POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	1 de 50

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

GIT DE PLANEACIÓN
GIT DE APOYO INFORMÁTICO

Julio de 2026

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	2 de 50

TABLA DE CONTENIDO

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	3 de 50

1. INTRODUCCIÓN

La presente Política de Administración del Riesgo establece los lineamientos y metodologías para identificar, evaluar, mitigar y monitorear los riesgos que puedan afectar la operación y los objetivos de la Contaduría General de la Nación (CGN). Se fundamenta en el Modelo Integrado de Planeación y Gestión (MIPG), la NTC-ISO 31000:2018, la Resolución 02277 del 3 de junio de 2025, Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia, las mejores prácticas basadas en el marco COSO-ERM y la Metodología General Ajustada (MGA WEB).

Además, se actualiza con los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, del Departamento Administrativo de la Función Pública (DAFP).

2. OBJETIVO

Establecer los lineamientos estratégicos y operativos para la administración integral de los riesgos en la Contaduría General de la Nación, con el fin de fortalecer la toma de decisiones, contribuir al cumplimiento de los objetivos estratégicos de la entidad y promover una cultura organizacional orientada al control y la prevención.

Asimismo, la política busca alcanzar un nivel de riesgo residual aceptable mediante la implementación efectiva de controles y acciones de mitigación junto con una marcada orientación hacia la generación de valor público, la integridad, la transparencia y el uso eficiente de los recursos públicos.

3. ALCANCE

La política será aplicable en todo nivel, a los procesos institucionales, activos y proyectos, de conformidad con cada tipo y clasificación de riesgo,

bajo la responsabilidad de las líneas de defensa, o terceros que operen a través de empresas privadas o mediante convenios administrativos realizados con entidades públicas. Sobre el particular es importante realizar las siguientes precisiones:

- **Riesgos de gestión:** se presentan en todos los procesos institucionales; están relacionados con eventos que pueden afectar el cumplimiento de las funciones, objetivos y metas de la Entidad. Identificarlos a tiempo permite la acertada toma de decisiones y evitar afectaciones en la operación institucional.

  En línea con lo anterior, se incluye en este alcance a los riesgos institucionales, los cuales corresponden a los riesgos de gestión con un nivel alto o extremo de impacto. Se caracterizan porque pueden comprometer seriamente la sostenibilidad y los objetivos estratégicos de la entidad, por lo que requieren una atención prioritaria y medidas efectivas de mitigación.

- **Riesgos para la integridad pública:** son aquellos que pueden impactar el ejercicio íntegro de la función pública como la corrupción, el soborno, el fraude y la inadecuada gestión del conflicto de intereses. Estos incluyen además los riesgos de Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP). La gestión de estos riesgos se realizará a partir de lo establecido en el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) y el Programa de Transparencia y Ética Pública.

- **Riesgos fiscales**: se presentan en todos los procesos institucionales, están relacionados con posibles afectaciones a los recursos públicos o bienes del Estado debido a eventos que generen pérdidas o perjuicios patrimoniales. Su adecuada gestión protege el patrimonio público y asegura su correcto uso.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	5 de 50

- **Riesgos de seguridad de la información:** aplican a todos los activos digitales, sistemas críticos y recursos tecnológicos de la CGN. Se refieren a la posibilidad de que amenazas internas o externas exploten vulnerabilidades en los activos de información, servicios de TI, generando afectaciones, pérdidas o acceso no autorizado a la información institucional. La adecuada gestión de estos riesgos permite garantizar la confidencialidad, integridad y disponibilidad de los datos, así como la continuidad y protección de los procesos institucionales.

- **Riesgos de ciberseguridad:** posibilidad de afectación a los activos digitales, infraestructuras tecnológicas, redes, sistemas de información o servicios digitales, ocasionada por amenazas cibernéticas internas o externas, ataques informáticos, accesos no autorizados, software malicioso, vulnerabilidades tecnológicas u otros eventos que comprometan la operación institucional y la seguridad digital.

- **Riesgos de continuidad de la operación:** posibilidad de interrupción parcial o total de los procesos, servicios, sistemas de información o capacidades institucionales, como consecuencia de eventos internos o externos que afecten la disponibilidad y continuidad de la operación, generando impactos sobre la prestación de servicios misionales y el cumplimiento de los objetivos institucionales de la CGN.

- **Riesgos en proyectos**: se presentan en todos los proyectos de inversión estructurados con la Metodología General Ajustada (MGA) y registrados en el Banco de Programas y Proyectos de Inversión Nacional (BPIN) del Departamento Nacional de Planeación (DNP), desde su etapa de prefactibilidad. Su identificación temprana facilita una mejor planeación, ejecución y uso eficiente de los recursos.

- **Riesgo emergente:** es una manifestación novedosa de riesgo que no se ha experimentado previamente. Para poder diferenciar entre los riesgos emergentes y los riesgos que pueden estar evolucionando con el tiempo,

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	6 de 50

RIMS utiliza el término "riesgos dinámicos", que son riesgos que se sabe que existen, pero que pueden cambiar con el tiempo.

4. GLOSARIO[1]

- **Activo de información**: en relación con la seguridad de la información, se refiere a cualquier tipo de dato, archivo, documento o recurso digital que tiene un valor para una organización y que debe ser protegido debido a su importancia para el funcionamiento o los objetivos de esta.
- **Amenazas**: causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.
- **Asegurar**: en el marco del Modelo Integrado de Planeación y Gestión (MIPG), se refiere a la garantía de que los procesos, actividades, operaciones y resultados de una entidad pública se realicen de acuerdo con las normas, políticas y planes establecidos. Esto implica la verificación y evaluación objetiva para asegurar la eficiencia, eficacia, transparencia y legalidad de la gestión.
- **Capacidad de riesgo:** es el máximo nivel de riesgo que la entidad puede soportar antes de que el logro de sus objetivos se vea comprometido.
- **Ciberseguridad**: se refiere a las actividades y medidas necesarias para proteger los activos de información, como la información procesada, almacenada y transportada por los sistemas de información interconectados, los usuarios involucrados y otros afectados por las ciberamenazas.

[1] Las fuentes de las definiciones de este numeral son las siguientes:
- Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7.
- https://www.dnp.gov.co/LaEntidad_/subdireccion-general-inversiones-seguimiento-evaluacion/direccion-proyectos-informacion-para-inversion-publica/Paginas/metodologia-general-ajustada-mga.aspx
- Guía de implementación de *RIMS Strategic Risk Management*

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	7 de 50

- **CICCI (Comité Institucional de Coordinación de Control Interno)**: órgano asesor encargado de coordinar y articular el control interno institucional, conforme a lo establecido por el Modelo Integrado de Planeación y Gestión (MIPG).
- **Confidencialidad**: propiedad de la información que la hace no disponible, es decir, que excluye de su divulgación a individuos, entidades o procesos no autorizados.
- **Control**: medida que permite reducir o mitigar un riesgo.
- **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".*
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Factor de riesgo**: son las fuentes generadoras de riesgo, es decir, la condición que, de presentarse, aumenta la probabilidad de ocurrencia del riesgo. No son causas directas, pero incrementan el nivel de exposición.
- **Fraude**: corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo buscando un beneficio personal o de terceros.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	8 de 50

- **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.
- **Gestión del riesgo fiscal**: son las actividades que debe desarrollar la Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales.
- **Inadecuada gestión del conflicto de intereses:** ejecución de comportamientos definidos por códigos de conducta sobre la declaración y gestión del conflicto de intereses por parte de quien tenga un interés particular en un asunto público. Se materializa al no declararse bajo impedimento para tomar cualquier decisión relacionada con el asunto público involucrado.
- **Integridad**: propiedad de exactitud y completitud de la información. Este principio de seguridad garantiza que los datos no sean alterados, manipulados o dañados de manera intencionada o accidental, permaneciendo exactos y fiables a lo largo del tiempo, ya sea en su transmisión o almacenamiento.
- **Integridad pública**: es la posibilidad de que una persona, actuando desde un comportamiento ético, se adecúe a una serie de códigos de conducta preestablecidos. Particularmente se espera que los servidores, y en general los colaboradores de las entidades públicas, se comporten de forma que privilegien el interés general del Estado en todas las decisiones que deben tomar en el ejercicio de sus funciones o del servicio que prestan.
- **Impacto**: consecuencias o efectos negativos que puede generar la materialización de un riesgo en los objetivos, procesos o activos de la organización.
- **Indicadores clave de proceso (KPI):** son aquellos que se diseñan para medir el cumplimiento de la misión institucional, desde lo estratégico hasta lo operativo. Su definición y esquema de alertas tempranas depende de las características del proceso, plan, programa o proyecto que se analice y de sus indicadores clave de desempeño.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	9 de 50

- **Indicadores Clave de Riesgo (KRI):** son *"(…) métricas utilizadas por las organizaciones para proporcionar una señal temprana de exposiciones al riesgo, cada vez mayores en diversas áreas de la organización. (…) estos indicadores proporcionan información oportuna sobre riesgos emergentes y potenciales que pueden tener impacto sobre el logro de los objetivos de la organización, así como las medidas en las cuales diferentes eventos o puntos desencadenantes, pueden indicar problemas que se desarrollan internamente dentro de las operaciones de la organización o los riesgos potenciales relacionados con eventos externos, esto quiere decir que pueden ofrecer información valiosa para la administración y la junta directiva de cada organización para tomar las medidas correctivas y preventivas para mitigar los riesgos y velar por el cumplimiento de los objetivos establecidos."*
- **Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP:** prácticas y conductas que comprometen 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.
- **Metodología General Ajustada (MGA)**: es un método para la formulación y estructuración de proyectos de inversión pública, desarrollada por el Departamento Nacional de Planeación (DNP).
- **Nivel de aceptación del riesgo**: es el nivel de riesgo que la entidad está dispuesto a asumir en relación con su direccionamiento estratégico y su cumplimiento legal. Este nivel puede variar por cada tipología de riesgo definida al interior de la entidad.
- **Niveles de madurez para la gestión del riesgo (COSO-ERM):** estado de desarrollo/implementación de componentes y principios del marco, usado para definir brechas y planes de mejora.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	10 de 50

- **Programa de Transparencia y Ética Pública (PTEP)**: es el conjunto de acciones que una entidad pública define e implementa para promover, al interior de la organización, una cultura de la legalidad e identificar, medir, controlar y monitorear los riesgos de corrupción que se presentan en el desarrollo de su misión.
- **Probabilidad**: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente corresponderá a la frecuencia estimada con la que se ejecuta la actividad expuesta al escenario de riesgo en un periodo de un (1) año.
- **Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
  Nota: los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo emergente:** es una manifestación novedosa de riesgo que no se ha experimentado previamente. Para poder diferenciar entre los riesgos emergentes y los riesgos que pueden estar evolucionando con el tiempo, RIMS utiliza el término "riesgos dinámicos", que son riesgos que se sabe que existen, pero que pueden cambiar con el tiempo.
- **Riesgo inherente**: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo residual**: es el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **SIGRIP:** es un sistema de gestión que permite prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), de manera integral. Contar con un sistema en la entidad garantiza que se

interrelacionen e interactúen los diferentes elementos para asegurar una gestión integral del riesgo.

- **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* […].
- **Tolerancia del riesgo:** corresponde al valor de la máxima desviación que se admite del nivel de riesgo con respecto al valor de la aceptación de riesgo determinado por la entidad.
- **Vulnerabilidad**: debilidad de un activo o control que puede ser explotado por una o más amenazas.

5. NIVELES DE RESPONSABILIDAD PARA EL MANEJO DE LOS RIESGOS

El Modelo Integrado de Planeación y Gestión (MIPG), en la dimensión 7 denominada "Control Interno", establece la gestión del riesgo y el control como una responsabilidad compartida, estructurada a través de una línea estratégica y tres (3) líneas de aseguramiento. A continuación, se detallan las responsabilidades asignadas a cada una de estas líneas:

LÍNEA ESTRATÉGICA Define el marco general para la gestión del riesgo y el control, supervisa su cumplimiento.	
RESPONSABLE	**RESPONSABILIDAD**
Alta Dirección Comité Institucional de Coordinación	• Asumir la responsabilidad primaria del Sistema de Control Interno, de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo. • Definir e impartir lineamientos relacionados con el marco general para la administración de los riesgos.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	12 de 50

LÍNEA ESTRATÉGICA Define el marco general para la gestión del riesgo y el control, supervisa su cumplimiento.	
de Control Interno	• Aprobar la Política de Administración del Riesgo. • Realizar recomendaciones orientadas a la mejora y actualización de la Política de Administración del Riesgo. • Supervisar el cumplimiento de la Política de Administración del Riesgo. • Revisar los resultados del monitoreo y seguimiento de los riesgos, generar alertas y recomendaciones cuando sea necesario. • Identificar conflictos de interés o su inadecuado manejo que puedan generar Riesgos para la Integridad Pública. • Revisar y aprobar las matrices de riesgos. • Definir y aprobar el apetito, tolerancia y capacidad de riesgo por tipología de riesgo. • Aprobar los umbrales y lineamientos e indicadores clave de riesgo (KRI). • Analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP. • Asegurar la articulación de la política con SIGRIP/PTEP para riesgos de integridad pública.

PRIMERA LÍNEA DE ASEGURAMIENTO Desarrolla e implementa procesos de control y de gestión de riesgos a través de su identificación, análisis, monitoreo y acciones de mejora.	
RESPONSABLE	**RESPONSABILIDAD**
Líderes de Proceso Director de Proyectos y Formuladores de Proyectos	• Promover la administración de los riesgos en los equipos internos de trabajo. • Identificar, analizar, valorar y actualizar, cuando sea necesario, los riesgos del proceso o proyecto bajo su responsabilidad.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	13 de 50

PRIMERA LÍNEA DE ASEGURAMIENTO Desarrolla e implementa procesos de control y de gestión de riesgos a través de su identificación, análisis, monitoreo y acciones de mejora.	
Integrantes de Equipo Operativo del Sistema de Gestión y Desempeño	• Diseñar, aplicar y monitorear los controles de manera directa, para mitigar los riesgos identificados y proponer mejoras para su gestión. • Documentar la identificación del riesgo, análisis de causas, acciones de control establecidas, valoración y gestión de los riesgos en la matriz de riesgos. • Orientar el desarrollo e implementación de las políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la Entidad. • Verificar directamente el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y que su documentación se encuentre soportada en los procedimientos de los procesos. • Efectuar el monitoreo a los mapas de riesgo a su cargo, analizar los resultados del seguimiento y formular, establecer o adoptar las acciones correspondientes ante cualquier desviación. • Reportar al GIT de Planeación y al GIT de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información, los avances y soportes (evidencias) de la gestión de los riesgos dentro de los plazos establecidos. • Comunicar al equipo de trabajo los resultados de la gestión del riesgo. • Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Establecer, documentar y gestionar la implementación de planes de mejoramiento para los riesgos que se identifique su materialización.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	14 de 50

PRIMERA LÍNEA DE ASEGURAMIENTO Desarrolla e implementa procesos de control y de gestión de riesgos a través de su identificación, análisis, monitoreo y acciones de mejora.	
	• Reportar indicadores, umbrales y eventos emergentes a la segunda línea para consolidación y monitoreo. • Ejecutar y monitorear los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.
Servidores públicos y colaboradores	• Participar en las charlas o sensibilizaciones y actividades de fortalecimiento de la cultura de gestión del riesgo. • Participar en el diseño de los controles bajo su responsabilidad. • Ejecutar los controles conforme han sido diseñados. • Generar con oportunidad las alertas correspondientes, ante la posible materialización de los riesgos. • Informar al superior jerárquico o supervisor de contrato sobre los riesgos materializados o desviaciones en la aplicación de los controles. • Proponer mejoras a los controles existentes para optimizar su efectividad. • Reportar señales de alerta y participar en acciones de Integridad Pública – SIGRIP. • Identificar y evaluar los riesgos asociados a los procesos, actividades y activos de información identificados. • Implementar acciones preventivas y correctivas para mitigar la materialización de los riesgos. • Garantizar el cumplimiento de políticas, procedimientos y lineamientos institucionales en materia de gestión del riesgo y seguridad de la información.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	15 de 50

PRIMERA LÍNEA DE ASEGURAMIENTO	
Desarrolla e implementa procesos de control y de gestión de riesgos a través de su identificación, análisis, monitoreo y acciones de mejora.	
	• Custodiar adecuadamente los activos de información y hacer uso responsable de los recursos tecnológicos institucionales.

SEGUNDA LÍNEA DE ASEGURAMIENTO	
Asegura[2] que los controles y los procesos de gestión de riesgos implementados por la primera línea de aseguramiento, estén diseñados apropiadamente y funcionen conforme con lo establecido por las disposiciones legales y reglamentarias, así como por las políticas y procedimientos internos. Es responsable de evaluarla gestión de riesgos y controles ejecutados por la primera línea de aseguramiento, acompañando a los procesos en la administración de riesgos y en la consolidación de los mapas de riesgos.	
RESPONSABLE	**RESPONSABILIDAD**
GIT de Planeación	• Asesorar a la línea estratégica en la formulación y/o actualización de la política y los lineamientos generales para la administración de riesgos. • Coordinar la elaboración del diagnóstico de niveles de madurez COSO ERM y plan de mejora. • Articular la gestión de riesgos para la integridad de la gestión pública con SIGRIP/PTEP.
GIT de Apoyo Informático, Oficial de Seguridad y Privacidad de la Información articulado con el GIT de Planeación	• Actualizar la política de administración de riesgos, especialmente en lo relacionado con los riesgos de seguridad de la información y ciberseguridad. • Incorporar el despliegue metodológico completo de riesgos de seguridad de la información (inventario y clasificación de activos,

[2] Asociado a la garantía de que los procesos, actividades, operaciones y resultados de una entidad pública se realicen de acuerdo con las normas, políticas y planes establecidos. Esto implica la verificación y evaluación objetiva para asegurar la eficiencia, eficacia, transparencia y legalidad de la gestión.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	16 de 50

SEGUNDA LÍNEA DE ASEGURAMIENTO	
Asegura[2] que los controles y los procesos de gestión de riesgos implementados por la primera línea de aseguramiento, estén diseñados apropiadamente y funcionen conforme con lo establecido por las disposiciones legales y reglamentarias, así como por las políticas y procedimientos internos. Es responsable de evaluarla gestión de riesgos y controles ejecutados por la primera línea de aseguramiento, acompañando a los procesos en la administración de riesgos y en la consolidación de los mapas de riesgos.	
	amenazas/vulnerabilidades, controles y matriz) y sus KRIs asociados.
El GIT de Planeación y GIT de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información (según aplique)	• Acompañar a los líderes de los procesos y sus equipos en identificación de los riesgos y controles para la gestión de riesgos y su mejora continua. • Realizar seguimiento periódico a todos los riesgos, permitiendo que se generen recomendaciones y ajustes necesarios a los mapas de riesgos. • Realizar seguimiento a los controles aplicados por la primera línea de aseguramiento. • Presentar los mapas de riesgos consolidados para la socialización y aprobación al Comité Institucional de Coordinación de Control Interno.
GIT Logístico de Capacitación y Prensa	• Revisar que la información interna y externa de la Entidad, cumpla con las disposiciones legales, reglamentarias y demás lineamientos impartidos por la Presidencia de la República en materia de comunicación pública. • Realizar seguimiento a los controles aplicados por la primera línea de aseguramiento en materia de comunicaciones, capacitación y prensa.
Secretaría General en articulación con el Coordinador del	• Consolidar los avances del Plan Anual de Adquisiciones y generar alertas ante posibles retrasos o incumplimientos y reportar en el

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	17 de 50

SEGUNDA LÍNEA DE ASEGURAMIENTO	
Asegura[2] que los controles y los procesos de gestión de riesgos implementados por la primera línea de aseguramiento, estén diseñados apropiadamente y funcionen conforme con lo establecido por las disposiciones legales y reglamentarias, así como por las políticas y procedimientos internos. Es responsable de evaluarla gestión de riesgos y controles ejecutados por la primera línea de aseguramiento, acompañando a los procesos en la administración de riesgos y en la consolidación de los mapas de riesgos.	
GIT de Servicios Generales, Administrativos y Financieros	Comité de Coordinación de Control Interno para definir acciones de mejora. • Realizar seguimiento a los controles aplicados por la primera línea de aseguramiento en materia de contratación.
Secretaría General en articulación con el Coordinador del GIT de Talento Humano y Prestaciones Sociales	• Consolidar los avances sobre el Plan Institucional de Capacitación (PIC), Bienestar, Incentivos y temas de convivencia laboral, y generar alertas sobre la ejecución de recursos y reportar en el Comité de Coordinación de Control Interno para definir acciones de mejora. • Realizar seguimiento a los controles aplicados por la primera línea de aseguramiento en materia de gestión del talento humano.
Coordinador del GIT de Jurídica	• Verificar la gestión judicial, generar alertas sobre los procesos que se encuentran abiertos y sus cuantías, y reportar en las instancias correspondientes (Comité de Conciliación y el Comité Institucional de Coordinación de Control Interno) para definir acciones de mejora. • Realizar seguimiento a los controles aplicados por la primera línea de aseguramiento en materia de gestión jurídica. • 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 6.3.5.3 de la Guía para la Gestión

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	18 de 50

SEGUNDA LÍNEA DE ASEGURAMIENTO	
Asegura[2] que los controles y los procesos de gestión de riesgos implementados por la primera línea de aseguramiento, estén diseñados apropiadamente y funcionen conforme con lo establecido por las disposiciones legales y reglamentarias, así como por las políticas y procedimientos internos. Es responsable de evaluarla gestión de riesgos y controles ejecutados por la primera línea de aseguramiento, acompañando a los procesos en la administración de riesgos y en la consolidación de los mapas de riesgos.	
	Integral del Riesgo en Entidades Públicas, en su versión vigente. • Acompañar la identificación y valoración diferenciada de soborno, fraude, conflicto de intereses, corrupción y LA/FT/FP; y verificar la incorporación de elementos SIGRIP (debida diligencia, función de cumplimiento, herramientas).

TERCERA LÍNEA DE ASEGURAMIENTO	
Garantiza la efectividad del Sistema de Control Interno. A diferencia de las primeras dos líneas, que están enfocadas en la gestión operativa y el cumplimiento, la tercera línea proporciona una evaluación independiente y objetiva, identifica áreas de mejora y formula recomendaciones a partir de las acciones implementadas por las líneas responsables. Se encarga de realizar la medición de los avances de las acciones de respuesta y evaluación de la política.	
RESPONSABLE	**RESPONSABILIDAD**
Grupo Interno de Trabajo de Control Interno	• Asesorar proactiva y estratégicamente a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. • Asesorar a la primera línea en las metodologías para la identificación y administración de los riesgos y el diseño de controles, en coordinación con la segunda línea de aseguramiento (GIT de Planeación).

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	19 de 50

TERCERA LÍNEA DE ASEGURAMIENTO Garantiza la efectividad del Sistema de Control Interno. A diferencia de las primeras dos líneas, que están enfocadas en la gestión operativa y el cumplimiento, la tercera línea proporciona una evaluación independiente y objetiva, identifica áreas de mejora y formula recomendaciones a partir de las acciones implementadas por las líneas responsables. Se encarga de realizar la medición de los avances de las acciones de respuesta y evaluación de la política.	
	• Recomendar mejoras a la política para la administración del riesgo. • Evaluar la efectividad de los controles para evitar la materialización de riesgos. • Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. • Proponer esquemas de asesoría y acompañamiento articuladas con el GIT de Planeación, en el marco del Plan Anual de Auditorías y Seguimientos. • Articularse con la GIT de Planeación y el GIT de Apoyo Informático, para compartir información y análisis de contraste que permita monitorear la exposición de la Entidad al riesgo y realizar recomendaciones de forma integral con alcance preventivo. • Comunicar al Comité Institucional de Coordinación de Control Interno los posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. • Evaluar la coherencia entre el apetito, tolerancia y niveles de riesgo residual. • Verificar la pertinencia y confiabilidad de los KPI y KRI junto con sus umbrales. • Revisar la implementación del SIGRIP/PTEP y del diagnóstico de madurez COSO-ERM.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	20 de 50

TERCERA LÍNEA DE ASEGURAMIENTO	
Garantiza la efectividad del Sistema de Control Interno. A diferencia de las primeras dos líneas, que están enfocadas en la gestión operativa y el cumplimiento, la tercera línea proporciona una evaluación independiente y objetiva, identifica áreas de mejora y formula recomendaciones a partir de las acciones implementadas por las líneas responsables. Se encarga de realizar la medición de los avances de las acciones de respuesta y evaluación de la política.	
	• Realizar la Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.

6. METODOLOGÍA APLICADA

La Contaduría General de la Nación adopta para la administración del riesgo la metodología establecida por el Departamento Administrativo de la Función Pública (DAFP) en el documento denominado: "Guía para la Gestión Integral del Riesgo en Entidades Públicas" – Versión 7 que establece los pasos metodológicos aplicables de i) identificación y descripción del riesgo, ii) análisis del riesgo inherente, iii) diseño y análisis de controles y iv) valoración del riesgo residual, generales para todas las tipologías de riesgo establecidas en la CGN, así como la Metodología General Ajustada (MGA WEB). Estos documentos, emitidos por entidades del orden nacional, proporcionan los lineamientos necesarios para una gestión estructurada, coherente de los riesgos, alineada con los objetivos institucionales.

Adicional a lo anterior, para la administración de los riesgos de seguridad de la información y ciberseguridad, la entidad da cumplimiento a lo establecido en la norma ISO/IEC 27001 junto con sus anexos en la versión vigente, desde un enfoque sistemático y proactivo buscando salvaguardar la protección de los activos de información, implementando medidas para garantizar la confidencialidad, integridad y disponibilidad de la información.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	21 de 50

En concordancia con lo anterior, el enfoque aplicado es cíclico y participativo, y permite identificar, analizar, valorar y gestionar los riesgos de forma continua. En este sentido, la entidad ha definido que el paso a paso es el mismo para todos los riesgos, por tratarse de una política integral del riesgo. A través de este proceso, la Entidad fortalece la toma de decisiones, anticipa situaciones críticas y promueve una cultura de prevención y mejora permanente.

A continuación, se presentan las etapas que componen este ciclo, junto con una breve descripción de cada una.

Fuente: Elaboración propia a partir de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7 y la NTC ISO 31000:2018 gestión del riesgo. Directrices

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	22 de 50

Política de administración del riesgo: expresa el compromiso de la alta dirección frente a la gestión de riesgos, estableciendo los principios y lineamientos que orientan las acciones institucionales para anticipar, mitigar y responder adecuadamente ante posibles amenazas.

Identificación de riesgos: consiste en reconocer los eventos o situaciones que podrían afectar el cumplimiento de los objetivos institucionales. Se analizan tanto factores internos como externos, considerando el contexto estratégico, los procesos operativos y los proyectos en ejecución.

Para los riesgos de seguridad de la información y ciberseguridad, la identificación inicia con la identificación y clasificación de los activos de información y activos digitales de la Entidad, con el fin de determinar su criticidad, consecuencias, amenazas, vulnerabilidades, causas, eventos e impactos potenciales sobre la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de la operación y el cumplimiento de los objetivos institucionales.

Asimismo, estos riesgos identificados deberán contar con un código único de identificación, construido de la siguiente manera:

- Dos (2) últimas cifras del año de identificación del riesgo.
- Sigla del proceso responsable o dueño del riesgo.
- Sigla de la Entidad.
- Número consecutivo del riesgo.

AA + SIGLA DEL PROCESO + SIGLA ENTIDAD + CONSECUTIVO

La identificación de los riesgos de Integridad Pública se realiza considerando, como parte del análisis, los riesgos de gestión, la gestión preventiva del riesgo fiscal y los riesgos de seguridad de la información y ciberseguridad. Para la definición de los riesgos de Integridad Pública se

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	23 de 50

deben considerar, además, aspectos específicos como las actividades contempladas en los procedimientos establecidos en el SIGI que impliquen intercambio o manejo de recursos; el análisis detallado de las tareas previstas en dichos documentos; y la identificación de áreas susceptibles de generar consecuencias legales, impactos económicos o afectaciones reputacionales para la entidad.

Análisis y valoración de riesgos: busca comprender la naturaleza de cada riesgo identificado. Para ello, se evalúa su probabilidad de ocurrencia y su impacto potencial, se clasifican según su severidad (riesgo inherente y residual) y se identifican los controles existentes.

El análisis de riesgos de Seguridad de la Información y ciberseguridad se desarrolla a partir de los activos de información priorizados, considerando los procesos, servicios, tecnologías, personas y recursos asociados que puedan verse afectados por amenazas y vulnerabilidades identificadas en el contexto institucional.

Durante esta actividad se realiza la valoración del impacto potencial que tendría la materialización del riesgo sobre la entidad, considerando aspectos operacionales, reputacionales, legales, financieros, tecnológicos y de prestación del servicio, sin tener en cuenta inicialmente la efectividad de los controles existentes, con el propósito de determinar el nivel de riesgo inherente.

La valoración del riesgo de seguridad consiste en identificar, analizar y evaluar los controles existentes asociados a los riesgos de Seguridad de la Información y ciberseguridad, con el fin de determinar su capacidad para reducir la probabilidad de ocurrencia y/o el impacto de los eventos de riesgo identificados.

Los controles deberán relacionarse con las amenazas, vulnerabilidades,

causas y escenarios de riesgo previamente identificados, garantizando que su diseño, implementación y propósito contribuyan efectivamente a la protección de los activos de información y al cumplimiento de los objetivos institucionales.

Durante esta etapa se evaluará la efectividad, eficiencia y nivel de implementación de los controles existentes, así como la necesidad de establecer controles adicionales o fortalecer los actuales. Como resultado del proceso, se determinará el nivel de riesgo residual, entendido como el nivel de riesgo que permanece después de aplicar los controles existentes y las medidas de tratamiento definidas, permitiendo priorizar acciones y orientar la toma de decisiones para la gestión adecuada de los riesgos institucionales.

Tratamiento de riesgos: implica definir las acciones que se deben implementar para reducir, eliminar o aceptar los riesgos residuales. Esta etapa orienta la toma de decisiones sobre el manejo adecuado de los riesgos priorizados.

Para los riesgos de seguridad es importante la implementación oportuna de controles y planes de tratamiento que contribuyan a reducir la probabilidad e impacto de eventos que puedan afectar los objetivos institucionales, la operación, la información de la Entidad y contribuyan a la protección de los activos de información, activos digitales y servicios tecnológicos.

Para la definición de los controles se deberán considerar los lineamientos institucionales y los controles aplicables establecidos en el Anexo A de la ISO/IEC 27001:2022, asegurando la efectividad de las medidas implementadas y su contribución al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI)

Monitoreo y revisión: se realiza de forma continua por las tres líneas de aseguramiento, con énfasis en las responsabilidades de la primera y

segunda línea. Permite verificar si los riesgos están siendo gestionados conforme a lo planeado y si los controles aplicados son eficaces.

Evaluación: Aunque esta actividad involucra a las diferentes líneas de defensa, la evaluación se encuentra a cargo principalmente de la tercera línea de aseguramiento. Esta etapa garantiza una visión independiente sobre la efectividad del sistema de gestión de riesgos, permitiendo recomendar ajustes o mejoras.

En seguridad de la información, la evaluación permite determinar la efectividad de los controles implementados y establecer si el nivel de riesgo residual se encuentra dentro de los niveles de aceptación definidos por la CGN. Para ello, se considera tanto la probabilidad de ocurrencia como el impacto potencial sobre los activos de información, los servicios tecnológicos, la continuidad de la operación y el cumplimiento de los objetivos institucionales.

Comunicación y Consulta: es un proceso transversal que asegura que la información relacionada con los riesgos fluya de manera oportuna y comprensible. Favorece la participación de todos los actores y fortalece la cultura de gestión del riesgo dentro de la entidad.

Nota: para llevar a cabo las etapas metodológicas descritas, se implementarán diversas herramientas de control, destacando la Matriz de Riesgos de Gestión, Fiscales y de Integridad Pública en su versión vigente.

7. CONTEXTO

Para la identificación de los riesgos que podrían impactar su desempeño, la Entidad realizó en el marco de su planeación estratégica, un análisis de su entorno estratégico, considerando factores internos y externos que podrían influir en la consecución de los objetivos institucionales.

Contexto externo

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	26 de 50

En cuanto al contexto externo, la Entidad identificó los siguientes factores:

- **Competitivos:** se evaluaron aspectos como la imagen corporativa, las alianzas con instituciones públicas y privadas para ejecutar programas y proyectos, el apoyo de la cooperación internacional, así como la participación en eventos académicos y profesionales. Asimismo, se tuvo en cuenta la cultura contable, el conocimiento institucional y el posicionamiento de la CGN.
- **Sociales:** se destacó la inestabilidad e informalidad laboral en el país, la disminución de la oferta de personal calificado, la falta de información requerida y las situaciones de orden público que podrían afectar el cumplimiento de las funciones de la entidad.
- **Económicos:** se identificó el recorte presupuestal como un factor de riesgo que podría limitar la capacidad operativa de la Entidad.
- **Tecnológicos:** se consideraron tanto oportunidades como riesgos derivados de la automatización de procesos, los posibles ciberataques a los sistemas de información, los cambios tecnológicos, la escasez de proveedores de tecnología y la disponibilidad presupuestal para estos recursos.
- **Políticos:** se analizó la credibilidad en las instituciones del Estado, los cambios en la política general que afectan a la entidad, la estabilidad política y las normas que podrían afectar el cumplimiento de los objetivos de la entidad.
- **Ambientales:** incluye el entorno natural, el cambio climático y la ecología que podría impactar la misión y funciones de la entidad.
- **Geográficos:** se evaluó el nivel de desarrollo económico y social de las regiones que rodean la entidad.
- **Obligaciones generales de la entidad:** incluye la fuente legal, reglamentaria y sus posibles cambios, contractual, extracontractual u obligaciones profesionales. Agrupa los deberes (obligatorio cumplimiento), expectativas de las partes interesadas (cumplimiento facultativo) y compromisos (cumplimiento asumido).

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	27 de 50

Contexto interno

En relación con el contexto interno, la Entidad consideró los siguientes aspectos clave:

- **Capacidad Directiva:** se valoró la imagen que proyecta la alta dirección, la claridad en los planes estratégicos y operativos, la orientación institucional hacia el cumplimiento de la misión, así como la estructura organizacional y los mecanismos de toma de decisiones y control directivo sobre la operación.
- **Capacidad del Talento Humano:** se identificaron factores como la rotación de personal, la habilidad para atraer y retener talento calificado, el nivel de competencias del personal, la motivación y el sentido de pertenencia de los servidores públicos, además de los programas de formación y desarrollo profesional.
- **Capacidad Tecnológica:** se evaluó la capacidad de innovación de la entidad, la resistencia al cambio, la actualización e integración de sistemas, así como la seguridad de las plataformas tecnológicas y la competencia técnica de la entidad para ejecutar sus procesos.
- **Capacidad Competitiva**: se analizó la cultura contable que genera la CGN, el índice de desempeño, el impacto de los bienes y servicios entregados por la entidad a sus grupos de interés, la capacidad para ejecutar proyectos, la cultura organizacional, el conocimiento oportuno y capacidad de atención a las quejas y reclamos de los grupos de interés, la eficiencia de los procesos y servicios que presta o suministra la entidad, y la obtención de certificaciones en normas de calidad.
- **Capacidad Financiera**: se revisaron los niveles de eficiencia y eficacia en la ejecución presupuestal, el déficit o superávit acumulado o proyectado, así como la estructura de ingresos y gastos de la entidad.

8. NIVELES PARA CALIFICAR LA PROBABILIDAD

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	28 de 50

A continuación, se presentan los criterios de probabilidad que aplican para los riesgos de gestión, fiscal, riesgos para la Integridad Pública, de Seguridad de la Información y Ciberseguridad.

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas V7.

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo. Está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. En ese sentido, la probabilidad se calcula considerando la frecuencia con la que el proceso o actividad se ve expuesto al riesgo durante un periodo de un (1) año. De esta manera, se mide el número de veces que se presenta la oportunidad de materialización del riesgo en dicho periodo.

A continuación, se presentan los criterios de probabilidad que aplica para los riesgos de proyectos.

	Valor de la probabilidad
Raro	1
Improbable	2
Moderado	3
Probable	4
Casi seguro	5

Fuente: Metodología General Ajustada para Proyectos de Inversión – DNP

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	29 de 50

En los riesgos de seguridad de la información y ciberseguridad, los niveles para calificar la probabilidad son:

Nivel	Frecuencia de la Actividad	Probabilidad	Valor
Muy Baja	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años	1
Baja	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años	2
Media	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años	3
Alta	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año	4
Muy Alta	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año	5

Fuente: Elaboración propia

9. NIVELES PARA CALIFICAR EL IMPACTO

En los riesgos de gestión, fiscal, riesgos para la Integridad Pública y de Seguridad de la Información y ciberseguridad los niveles para calificar el impacto son los siguientes:

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	30 de 50

Nivel	Afectación económica	Reputacional*
Leve 20%	Afectación menor o igual a 10 SMLV	El riesgo afecta la imagen de algún área de la entidad
Menor 40%	Mayor a 10 y menor a 50 SMLV	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 y menor a 100 SMLV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Mayor a 100 y menor a 500 SMLV	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 SMLV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas V7
Nota: este aspecto no aplica para los riesgos fiscales.

Impacto	Descriptor
Moderado	Genera medianas consecuencias sobre la entidad.
Mayor	Genera altas consecuencias sobre la entidad.
Catastrófico	Genera consecuencias muy graves para la entidad.

Fuente: Elaboración propia

En los riesgos de proyectos, los niveles para calificar el impacto son:

Impacto	Valor del impacto
Insignificante	1
Menor	2
Moderado	3
Mayor	4
Catastrófico	5

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	31 de 50

En los riesgos de seguridad de la información y ciberseguridad, los niveles para calificar el impacto son:

Nivel del impacto	Consecuencias Cualitativas	Valor
LEVE 20%	* Sin afectación de la integridad. * Sin afectación de la disponibilidad. * Sin afectación de la confidencialidad.	**1**
MENOR 40%	* Afectación leve de la integridad. * Afectación leve de la disponibilidad. * Afectaciones leves de la confidencialidad.	**2**
MODERADO 60%	* Afectación moderada de la integridad por interés de empleados y terceros. * Afectación moderada de la disponibilidad por interés de empleados y terceros. * Afectación moderada de la confidencialidad por interés de empleados y terceros.	**3**
MAYOR 80%	* Afectación grave de la integridad por interés de los empleados y terceros. * Afectación grave de la integridad debido al interés de los empleados y terceros. * Afectación grave de la confidencialidad debido al interés de los empleados y terceros.	**4**
CATASTRÓFICO 100%	* Afectación muy grave de la integridad por interés de los empleados y terceros. * Afectación muy grave de la disponibilidad por interés de los empleados y terceros. * Afectación muy grave de la confidencialidad por interés de los empleados y terceros.	**5**

Fuente: Elaboración propia

10. NIVELES DE ACEPTACIÓN DEL RIESGO

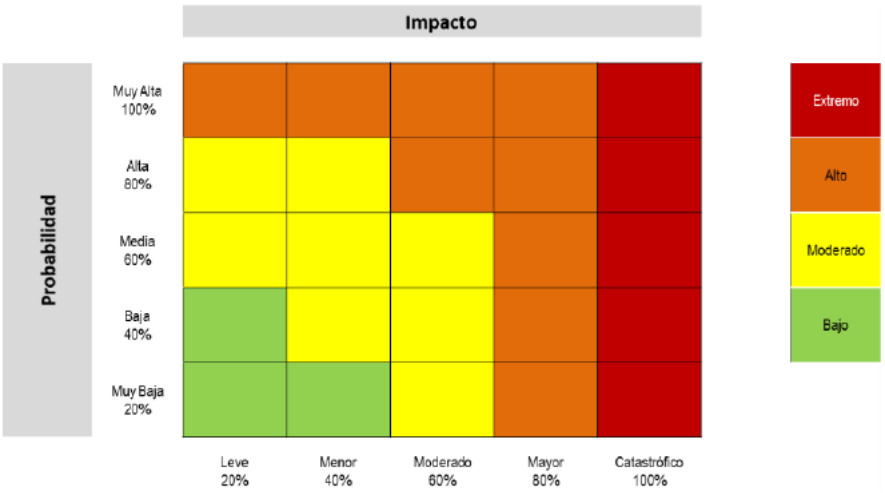
Para el caso de los riesgos de gestión, fiscales, proyectos y de seguridad de la información y ciberseguridad se consideran ACEPTABLES aquellos ubicados en nivel de riesgo bajo. Este concepto es aplicable a partir del resultado de valuación de controles y la obtención del riesgo residual, según la tipología a la cual le aplique.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	32 de 50

Los riesgos para la Integridad Pública y los de incumplimiento legal o regulatorio **NO TIENEN** nivel de aceptación, es decir la tolerancia es cero.

11. NIVELES DE SEVERIDAD DE LOS RIESGOS

Para los riesgos de la CGN se determinaron los siguientes niveles de severidad a través de la combinación entre la probabilidad y el impacto. Esto dio como resultado las 4 zonas de severidad en la matriz de calor que se muestra a continuación.



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas V7.

12. ESTRATEGIAS PARA COMBATIR EL RIESGO

Las estrategias para la mitigación de riesgos, incluyendo los Riesgos para la Integridad Pública, son establecidas por la primera línea de aseguramiento. En la CGN, estas opciones están orientadas a la toma de decisiones que permitan gestionar eficazmente los riesgos, a través de las siguientes acciones:

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	33 de 50

- **Reducir el riesgo:** El riesgo debe ser gestionado mediante la implementación de controles que permitan reevaluar el riesgo residual como aceptable para la entidad. Estos controles suelen reducir la probabilidad y/o el impacto del riesgo, minimizando sus efectos.

    - Transferir el riesgo: Tras un análisis, puede considerarse que la mejor estrategia es externalizar el proceso o transferir el riesgo mediante pólizas. En este caso, la responsabilidad económica recae sobre un tercero, aunque la responsabilidad reputacional sigue siendo de la entidad.
    - Mitigar el riesgo: Tras evaluar los niveles de riesgo, se implementan acciones para reducir su nivel. Esto no necesariamente implica añadir nuevos controles, sino realizar ajustes que disminuyan los efectos del riesgo.

- **Aceptar el riesgo:** Cuando el nivel de riesgo cumple con los criterios establecidos de aceptación, no se implementan controles adicionales y el riesgo es considerado aceptable. Esta estrategia aplica principalmente a los riesgos inherentes en la zona de bajo riesgo, aunque no se permite aceptar ningún riesgo relacionado con la corrupción. (Ningún riesgo para la Integridad Pública podrá ser aceptado)

- **Evitar el riesgo:** Si los escenarios de riesgo identificados se consideran demasiado extremos o inaceptables, se puede optar por evitar el riesgo, eliminando actividades o procesos que lo generen.

Para asegurar el logro de los objetivos institucionales, las actividades de control están orientadas tanto a prevenir como a detectar la materialización de los riesgos. La efectividad de estas actividades depende de la medida en que se logren los objetivos estratégicos y operativos de la Entidad.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	34 de 50

Es responsabilidad de la primera línea de aseguramiento establecer las actividades de control, lo que implica equilibrar los costos y los esfuerzos necesarios para su implementación, en relación con los beneficios finales esperados. Por lo tanto, para la implementación de acciones y controles, es esencial considerar aspectos como la viabilidad jurídica, técnica, institucional, financiera y económica, así como realizar un análisis de costo-beneficio.

De acuerdo con lo anterior, se presentan a continuación las opciones de tratamiento para cada nivel de riesgo:

Nivel de Exposición del Riesgo	Opción de Tratamiento	Detalle del Tratamiento
ZONA DE RIESGO EXTREMO	Reducir: Mitigar	Se deberán implementar inmediatamente las acciones que conlleven a reducir el riesgo. Las acciones preventivas tomadas deberán llevar a la implementación de nuevos controles que prevengan la materialización del riesgo y a mitigar el impacto.
ZONA DE RIESGO ALTO	Reducir: Mitigar o Transferir	Se deberán implementar acciones que conlleven a mitigar o transferir el riesgo. Se deberán implementar acciones preventivas que conlleven a mejorar o documentar los controles existentes.
ZONA DE RIESGO MODERADO	Reducir: Mitigar o Transferir	Se deberán implementar acciones que conlleven a reducir el riesgo. Se deberán implementar acciones preventivas que conlleven a fortalecer los controles existentes.
ZONA DE RIESGO BAJO	Aceptar	Se debe realizar seguimiento a los riesgos con el fin de verificar su impacto, probabilidad y la valoración de los controles.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas V7.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	35 de 50

13. MATERIALIZACIÓN DE RIESGOS

La siguiente tabla presenta las acciones a seguir por parte de para cada una de las líneas de aseguramiento en caso de que se materialice un riesgo.

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
Acciones generales frente a la materialización de riesgos.	1. Realizar el análisis de causas, estableciendo los impactos generados en el proceso y determinando las acciones correctivas, preventivas, y de mejora. Nota: En caso de considerarlo necesario, solicitar el acompañamiento metodológico de la segunda línea de aseguramiento.	1. El GIT de Planeación o el GIT de Apoyo Informático con apoyo del Oficial de Seguridad y Privacidad de la Información (según aplique) deben revisar el análisis de causas y las acciones correctivas de los Planes de Mejoramiento planteados por la primera línea de aseguramiento, y realizar las recomendaciones que permitan asegurar	1. Evaluar la efectividad de las acciones implementadas por la primera línea de aseguramiento. 2. Evaluar la efectividad de los controles planteados por la primera línea de aseguramiento sean efectivos, le apunten al riesgo y estén	1. El Comité Institucional de Coordinación de Control Interno - CICCI deberá realizar el monitoreo y seguimiento correspondiente del impacto generado, con el fin de tomar las acciones correspondientes que permitan asegurar el cumplimiento de los objetivos y metas institucionales. Lo anterior a partir de

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	36 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	2. Informar al GIT de Planeación como segunda línea de aseguramiento, sobre la materialización del riesgo. 3. Remitir al GIT de Planeación para su revisión, el Plan de Mejoramiento que incluya: análisis de causas, la evaluación de los impactos de la materialización del riesgo y las acciones correctivas propuestas por el proceso o proyecto, para mitigar el impacto	que los controles estén bien diseñados. 2. El GIT de Planeación o el GIT de Apoyo Informático con apoyo del Oficial de Seguridad y Privacidad de la Información (según aplique) deben presentar el Plan de Mejoramiento de la materialización del riesgo en el CICCI, el cual debe incluir como mínimo: la descripción del hallazgo, el tipo de hallazgo u observación, análisis de causa, descripción de la acción a realizar, el producto esperado, fecha iniciación de la acción, fecha	funcionando en forma adecuada. 3. Verificar y evaluar la efectividad de las acciones implementadas en el Plan de Mejoramiento.	los informes presentados por la segunda y tercera línea de aseguramiento. 2. Adoptar las acciones que considere pertinentes, las cuales serán de obligatorio cumplimiento para cada una de las líneas de aseguramiento. 3. Impartir lineamientos orientados a prevenir que el riesgo se vuelva a materializar.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	37 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	y evitar que el riesgo se vuelva a materializar. 4. Atender las recomendaciones realizadas por la segunda y tercera línea, para la identificación de riesgos. 5. Revisar y ajustar los controles existentes. De ser necesario, establecer nuevos controles asociados al riesgo materializado, teniendo en cuenta el Plan de Mejoramiento definido.	finalización de la acción, responsable de la acción, seguimiento y el estado. 3. Realizar seguimiento a las acciones de monitoreo implementadas por la primera línea de aseguramiento. 4. Verificar el cumplimiento de las acciones planteadas en el Plan de Mejoramiento y se actualizó el Mapa de Riesgos correspondiente.		

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	38 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	6. Revisar y actualizar el Mapa de Riesgos correspondiente, en particular las causas, riesgos y controles, estableciendo acciones preventivas y de mejora. 7. Dar cumplimiento estricto al Plan de Mejoramiento propuesto.			
Acciones específicas respecto a los Riesgos para la Integridad Pública frente a su materialización	1. Revisar las causas asociadas a la materialización del Riesgo para la Integridad Pública y adoptar las medidas	1. El GIT de Planeación debe revisar el Mapa de Riesgos para la Integridad Pública, en particular, las causas, riesgos y controles.	1. Verificar y evaluar la efectividad de las acciones planteadas en el Plan de Mejoramiento.	1. Una vez surtido el conducto regular establecido por la Entidad y dependiendo del alcance (normatividad

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	39 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	correspondientes para evitar el mayor impacto. 2. Establecer nuevos controles que permitan prevenir que se vuelva a materializar. 3. Solicitar el acompañamiento del GIT de Jurídica para determinar la pertinencia de adelantar las indagaciones correspondientes.	2. El GIT de Planeación debe llevar a cabo un monitoreo de los procesos que han materializado riesgos. 3. El GIT de Planeación debe consolidar y publicar en la página web de la CGN, el Mapa de Riesgos para la Integridad Pública actualizado.	2. Verificar y evaluar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los Riesgos para la Integridad Pública. 3. Verificar si se tomaron las acciones y se actualizó el mapa de Riesgos para la Integridad Pública.	asociada al hecho de corrupción materializado), analiza y determina la aplicabilidad del proceso disciplinario e informa a la instancia respectiva. 2. Informar a las autoridades correspondientes de la ocurrencia de un hecho de corrupción.
Acciones específicas respecto a los riesgos de seguridad de la información, y	1. En caso de materialización de un riesgo de seguridad digital y ciberseguridad, se debe informar,	1. El GIT de Apoyo Informático con apoyo del Oficial de Seguridad y Privacidad de la Información de la	1. Verificar y evaluar el diseño e idoneidad de los controles y si son adecuados para	No aplica.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	40 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
ciberseguridad frente a su materialización	adicionalmente, al GIT de Apoyo Informático y al Oficial de Seguridad y Privacidad de la Información de la CGN. 2. En la elaboración de los controles para mitigar o tratar el riesgo, se debe tener en cuenta lo establecido en "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se	CGN, debe supervisar y acompañar el proceso de implementación de los Planes de Mejoramiento, verificando que la primera línea de aseguramiento ejecute las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado. 2. El GIT de Apoyo Informático con apoyo del Oficial de Seguridad y Privacidad de la Información debe efectuar la evaluación de los Planes de	prevenir o mitigar los riesgos. 2. Considerar la pertinencia de priorizar en el Plan Anual de Auditorías y Seguimientos la evaluación a la efectividad del Plan de Contingencia y Tratamiento de Incidentes de Seguridad de la Información, Seguridad Digital y ciberseguridad. 3. Emitir recomendaciones orientadas a fortalecer los controles de seguridad digital	

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	41 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	ajusten al análisis de riesgos. 3. Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información, seguridad digital y ciberseguridad que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar tanto en el Plan de Mejoramiento como en el registro de los incidentes de	Mejoramiento, realizar nuevamente la valoración de los riesgos de seguridad de la información y ciberseguridad para verificar su efectividad, y realizar la actualización de los Mapas de Riesgo de Seguridad de la información, digital y ciberseguridad. 3. El GIT de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información debe actualizar el registro de los incidentes de seguridad digital y ciberseguridad que se hayan materializado, con el fin de analizar	y minimizar vulnerabilidades en los sistemas de información.	

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	42 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	seguridad digital y ciberseguridad. 4. Realizar los correctivos necesarios frente a los usuarios e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existentes, documentar en el Plan de Mejoramiento Institucional y actualizar el Mapa de Riesgos de Seguridad de la	las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar, según lo indicado en los lineamientos para la gestión del riesgo de seguridad digital y ciberseguridad. 4. El GIT de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información debe garantizar la capacitación continua a los colaboradores sobre seguridad de la información, digital y ciberseguridad, sensibilizando el manejo seguro de la		

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	43 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	información y ciberseguridad. 5. Implementar buenas prácticas de seguridad digital, tales como el uso de contraseñas seguras, el manejo adecuado de la información confidencial y la protección contra ataques de ingeniería social.	información y la prevención de ataques cibernéticos.		
Acciones específicas respecto a los riesgos fiscales frente a su materialización	1. Realizar los correctivos necesarios e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de	1. El GIT de Planeación debe llevar a cabo un monitoreo de los procesos que han materializado riesgos. 2. Presentar a la Línea Estratégica un reporte relacionado con las observaciones	1. Verificar y evaluar la efectividad de las acciones planteadas en el Plan de Mejoramiento.	1. Analizar y determinar la pertinencia de compulsar la información a la instancia correspondiente interna o externa, con el fin de que se indaguen las

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	44 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	mejora, así como la revisión de los controles existentes, documentar en el Plan de Mejoramiento Institucional y actualizar el Mapa de Riesgos. 2. Solicitar el acompañamiento del GIT de Jurídica para analizar los hechos constitutivos de la materialización del riesgo fiscal y adoptar las acciones correspondientes. 3. Presentar a la segunda línea de	detectadas en el monitoreo del riesgo materializado.	2. Verificar y evaluar el diseño y efectividad de los controles, si se encuentran orientados a mitigar los riesgos fiscales y presentar a la línea estratégica las recomendaciones que se consideren pertinentes. 3. Verificar si se tomaron las acciones y se actualizó el mapa de riesgos en lo relacionado con los riesgos fiscales.	circunstancias que dieron lugar a la materialización del riesgo fiscal.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	45 de 50

	Primera Línea de aseguramiento	Segunda Línea de aseguramiento	Tercera Línea de aseguramiento	Línea Estratégica
	aseguramiento un informe detallado sobre los hechos y causas constitutivas de la materialización del riesgo fiscal y las acciones y decisiones adoptadas con el acompañamiento del GIT de Jurídica			

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	46 de 50

14. MONITOREO Y REVISIÓN

Primera línea de aseguramiento:

La primera línea de aseguramiento (líderes de los procesos) será responsable de elaborar la matriz de riesgos, para lo cual deberá identificar los riesgos, analizar las causas y establecer acciones que están directamente relacionadas a mitigar las causas y los riesgos establecidos de manera coherente, realizar el monitoreo y la revisión periódica de la aplicación de los controles establecidos para la gestión de riesgos con una periodicidad mínimo trimestral. De igual manera, incorporar seguimiento a Indicadores Clave de Riesgo (KRI) articulados con KPI, definiendo umbrales de alerta alineados con el apetito y tolerancia al riesgo; los resultados deberán reportarse en el marco del esquema de líneas de aseguramiento.

Este ejercicio debe concretarse en un informe que incluya:

- El seguimiento a los riesgos identificados.
- La aplicación de los controles.
- Avance en la implementación de los planes de acción.
- Registro de la materialización de riesgos.
- Reporte de novedades relevantes relacionadas con la gestión del riesgo.
- El comportamiento de KRIs priorizados, análisis de tendencias y acciones preventivas cuando se acerquen o excedan los umbrales.

El informe deberá remitirse al GIT de Planeación y, en el caso de riesgos asociados a seguridad de la información, se deberá remitir al GIT de Apoyo Informático y al Oficial de Seguridad y Privacidad de la Información, dentro de los primeros diez (10) días hábiles del mes siguiente al cierre de cada trimestre.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	47 de 50

Lo anterior, teniendo en cuenta los siguientes cortes trimestrales:

- Primer trimestre: 31 de marzo
- Segundo trimestre: 30 de junio
- Tercer trimestre: 30 de septiembre
- Cuarto trimestre: 31 de diciembre

Segunda línea de aseguramiento:

El GIT de Planeación y el GIT de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información (para riesgos de seguridad de la información y ciberseguridad) realizarán trimestralmente el seguimiento al monitoreo reportado por la primera línea de aseguramiento mediante el análisis de una muestra aleatoria de procesos. A partir de esta revisión, emitirán observaciones, alertas y recomendaciones, dentro del mes siguiente al respectivo corte.

Asimismo, establecer el mecanismo de comunicación y reporte de KRIs: consolidación por segunda línea, revisión/retroalimentación por tercera línea y análisis/aprobación de ajustes de umbrales por la Línea Estratégica (CICCI u instancia equivalente).

15. EVALUACIÓN

El GIT de Control Interno (Tercera Línea de aseguramiento) realizará la evaluación de los riesgos de la entidad en el marco de las auditorías internas o seguimientos incluidos en el Plan de Auditoría y Seguimiento aprobado por el Comité Institucional de Coordinación de Control Interno para cada vigencia. También, verificará el apetito/tolerancia y su cumplimiento, pertinencia y confiabilidad de KRIs/KPIs, así como la revisión del avance del diagnóstico de madurez (COSO-ERM) y planes de mejora.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	48 de 50

La evaluación a los Riesgos para la Integridad Pública tendrá una periodicidad semestral; el informe de los resultados se realizará y se publicará en la página web de la Entidad en las siguientes fechas:

- Primer seguimiento: con corte al 30 de junio. En esa medida, la publicación del informe deberá surtirse dentro del mes de agosto.
- Segundo seguimiento: con corte al 31 de diciembre. La publicación del informe deberá surtirse dentro del mes de febrero de la siguiente vigencia.

Es importante precisar que, la evaluación incluye el monitoreo y reporte de primera línea, así como el seguimiento de segunda línea, los cuales se emiten en el mes siguiente a la fecha de corte; en ese sentido, la realización y publicación del informe de evaluación de la tercera línea se efectuará en los meses de agosto y febrero.

Con relación a los riesgos de gestión, fiscal, de seguridad de la información y Ciberseguridad y proyectos, el GIT de Control Interno podrá incluir una muestra aleatoria dentro de la evaluación semestral a los Riesgos para la Integridad Pública.

En todo caso, dichos riesgos deberán ser evaluados mínimo una (1) vez al año, para lo cual, el GIT de Control Interno dentro de su independencia, podrá establecer la metodología que considere pertinente, con el fin de garantizar la evaluación de la mayor cantidad de riesgos de gestión, fiscal, de seguridad de la información y ciberseguridad y proyectos.

Adicionalmente, en el desarrollo del Plan Anual de Auditorías y Seguimientos, el GIT de Control Interno evaluará los riesgos asociados a los procesos, procedimientos, proyectos y políticas objeto de las auditorías o evaluaciones e informes de ley.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	49 de 50

16. DIVULGACIÓN

La Política de Administración del Riesgo y los mapas de riesgos correspondientes (gestión, fiscales, integridad pública, seguridad de la información, ciberseguridad y de proyectos) se divulgarán a través de la página web de la Contaduría General de la Nación, con el fin de dar a conocer la gestión realizada por los procesos a todas las partes interesadas. Asimismo, se asegurará su publicación de conformidad con los lineamientos del Programa de Transparencia y Ética Pública (PTEP).

17. CAPACITACIÓN

La administración del riesgo es un eje fundamental para el cumplimiento de los objetivos institucionales. Por tanto, se deberá garantizar, como mínimo, la realización de una capacitación anual (ya sea de carácter interno o externo) dirigida a los servidores públicos.

Esta formación permitirá fortalecer sus competencias y asegurar una administración del riesgo coherente, eficaz y alineada con los procesos de la entidad. Entre otros temas debe incluir contenidos sobre: SIGRIP/PTEP (integridad pública), apetito/tolerancia/capacidad de riesgo, niveles de madurez (COSO-ERM), diseño de controles y construcción/uso de KRIs.

Resumen de versiones

Fecha	Versión	Descripción de los cambios
Mayo de 2023	V1	Actualización basada en la Guía para la Administración del Riesgo y diseño de controles en entidades públicas V4 – Departamento Administrativo de la Función Pública (DAFP).
Agosto de 2025	V2	Actualización basada en la Guía para la Administración del Riesgo y diseño de controles en entidades públicas V6 –

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO			
PROCESO:	PLANEACIÓN INTEGRAL		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
08/07/2026	PI-POL02	03	50 de 50

		Departamento Administrativo de la Función Pública (DAFP).
Mayo de 2026	V3	Actualización basada en la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7 – Departamento Administrativo de la Función Pública (DAFP).