAD FRENTE A LOS INDICADORES CLAVE DE RIESGO (KRI)
		del umbral esperado, la primera línea de defensa debe actuar para corregir las desviaciones identificadas. • Establecer y aplicar las acciones de mejora requeridas para optimizar la operación de los procesos, planes, programas o proyectos de acuerdo con los resultados de las métricas aplicadas.
2ª Línea de Aseguramiento	Oficina Asesora de Planeación, Gerencias de Riesgos o quien haga sus veces	• Asegurar que los indicadores claves de riesgo estén alineados con los objetivos estratégicos y operativos de la entidad. • Proponer la inclusión de los lineamientos en materia de indicadores claves de riesgo en la estructura de la política para la gestión integral de riesgos, para aprobación por parte de la Alta Dirección. • Establecer las metodologías que guíen la medición, seguimiento y monitoreo de los indicadores claves de riesgo, asegurando que se utilicen las mejores prácticas y se implementen de manera efectiva. • Consolidar los indicadores claves de riesgo con mayor criticidad frente al logro de los objetivos y presentarlos periódicamente ***(establecer una periodicidad concreta)*** ante la Línea Estratégica para su análisis y toma de decisiones. • Asesorar y supervisar a la 1ª línea para la correcta identificación, formulación e implementación de los indicadores claves de riesgo.
3ª Línea de Aseguramiento	Jefe Oficina Asesora de Control Interno o quien haga sus veces	• Verificar si los indicadores claves de riesgo están definidos y se aplican por parte de los responsables. • Evaluar si los indicadores claves de riesgo son pertinentes y eficaces para la oportuna generación de alertas y/o implementación de correctivos. • Informar a la Alta Dirección en coordinación con la 2ª línea, cuando se detecten deficiencias o brechas en los indicadores claves de riesgo para que tomen decisiones
		sobre las medidas preventivas y correctivas que deben implementarse. • Asesorar y acompañar a la Alta Dirección en el análisis de los resultados de los indicadores claves de riesgo, así como en la incorporación de estrategias para la identificación y monitoreo estratégico de los indicadores claves de riesgo.

Es fundamental comprender que el resultado del cálculo del KRI se relaciona directamente con el apetito al riesgo, y debe ser analizado de cara a la declaración de apetito de la entidad bajo las siguientes consideraciones.

i) **Valor del KRI dentro del apetito al riesgo:** Significa que la operación de la entidad, y por ende el riesgo se sigue moviendo dentro delo que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta

dirección.

ii) **Valor del KRI que excede el apetito al riesgo:** Significa que el riesgo ha superado el umbral que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. En este caso se deben tomar **acciones correctivas o de mitigación** para llevar el riesgo de nuevo hacia un rango tolerable.

iii) **Valor del KRI se acerca al umbral de alerta definido:** Revela que el riesgo se ha ido aumentando y que podría salir del umbral de alerta si continua así.

15. NIVELES DE APETITO DEL RIESGO, TOLERANCIA DEL RIESGO Y CAPACIDAD DEL RIESGO

- El nivel de apetito de riesgo definido como el nivel de riesgo que la Entidad busca asumir para poder lograr sus objetivos, sin necesidad de establecer controles adicionales tendientes a disminuir su probabilidad o su impacto se ha definido de acuerdo con los siguientes criterios.
- El análisis para la toma de las decisiones se realiza tomando como base el nivel de riesgo residual a excepción de cuando el análisis se realiza sobre procesos nuevos, frente a lo cual el análisis se realiza con base en el nivel de riesgo inherente.
- La entidad solo buscará asumir los riesgos cuyo nivel de riesgo sea evaluado como BAJO sin necesidad de establecer medidas adicionales para su mitigación**.**
- Ningún riesgo de corrupción podrá aceptarse, por lo que ningún riesgo de corrupción se puede evaluar en nivel bajo.
- Los riesgos calificados como EXTREMOS no pueden ser admitidos bajo ninguna circunstancia por la entidad debido a que su materialización impediría el logro de objetivos de la entidad

16. REQUISITOS Y CUMPLIMIENTO

Norma	Contenido
Acto Legislativo 04 de 2019	Por medio del cual se reforma el Régimen de Control Fiscal
Circular Conjunta 100-01 de 2021	Emite directrices para la implementación de seguridad digital en entidades públicas
COSO-ERM (2017)	Marco actualizado de Gestión de Riesgos Empresariales del Committee of Sponsoring Organizations of the Treadway Commission, centrado en integrar la gestión de riesgos con la estrategia y el desempeño

Norma	Contenido
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1122 de 2024	Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
Decreto 620 de 2020	Política de seguridad digital Fortalece la política de seguridad digital para entidades públicas, incluyendo la gestión de riesgos de seguridad de la información.
Guia N. 7 gestion del riesgo	Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP).
ISO 27001	Sistema de Gestión de Seguridad de la Información (SGSI
ISO/IEC 27001 e ISO/IEC 31000	Estándares internacionales de gestión de seguridad de la información y riesgos.
ISO31000:2018-numeral 5.2	Establece un marco de referencia que tiene como objetivo ayudar a las organizaciones a integrar la gestión del riesgo en todas sus actividades y funciones principales
La Ley 610 de 2000	Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.
Ley 1273 de 2009	Define delitos informáticos y protege la integridad de los datos.
Ley 1581 de 2012 y Decreto 1377 de 2013	Protección de datos personales
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública
Ley 2195 de 2022	Por medio de la cual se adoptan medidas en materia de transparencia, prevencion y lucha contra la corrupcion y se dictan otras disposiciones.
Ley 594 de 2000	Ley General de Archivos de Colombi
Ley 87 de 1993	Por el cual se definen normas para el ejercicio del control interno

17. DEFINICIONES

Con el propósito de facilitar la comprensión de la Política se deben tener en cuenta las siguientes definiciones.

- **Administración 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

- **Apetito del riesgo:** es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Causa**: Medios, circunstancias, situaciones o agentes generadores del riesgo. Algunas fuentes de riesgos son: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.
- **Causa Raíz**: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Evaluación del riesgo**: Determinación de las prioridades de gestión del riesgo, mediante la comparación del nivel de riesgo hallado (riesgo inherente) y la evaluación de las medidas de control existentes. Es una etapa que busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual.
- **Gestión del riesgo**: Es el conjunto de "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Contempla las etapas de política de administración del riesgo, construcción del mapa de riesgos, comunicación y consulta, monitoreo y revisión y seguimiento.
- **Probabilidad**: se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.
- **Impacto**: consecuencias o efectos que pueden ocasionar a la organización la materialización del riesgo

18. COMUNICACIÓN REVISIÓN Y SEGUIMIENTO

Los líderes de proceso monitorean constantemente los controles definidos para los riesgos y las acciones del plan de acción, cuando haya lugar.

La Oficina de Planeación, cumplirá con las acciones de monitoreo de acuerdo con las responsabilidades como segunda línea de defensa trimestralmente.

La Oficina de Control Interno lleva a cabo el seguimiento a la administración del riesgo como se determina en los roles y responsabilidades.

19. CONTROL DE CAMBIOS

N°. de Versión	Fecha de Versión	Autor	Revisado por	Aprobado por	Descripción del cambio
01	11/06/2024	Gerencia general	Dirección de planeación Institucional	Comité Institucional de Gestión y Desempeño	Creacion del documento
02	28/01/2026	Gerencia general	Dirección de planeación Institucional	Comité Institucional de Gestión y Desempeño	Actualizacion según Guía para la gestión integral del riesgo en entidades públicas Versión 7 2025