IGAC
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Sistema de Gestión Integrado MIPG

SGC
Sistema de Gestión de Calidad

SGA
Sistema de Gestión Ambiental

SGSST
Sistema de Gestión de la Seguridad y Salud en el Trabajo

SGD
Sistema de Gestión Documental

SCI
Sistema de Control Interno

SLNS
Sistema Laboratorio Nacional de Suelos

SGSI
Sistema de Gestión de Seguridad de la Información

IGAC
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Sistema de Gestión Integrado MIPG

Procedimiento

Administración del Riesgo

Código: PC-PRC-03 **Versión:** 2 **Vigente desde:** 21/05/2024

1. OBJETIVO

Establecer las actividades requeridas para la administración del riesgo que incluye, la identificación de cuestiones internas y externas a través del análisis de las herramientas estratégicas definidas por la entidad e identificar, analizar, valorar y tratar los riesgos en los procesos del IGAC, con el fin de determinar los controles encaminados a reducir y mitigar los riesgos para el logro de los objetivos institucionales y el cumplimiento tanto de requerimientos obligatorios como voluntarios de la entidad.

2. ALCANCE

Inicia con el análisis del contexto estratégico, continúa con la identificación del Riesgo y finaliza con la evaluación a la administración del Riesgo. Este procedimiento aplica a todos los procesos, subprocesos y proyectos del IGAC en la sede central y direcciones territoriales.

3. DEFINICIONES

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.
- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección y del órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:
- **Bien de uso público:** Aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.
- Ejemplos: Las calles, plazas, puentes, vías, parques etc.
- **Bienes fiscales:** Aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección y el órgano de gobierno que no sería posible el logro de los objetivos de la entidad.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata por causa inmediata.
- **Causa raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. Nota: Tratándose de riesgo fiscal, la causa raíz se relaciona con el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Para los riesgos fiscales, es el control accionado en la

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

- **Control detectivo**: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Para los riesgos fiscales es el control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
- **Control fiscal interno (CFI):** Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público.
- **Control fiscal multinivel:** Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación del control social.
- **Control Preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Para los riesgos fiscales es el control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **Gestión del riesgo fiscal:** Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
- **Gestor fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)4" .
- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales".
- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

- **Patrimonio público:** Se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).
- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Punto de Riesgo:** Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, como lo son: aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales.
- **Proyecto**: Es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único, Tiene un principio y un final definidos; El final se alcanza cuando se logran los objetivos del proyecto, los proyectos contienen elementos repetitivos en algunos entregables y actividades del proyecto. En los proyectos pueden existir incertidumbres o diferencias entre productos, servicios o resultados que el proyecto genera, estos se generan en todos los niveles de institución
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).
- **Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001:2022).
- **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.
- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. POLÍTICAS DE OPERACIÓN

4.1 LEGALES

- Leyes.
  - Ley 2195 de 2022: "Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones". Artículo 37.

- Ley 1474 de 2011: "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" Capítulo VI, Articulo 73 "Plan Anticorrupción y de Atención al Ciudadano".
- Ley 610 de 2000: "Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías". Artículo 3°.
- Ley 489 de 1998: "Normas para el ejercicio del control interno en las entidades y organismos del Estado".
- Ley 87 de noviembre de 1993: "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado". Artículo 2 literal a) y f.

° Decretos.
- Decreto 403 de 2020: "Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal". Artículo 4.
- Decreto 1499 del 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 124 del 2016 del Departamento Administrativo de la Presidencia de la República: "Por el cual se sustituye el título 4 de la parte 1 del libro 2 del Decreto 1081 de 2015 relativo al "Plan anticorrupción y de atención al ciudadano".
- Decreto 943 de 2014: "Por el cual se actualiza el Modelo Estándar de Control Interno MECI 2014".
- Decreto 2641 de 2012: "Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011".

4.2 TÉCNICAS RELACIONADAS

° Normas Técnicas.
- NTC ISO 9001:2015 Sistema de Gestión de la Calidad - Requisitos
- NTC ISO 14001:2015 Sistema de Gestión Ambiental - Requisitos.
- NTC-ISO/IEC 27001:2022 Sistemas de Gestión de la Seguridad de la Información
- NTC-ISO 31000:2018 Gestión del Riesgo. Principios y Directrices.

° Otras.
- Guía Técnica Colombiana GTC-ISO/IEC 27002:2022 Código de práctica para controles de seguridad de la información.
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Departamento Administrativo de la Función Pública (DAFP), versión 6 - noviembre de 2022.

4.3 DE PROCEDIMIENTO

° Aplican para este procedimiento los lineamientos definidos en el documento Política de Administración del Riesgo, vigente del IGAC.
° El comité de Coordinación de Control Interno revisará y actualizará, si hay lugar a ello, la política Administración del riesgo por lo menos una vez en el año, preferiblemente en el primer trimestre o cuando sea requerido por alguna circunstancia particular.
° Con el fin de mantener una base histórica de los Riesgos de la entidad, si surge algún cambio frente al mapa de riesgos (crear o eliminar), se debe continuar con la enumeración de los Riesgos ya identificados.
° El mapa de riesgos institucional se actualiza y se publica interna y externamente, a más tardar el 31 de enero de cada vigencia, de acuerdo con los términos establecidos en la normatividad aplicable.
° Dentro de la verificación realizada por la Oficina Asesora de Planeación – OAP al mapa de riesgos institucional, se efectúa el análisis del contexto estratégico de los riesgos, de manera que se determine si es precisa su actualización.
° La identificación, análisis y valoración de riesgos se hará con enfoque de procesos, subprocesos, y proyectos a nivel nacional, no habrá mapas de riesgos por Dirección Territorial, sin embargo se

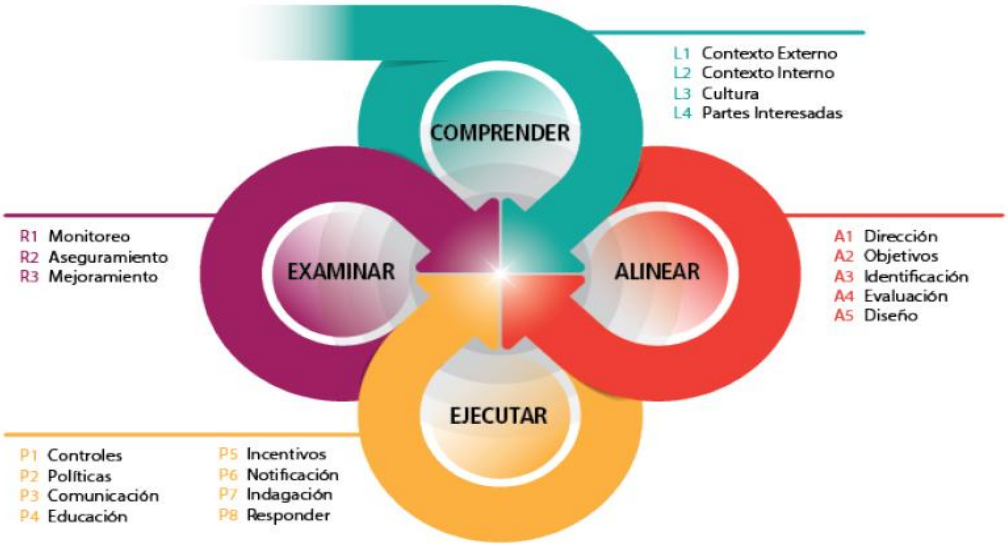
tendrán en cuenta las características y/o condiciones de cada dirección territorial en el análisis y valoración de los riesgos de los procesos en los que intervienen

- Si un riesgo se elimina, se debe contar con la debida justificación del proceso responsable.
- Los Riesgos de Proyectos se desarrollarán en las herramientas dispuestas por la entidad para tal fin. Para los riesgos de seguridad de la información, se hará gestión de riegos sobre los activos de información clasificados con nivel de criticidad "alto", de acuerdo con lo definido en el inventario de activos de información por procesos del Instituto.

4.3.1 GENERALIDADES

Con el fin de dar cumplimiento a los lineamientos establecidos en nuestra Política de Administración del Riesgo vigente, la administración del Riesgo en el IGAC, se desarrolla en el marco de la metodología de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 y se articula con el modelo de capacidades (Gobierno, Riesgo y Cumplimiento – GRC). Por lo anterior la estructura de este procedimiento se alinea con los siguientes componentes y elementos que establece el modelo GRC:

Figura 1. Vista de componentes y elementos del modelo de capacidad GRC



Fuente: Adaptado del Modelo de Capacidad de GRC. Red Book de OCEG. Versión 3.

4.3.2 COMPRENDER

Para la implementación de la gestión del riesgo, es necesario realizar un análisis del contexto estratégico de la entidad para establecer su complejidad, procesos, planeación institucional, entre otros aspectos, lo anterior para conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología y modelo en general.

En este sentido, el Instituto debe actualizar periódicamente el contexto estratégico, con el fin de responder a los nuevos programas, objetivos y metas del Plan Nacional de Desarrollo. Para ello, debe implementar la herramienta integrada de diagnóstico, análisis y toma de decisión.

Esta herramienta integrada se despliega a través de las siguientes herramientas: ✓ Un análisis PESTEL ✓ Un análisis de las cinco fuerzas de PORTER ✓ Un análisis de matriz DOFA ✓ Un análisis EFI y EFE ✓ Un desarrollo y clasificación de estrategias.

4.3.2.1 CUESTIONES A TENER EN CUENTA EN EL ANÁLISIS DEL CONTEXTO EXTERNO

Se debe analizar y entender el contexto externo del negocio en el que la entidad opera. Se describen a continuación los posibles factores que componen las amenazas y oportunidades:

- **Económicos y Financieros**: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
- **Legal y reglamentario**: Se refiere a todo lo establecido por la ley o que esté conforme con ella.
- Ambiental: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible, contaminación.
- **Político**: Cambios de gobierno y administración, políticas públicas, regulación.
- Sociales y Culturales: Demografía, responsabilidad social, orden público, atentados, vandalismo, asalto a la oficina.
- **Tecnológico:** Avances en tecnología, acceso a sistemas de información externos, gobierno digital, suplantación de identidad, virus informáticos, interoperabilidad de los sistemas de información de gobierno, transformación digital.
- **Otro**: Se refiere a una categoría diferente a las mencionadas anteriormente.

4.3.2.2 CUESTIONES A TENER EN CUENTA EN EL ANÁLISIS DEL CONTEXTO INTERNO

Se debe analizar y entender las características o aspectos esenciales del ambiente en el cual el IGAC busca alcanzar sus objetivos. Se debe considerar factores como:

- **Recursos Financieros-Económicos**: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
- **Planeación**: Se refiere al accionar que tiene que ver con políticas, planes, programas y proyectos al interior de la entidad.
- **Talento Humano**: Estructura y cultura organizacional. Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional. Se analiza posible dolo e intención frente a la corrupción, fraude interno (corrupción, soborno). Para el tema de Seguridad de la información, corresponde al personal que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información.
- **Procesos**: Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización. Falta de procedimientos, errores de grabación, autorización, errores en cálculos para pagos internos y externos y falta de capacidad.
- **Tecnología**: Analizar o identificar la infraestructura tecnológica existente en la entidad y el estado de operación de esta.
- **Infraestructura**: Eventos relacionados con la infraestructura física de la entidad. Derrumbes, incendios, inundaciones, daños a activos fijos.
- **Coordinación y Comunicación**: Canales utilizados y su efectividad, así como adecuado y oportuno flujo de la información necesaria para el desarrollo de las operaciones.
- **Otro**: Se refiere a una categoría diferente a las mencionadas anteriormente.

4.3.2.3 CULTURA

Se debe entender la cultura organizacional existente en la entidad y la forma en la que los servidores públicos entienden como la gestión de riesgos impacta de manera directa en el desarrollo de sus actividades y la forma en la que esta gestión soporta la toma de decisiones y el cumplimiento de los objetivos estratégicos.

Por lo anterior se debe impulsar a nivel institucional, una cultura de gestión del riesgo, a través de socializaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.

4.3.2.4 PARTES INTERESADAS

Es importante conocer las necesidades y expectativas de las partes interesadas, debido a su efecto potencial en la capacidad del IGAC, para proporcionar productos y servicios que satisfagan los

requisitos de los usuarios, inherentes, legales y reglamentarios. De esta manera en las caracterizaciones de los procesos, se identificaron sus clientes/usuarios, partes interesadas o grupos de interés y los productos o servicios que se les suministra. Utilizando las caracterizaciones del proceso, se elaboró una matriz general de las partes interesadas en la cual se identifica la necesidad y expectativa de la parte interesada y cómo el proceso y la entidad le da cumplimiento. Esta matriz se debe revisar anualmente y ajustar si hay lugar a ello.

4.3.3 ALINEAR

4.3.3.1 DIRECCIÓN

Se debe establecer la declaración de propuesta de valor, propósito central (misión), objetivo retador (visión), objetivos estratégicos, valores institucionales, objetivos, metas, políticas, y demás directrices para la toma de decisiones. En ese sentido el IGAC ha definido el propósito central (misión), objetivo retador (visión) y los objetivos estratégicos de la entidad, los cuales se revisan periódicamente a partir de un ejercicio de planeación estratégica que permite modelar la proyección de la entidad a corto, mediano y largo plazo, considerando para el efecto el plan nacional de desarrollo, las políticas públicas aplicables al IGAC, los requerimientos, expectativas, necesidades y prioridades de la ciudadanía y las partes interesadas, así como el presupuesto asignado al Instituto, los cuales se encuentran consignados en la página Web e IGACNET. De igual manera desde la Subdirección de Talento Humano se cuenta con una declaración formal de los valores institucionales.

4.3.3.2 OBJETIVOS

La entidad debe analizar los objetivos estratégicos y de los procesos, con el fin de identificar los posibles riesgos que afecten su cumplimiento y que puedan ocasionar su éxito o fracaso.

Es necesario revisar que los objetivos estratégicos y de procesos se encuentren alineados con el propósito central (misión) y objetivo retador (visión), así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo. Pero además, se debe revisar que los objetivos del proceso contribuyan al cumplimiento de los objetivos estratégicos. Los objetivos estratégicos se encuentran disponibles en la página Web e IGACNET.

4.3.3.3 IDENTIFICACIÓN DEL RIESGO

En este elemento, el objetivo es identificar los riesgos que estén o no bajo el control de la entidad, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance, los proyectos, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

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

Figura 2. Estructura para redacción del Riesgo

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

Ejemplo:
Posibilidad de = Afectación económica + por multa y sanción del ente regulador + debido a adquisición de bienes y servicios fuera de los requerimientos normativos.

Descripción del Riesgo Fiscal.
Para redactar un riesgo fiscal se debe tener en cuenta:

- Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
- Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
- Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
- Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

Ejemplo: Posibilidad de efectos dañoso sobre bienes públicos + por pérdida, extravío o hurto de bienes muebles de la entidad + a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén.

Riesgos de Corrupción.
Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:
ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

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

Riesgos Seguridad de la Información.
En la fase de Identificación de riesgos relacionados con seguridad de la información, se analizan las causas del riesgo que podrían comprometer los criterios de confidencialidad, integridad y disponibilidad de la información y los activos de información de la entidad, para lo cual se debe tener en cuenta lo siguiente:

- Flujo de información (entradas, salidas, procesamiento) y la respectiva caracterización de los procesos de la entidad.
- Inventario de activos de información de cada proceso.
- Clasificación de los activos de información de los procesos.
- Identificación de las vulnerabilidades y amenazas asociadas a los activos de información.

Las actividades para ejecutar el análisis de riesgos de gestión relacionados con seguridad de la información son:

- **Identificación de activos de información:** En esta actividad, todos los responsables de procesos del IGAC, deben identificar los activos de información asociados a su proceso. Ver en el listado maestro de documentos, el procedimiento vigente de "*Gestión de Activos de información*" emitido desde el proceso Gestión Estratégica de Tecnología.
- **Identificación del riesgo:** Se podrán identificar los siguientes 3 riesgos inherentes de seguridad de la información:
  - Pérdida de confidencialidad
  - Pérdida de Integridad y

- Pérdida de la disponibilidad.

La identificación de amenazas y vulnerabilidades en este tipo de riesgos, serán realizadas con base en los lineamientos de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, en su capítulo 6 Lineamientos riesgos de seguridad de la información y el Anexo técnico "Modelo de Gestión de Riesgos de seguridad de la información en entidades públicas (Anexo 4 – DAFP)

4.3.4 EJECUTAR

4.3.4.1 CONTROLES

Valoración de controles: Un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

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

Estructura para la descripción del control: La estructura para la descripción del control debe contar con los siguientes variables: responsable de ejecutar el control, acción mediante verbos y el complemento (como se realiza al actividad de control, evidencia, periodicidad, y observaciones o desviaciones de aplicar el control)

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

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

Controles asociados a la seguridad de la información:

Se deben identificar los controles aplicables de acuerdo con el Anexo A. de la norma ISO 27001:2022, y validar su existencia al interior de la entidad y si los mismos se encuentran documentados.

Con base en lo anterior se debe validar la eficacia de los controles existentes, y de comprobar su ineficacia se debe eliminar o reemplazar por otro control más adecuado.

4.3.4.2 INCENTIVOS

Implementar incentivos que motiven conductas deseables y reconocer aquellos que contribuyen a resultados positivos para reforzar las conductas deseadas, en el marco de la administración del Riesgo.

En el IGAC se cuenta con el Plan de Bienestar e Incentivos, en el cual el programa de Incentivos busca reconocer el buen desempeño de los servidores públicos tanto de manera grupal como individual en el cumplimiento de sus labores y en la consecución de resultados de gestión. La formulación de este programa en la entidad está relacionada con otorgar los estímulos necesarios para lograr un mejor desempeño institucional, de esta manera se logra incrementar el sentido de pertenencia en los servidores, la motivación en la ejecución de las actividades orientando su actuar en el compromiso con el logro de Objetivos Estratégicos Institucionales.

4.3.5 NOTIFICACIÓN

4.3.5.1 MATERIALIZACIÓN DE RIESGOS Y LA AUTOEVALUACIÓN A LA ADMINISTRACIÓN DEL RIESGO

Dentro de la autoevaluación realizada por los procesos, subprocesos y direcciones territoriales al seguimiento a los controles, se puede manifestar la materialización de un riesgo, para lo cual se deben tener en cuenta los siguientes elementos:

- Que se cuente con las pruebas (evidencia) que demuestren que el evento denominado como riesgo pasó a ser realidad (Se materializó).
- El registro de la manifestación de materialización del riesgo en las herramientas dispuestas por la entidad.

Acciones ante los riesgos materializados.

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

- Informar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado.
- La OAP revisará la manifestación de materialización del riesgo del proceso o subproceso identificando su lugar de ocurrencia (Sede Centra o Dirección Territorial) en la herramienta para seguimiento de Riesgos.
- Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento.
- Revisar los controles existentes.
- Realizar la valoración del riesgo y actualizar el mapa de riesgos si es necesario.

Acciones para seguir en caso de materialización de riesgos de corrupción.

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

- Informar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado.
- La OAP revisará la manifestación de materialización del riesgo del proceso o subproceso identificando su lugar de ocurrencia (Sede Centra o Dirección Territorial) en la herramienta para seguimiento de Riesgos.
- Informar a las instancias internas (Oficina de Control Interno Disciplinario).
- Informar a las autoridades de la ocurrencia del presunto hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario).
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.

En la herramienta para seguimiento de Riesgos, se realiza el seguimiento en la Sede Central (SC) y Direcciones Territoriales (DT), a la ejecución de controles inmersos en el mapa de riesgos institucional, así como a la materialización de riesgos, por lo menos de forma cuatrimestral, de acuerdo con el cronograma definido por la OAP.

Si por alguna razón un control que debía realizarse no se ejecutó durante el cuatrimestre, se tendrá un concepto no favorable la evaluación realizada por la OCI. Lo anterior aumenta la probabilidad de materialización del Riesgo.

En caso de que exista la no ejecución del control, se deberá registrar en la herramienta para seguimiento de Riesgos la justificación, y si es el caso, adjuntar a la carpeta drive el documento que soporte la no ejecución del control.

Cuando no se presenta la actividad que da origen a la ejecución del control, en el momento de seguimiento, el proceso, subproceso o Dirección Territorial, debe registrar en la herramienta para seguimiento de Riesgos la meta y ejecución en 0 (cero), indicando que para ese periodo no se llevó a cabo el control por dicha situación. El concepto por parte de la OCI para el periodo de seguimiento será "Sin meta asignada para el periodo".

Acciones para seguir en caso de materialización de riesgos de seguridad de información.
Para el caso de materialización de riesgos de seguridad de la información, se debe tener en cuenta los lineamientos establecidos en el procedimiento "gestión de incidentes de seguridad de la información".

4.3.6 INDAGACIÓN

Periódicamente, se debe buscar información para comprender las percepciones acerca del desempeño de la gestión de riesgos y la ocurrencia de hechos y actividades indeseadas. Por anterior se debe establecer varios mecanismos para obtener las opiniones:

- Utilizar reuniones o conversaciones relevantes que se tiene con públicos objetivo (reuniones de empleados, sesiones del CIGD y del CICCI, reuniones con entidades de gobierno, auditorías, etc.) para obtener información.
- Lograr a través de la socialización interna y externa del proyecto de mapa de riesgos institucional, conocer las consideraciones y sugerencias sobre el proyecto del mapa de riesgos institucional; y llevar a cabo los ajustes, modificaciones o incursiones sugeridas, previo a un análisis institucional.
- Definir encuestas frente a la administración del Riesgo, así como el método de entrega de la encuesta, la oportunidad de responder en forma anónima e incentivar por participar. Estas encuestas nos permitirán identificar mejoras frente a la Administración del Riesgo.

5. DESARROLLO

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
1.	Planificar la administración de riesgos para la vigencia.	Definen las actividades para la construcción, actualización y/o ajustes, seguimiento y administración del Mapa de Riesgos Institucional.	Responsable Riesgos Oficina Asesora de Planeación	Plan de Acción Anual. Plan Anticorrupción y Atención al Ciudadano. Informes de seguimientos a los Riesgos Institucionales Matriz de Riesgos Institucional del periodo anterior.	La formulación del mapa de riesgos institucional se realiza durante el último trimestre del año preferiblemente.
2.	Actualizar el Mapa de Riesgos Institucional.	Coordinan las actividades necesarias para hacer en mesas de trabajo la formulación, revisión y/o actualización del Mapa de Riesgos Institucional.	Servidores Públicos y contratistas. (Todos los procesos) Responsable Riesgos de la Oficina Asesora de Planeación	Cronograma de trabajo Tener en cuenta las guías emitidas por Función Pública en relación con la administración del riesgo.	Verifican que las caracterizaciones de los procesos estén actualizadas.
3.	Identificar el riesgo.	En mesa de trabajo y bajo el liderazgo de la OAP se realizan las siguientes actividades:	Servidores Públicos y contratistas.	Registros de asistencia a mesas de trabajo.	Verifican que el riesgo identificado esté asociado al objetivo del subproceso (o proceso cuando aplique), es

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
		° Analizan el contexto Estratégico. ° Identificación de los puntos de Riesgos. ° Identificación de áreas de impacto. ° Identifican, describen y clasifican los riesgos institucionales del subproceso (o proceso si aplica) y sus factores de riesgo, especificando las causas y estableciendo las posibles consecuencias que la materialización de éstos pueda generar. ° Analizan los riesgos institucionales identificados, con base en los criterios definidos en la Política de administración del riesgo, tanto para la probabilidad como para el impacto.	(Todos los procesos) Responsable Riesgos de la Oficina Asesora de Planeación	Propuestas mapa de riesgos por proceso.	decir identifican los posibles riesgos que afecten el cumplimiento del objetivo. Para los riesgos de seguridad de la información se contará con el apoyo del profesional que ejerza las obligaciones o funciones como Oficial de seguridad de la información quien además de apoyar la identificación de riesgos guiará la identificación de amenazas y vulnerabilidades
4.	Valorar el riesgo.	Valoran la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona del riesgo inherente. Valoran y evalúan los controles existentes en el subproceso (o proceso si aplica) a nivel nacional, con el fin de determinar la zona del riesgo residual. La descripción del control debe contar con la estructura establecida en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, v. 6. Deciden el manejo que se le dará a los riesgos institucionales identificados, los cuales pueden ser aceptar, reducir o evitar	Servidores Públicos y contratistas. (Todos los procesos) Responsable Riesgos de la Oficina Asesora de Planeación	Registros de asistencia a mesas de trabajo. Propuestas mapa de riesgos por proceso.	La OAP verifica el cumplimiento de la Política de Administración del Riesgo aprobada. La OAP verifica los atributos definidos para cada control Cuando en el mapa de riesgos de la entidad, el riesgo residual se ubique en una zona de riesgo Alto o Moderado, se deberá analizar la pertinencia de implementar acciones de manejo del riesgo adicionales a los controles existentes. Estas acciones se incluirán en el Plan de Manejo de Riesgos que especifique: a) Responsable, b) Actividad, c) producto y d) fecha inicio y fin. Para los riesgos de seguridad de la información se tienen en cuenta los controles establecidos en el anexo A de la norma ISO27001:2022.
5.	Generar borrador del Mapa de Riesgos Institucional.	Con la información formulada, revisada y/o actualizada en las actividades anteriores, se genera el borrador del	Responsable Riesgos de la Oficina Asesora de Planeación	Propuestas mapa de riesgos por proceso consolidado.	

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
		Mapa de Riesgos Institucional consolidado.			
6.	Generar la versión definitiva oficial del Mapa de Riesgos Institucional.	Disponer interna y externamente por lo menos entre 5 y 7 días hábiles, el mapa de riesgos institucional versión previa o borrador, para obtener aportes de las partes interesadas. Revisan con los procesos involucrados, las observaciones realizadas en la participación. Realizan los ajustes pertinentes si hay lugar a ello. Consolida la versión definitiva oficial del mapa de riesgos institucional.	Servidores Públicos y contratistas. (Todos los procesos) Responsable Riesgos de la Oficina Asesora de Planeación	Mapa de riesgos por proceso aprobado y publicado. Publicación en web institucional	La OAP verifica las observaciones presentadas en el ejercicio de participación, identificando si hay que realizar modificaciones significativas en la estructura de los riesgos y sus controles.
7.	Aprobar el Mapa de Riesgos Institucional.	Revisan y aprueban el Mapa de Riesgos Institucional consolidado.	Comité Institucional de Gestión y Desempeño	Mapa de riesgos por proceso aprobado. Acta del Comité Institucional de Gestión y Desempeño.	Aprobar el Mapa de Riesgos Institucional.
8.	Publicar la versión definitiva del Mapa.	Una vez aprobada por el Comité Institucional de Gestión y Desempeño se debe hacer la Publicación en el portal web institucional	Profesional encargado de publicar en la web. (Oficina Asesora de Planeación)	Publicación en web institucional	Plazo máximo para la publicación 31 de enero de cada vigencia
9.	Socializar Mapa de Riesgos Institucional.	Da a conocer el Mapa de Riesgos Institucional definitivo y aprobado a servidores públicos y contratistas que trabajan en sus respectivos procesos, subprocesos y direcciones territoriales.	Líderes de Procesos y responsables de subprocesos. Directores Territoriales. (Toda la entidad)	Piezas comunicativas. Registros de asistencia.	Revisan que todos los procesos, subprocesos y direcciones territoriales realicen la socialización del mapa de riesgos institucional.
10.	Cargar en la herramienta para seguimiento de Riesgos.	Cargar en la herramienta para seguimiento de Riesgos, el Mapa de Riesgos oficial por subproceso (o proceso si aplica)	Profesional encargado de la herramienta para seguimiento de Riesgos (Oficina Asesora de Planeación)	Herramienta Seguimiento Riesgos	Correo informando a responsables del proceso el cargue del Mapa de Riesgos Institucional en la herramienta para seguimiento de Riesgos.
11.	Hacer seguimiento al mapa de riesgos institucional aprobado.	Aplican los controles establecidos y hace seguimiento cuatrimestral a la ejecución de los controles en la herramienta para seguimiento de Riesgos, cargando las evidencias	Líderes de Procesos y responsables de subprocesos. Directores Territoriales.	Herramienta Seguimiento Riesgos Repositorio de evidencias	

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
		respectivas en el repositorio dispuesto por la OAP. En esta actividad realiza acompañamiento la OAP, con el fin de hacer seguimiento al debido cumplimiento de los controles y sus evidencias.	(Toda la entidad)		
12.	Realizar ajustes en el mapa de riesgos institucional.	Realiza ajustes en el mapa de riesgos institucional, de acuerdo con las mejoras solicitadas por los procesos. Para estos casos de ajustes al mapa de riesgos, no se debe llevar a aprobación al Comité Institucional de Gestión y Desempeño el mapa de riesgos institucional.	Servidores Públicos y contratistas. (Todos los procesos) Responsable Riesgos de la Oficina Asesora de Planeación	Mapa de riesgos por proceso aprobado.	Solo un mes antes de los seguimientos, los procesos en sede central podrán ajustar los controles definidos y las evidencias identificadas en el mapa de riesgos institucional aprobado en la vigencia y deberán realizar las respectivas socializaciones a los impactados con el cambio.
13.	Realizar y publicar Evaluación.	Realiza evaluación cuatrimestral a la administración del riesgo institucional, genera el informe respectivo y publica de acuerdo con la normatividad relacionada vigente.	Responsable Riesgos de la Oficina Asesora de Planeación (Oficina de Control Interno) Profesional encargado de publicar en la web. (Oficina Asesora de Planeación)	Herramienta para seguimiento de Riesgos Informe de efectividad a los controles del mapa de riesgos institucional Publicación en web institucional	Verifican el repositorio de evidencias establecidas en los controles frente al seguimiento registrado en la herramienta para seguimiento de Riesgos.
FIN DEL PROCEDIMIENTO					

6. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
21/05/2024	° Hace parte del proceso de **Direccionamiento Estratégico y Planeación,** del subproceso de **Gestión de Procesos.** ° Se actualiza el procedimiento "Administración del Riesgo", código **PC-PRC-03**, versión 1, a procedimiento del mismo nombre, código **PC-PRC-03,** versión 2. ° Se deroga el instructivo "Uso de la Herramienta PLANIGAC", código **IN-RIE-PC01-01**, versión 1. ° Se ajusta la periodicidad de seguimiento de los riesgos institucionales, paso de trimestral a cuatrimestral.	**2**
26/ 03/2024	° Se adopta como versión 1 debido a la actualización de la Cadena de Valor en Comité Institucional de Gestión y Desempeño del 3 de marzo del 2023, nuevos lineamientos frente a la generación, actualización y derogación de documentos del SGI. ° Hace parte del proceso de **Direccionamiento Estratégico y Planeación,** del subproceso de **Gestión de Procesos.** ° Se actualiza el procedimiento "Administración del Riesgo", código **PC-RIE-01**, versión 1, a procedimiento del mismo nombre, código **PC-PRC-03,** versión 1.	**1**

FECHA	CAMBIO	VERSIÓN
	° Se ajusta el documento según los lineamientos definidos en la Guía Departamento Administrativo de la Función Pública (DAFP), versión 6 – noviembre de 2022 y el Modelo de Capacidades Gobierno, Riesgo y Cumplimiento – GRC. ° Se incorporan definiciones y normatividad relacionada con el Riesgo Fiscal y activo, se incluye en las Políticas de Operación, el numeral 5.1 relacionado específicamente con el riesgo fiscal. ° En el capítulo de Desarrollo, se incluye el despliegue de la metodología DAFP y GRC. ° En el capítulo del paso a paso, se realiza la modificación de las actividades 3 y 4 relacionadas con identificación y valoración del Riesgo, con el fin de dar mayor claridad sobre las actividades que se ejecutan en estas fases de la administración del Riesgo. ° Se dan nuevos lineamientos frente a la materialización de riesgos y frente a los Riesgos de Seguridad de la Información.	

ELABORÓ Y/O ACTUALIZÓ	REVISÓ TÉCNICAMENTE	REVISÓ METODOLÓGICAMENTE	APROBÓ
Nombre: Karen Lorena Cañizales Manosalva. **Cargo:** Contratista. Oficina Asesora de Planeación. **Nombre:** Orlando José Maya Martínez. **Cargo:** Contratista. Oficina Asesora de Planeación.	**Nombre:** Carlos Rafael González Contreras. **Cargo:** Contratista. Oficina Asesora de Planeación. **Nombre:** Fabián Eduardo Camelo Sánchez **Cargo:** Jefe de Oficina. Oficina Asesora de Planeación.	**Nombre:** Lida Carolina Zuleta Alemán. **Cargo:** Profesional Especializado. Oficina Asesora de Planeación.	**Nombre:** Comité de Coordinación de Control Interno 20 de mayo del 2024. **Nombre:** Fabián Eduardo Camelo Sánchez **Cargo:** Jefe de Oficina. Oficina Asesora de Planeación.