



POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

GIT DE PLANEACIÓN
Mayo de 2023

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Piso 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00



SC-
7328-1



SA-CER
366516



OS - CER
366518



OS-CER
660642



TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	3
2. ALCANCE	3
3. OBJETIVOS	4
4. GLOSARIO	4
5. CONTEXTO.....	7
6. RIESGOS INSTITUCIONALES.....	8
7. MAPA DE RIESGO INSTITUCIONAL.....	8
8. RIESGOS DE PROYECTOS.....	9
9. MAPA DE RIESGOS DE PROYECTOS.....	9
10. METODOLOGÍA APLICADA	9
11. PERIODICIDAD.....	9
12. NIVELES DE RESPONSABILIDAD Y AUTORIDAD PARA EL MANEJO DE LOS RIESGOS.....	10
13. NIVELES DE ACEPTACIÓN DEL RIESGO	12
14. NIVELES PARA CALIFICAR EL IMPACTO.....	12
15. OPCIONES PARA TRATAMIENTO Y MANEJO DE RIESGOS	15
16. RECURSOS.....	16
17. DIVULGACIÓN	16
18. CAPACITACIÓN.....	16
19. ACOMPAÑAMIENTO DE PLANEACIÓN	17
20. ACCIONES PARA SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO	17



SC-
7328-1



SA-CER
366516



OS – CER
366518



OS-CER
660642



1. INTRODUCCIÓN

La política de administración del riesgo de la Unidad Administrativa Especial Contaduría General de la Nación (CGN) denota el grado de compromiso de la entidad frente al cumplimiento de los objetivos estratégicos y del plan de acción institucional, direccionando a los procesos a asumir un pensamiento basado en riesgos, que permita anticiparse, disminuir y contrarrestar el impacto de eventos inesperados.

Es importante resaltar que esta política toma como base el Modelo Integrado de Planeación y Gestión MIPG, la Norma Técnica Colombiana NTC-ISO 31000:2018, el Decreto 2641 del 2012, la Metodología General Ajustada (MGA WEB) y la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” v4, expedida por la Presidencia de la República, Ministerio de Tecnologías de la Información y las Comunicaciones, el Departamento Administrativo de la Función Pública y Departamento Nacional de Planeación.

2. ALCANCE

La Administración del Riesgo en la UAE Contaduría General de la Nación tendrá el siguiente alcance:

- Riesgos de Gestión y Corrupción: Todos los procesos de la CGN.
- Riesgos del Sistema de Gestión de Seguridad de la Información - Seguridad Digital: Los procesos que hacen parte del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI), como lo son los procesos misionales (Normalización y Culturización Contable, Centralización de la Información y Consolidación de la Información) y el proceso de Gestión TICs.
- Riesgos de Proyecto: Aplica para los proyectos de inversión inscritos en el Banco de Programas y Proyectos de Inversión Nacional del Departamento Nacional de Planeación - DNP.





Esta política de administración del riesgo contribuye al control interno de la entidad, y fomenta la cultura del autocontrol al interior de los procesos.

3. OBJETIVOS

- Establecer los parámetros necesarios para una adecuada administración de los riesgos a través de los elementos: contexto estratégico; identificación de riesgos; análisis de riesgos; valoración de riesgos; políticas de administración del riesgo, su trazabilidad, registro y monitoreo.
- Orientar la toma de decisiones.
- Incentivar el pensamiento basado en riesgos dentro de la entidad.
- Buscar la mejora continua en cada uno de los procesos.
- Realizar seguimiento a los riesgos asociados a los proyectos de inversión de la CGN, con el fin de reducir el nivel de riesgo en las etapas de inversión y operación de los proyectos.
- Establecer una adecuada gestión mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante situaciones que afecten el cumplimiento misional y el logro de los objetivos.

4. GLOSARIO

- **Apetito del Riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.
- **CICCI:** Comité Institucional de Coordinación de control Interno.
- **Factores de Riesgo:** Fuente generadora de los eventos de riesgos operativos.
- **Riesgos Operativos:** Posibilidad de incurrir en pérdidas por errores, fallas, deficiencias en el Talento Humano, Procesos, Tecnología, Infraestructura y Eventos Externos.





- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **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.
- **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.
- **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.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **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.
- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de Frecuencia o Factibilidad.
- **Impacto:** Se entiende como las consecuencias que pueden ocasionar a la organización la materialización del riesgo.
- **Riesgo Inherente:** Es aquel riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.





- **Riesgo Residual:** Nivel de riesgo permanente luego de tomar medidas de tratamiento del riesgo.
- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.
- **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.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Integridad:** propiedad de exactitud y completitud.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Tolerancia al Riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Apetito al Riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Metodología General Ajustada- MGA:** es una aplicación informática que sigue un orden lógico para el registro de la información más relevante resultado del proceso de formulación y estructuración de los proyectos de inversión pública.





5. CONTEXTO

Para la identificación de riesgos la entidad realiza un análisis de su entorno estratégico a partir de los siguientes factores internos y externos:

Contexto externo

- **Económicos y financieros:** Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
- **Políticos:** Cambio de Gobierno, legislación, políticas públicas, regulación.
- **Sociales:** Demografía, responsabilidad social, orden público.
- **Tecnológicos:** Avances en tecnología, acceso a sistemas de información externos, Gobierno en línea.
- **Ambientales:** Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
- **Legales y reglamentarios:** Normativa externa.
- **Pandemia:** Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

Contexto interno

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





Contexto del proceso

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

6. RIESGOS INSTITUCIONALES

El mapa de riesgos institucional se consolidará a partir de aquellos riesgos de gestión ubicados en la zona extrema y alta, a estos se les efectuará seguimiento y monitoreo continuo por parte de los líderes de proceso o responsables asignados para tal fin, quienes deberán garantizar que los controles se ejecuten en los tiempos estipulados, evitando con ello la materialización de los riesgos.

7. MAPA DE RIESGO INSTITUCIONAL

La información correspondiente a los riesgos ubicados en la zona extrema y alta se consolidará en el formato denominado “Mapa de riesgos institucional”, el cual será presentado al Comité Institucional de Coordinación de Control Interno, para su respectiva revisión y aprobación.





8. RIESGOS DE PROYECTOS

El mapa de riesgos de proyectos se consolidará a partir de aquellos riesgos de los proyectos de inversión identificados en la etapa de prefactibilidad y con independencia de la valoración que se realice para cada uno de estos. A los riesgos se les efectuará seguimiento continuo por parte de los Gerentes de proyectos con el apoyo de los Formuladores de proyectos, quienes deberán ejecutar las medidas de mitigación y los controles en los tiempos estipulados, evitando con ello la materialización de los riesgos.

9. MAPA DE RIESGOS DE PROYECTOS

La información correspondiente a los riesgos de los proyectos de inversión de la CGN se consolidará en el formato denominado “Mapa de riesgos de proyectos”, el cual será presentado al Comité Institucional de Coordinación de Control Interno, para su respectiva revisión y aprobación.

10. METODOLOGÍA APLICADA

La metodología aplicada para la administración del riesgo será la contemplada en la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” v4 y la “Metodología General Ajustada (MGA WEB)”, expedida por la Presidencia de la República, Ministerio de Tecnologías de la Información y las Comunicaciones, el Departamento Administrativo de la Función Pública y el Departamento Nacional de Planeación, respectivamente.

11. PERIODICIDAD

La revisión de los mapas de riesgos de Gestión, Corrupción, Seguridad de la Información - Seguridad Digital y de proyectos de la





UAE Contaduría General de la Nación, se realizará como mínimo dos veces al año o cuando las circunstancias lo ameriten, a partir de modificaciones o cambios sustanciales en el contexto estratégico, cambios relevantes en los procesos y/o procedimientos, o cualquier hecho sobreviniente externo o interno que afecte la operación de la entidad.

El jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento a la gestión del riesgo de acuerdo con lo establecido en la “Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces”, MIPG y “Estrategias para la Construcción del Plan Anticorrupción y de atención al ciudadano” ésta última define los siguientes cortes de seguimiento a los riesgos de corrupción:

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

Adicionalmente se deberá presentar un informe cuatrimestral que contenga los resultados de los seguimientos a los riesgos de los procesos, con el fin de evidenciar la materialización, la creación, modificación o eliminación de alguno de ellos.

12. NIVELES DE RESPONSABILIDAD Y AUTORIDAD PARA EL MANEJO DE LOS RIESGOS

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El





Modelo Integrado de Planeación y Gestión - (MIPG) en la dimensión siete (7) "Control Interno" desarrolla a través de la Línea Estratégica y las tres (3) Líneas de Defensa de responsabilidad de la gestión del riesgo y control.

LÍNEA ESTRATÉGICA

Define el marco general para gestión del riesgo y el control, supervisa su cumplimiento, está a cargo de la alta dirección.



1

1ra LÍNEA DE DEFENSA

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

A cargo de los líderes de cada uno de los procesos con el apoyo de sus colaboradores y el integrante del Equipo Operativo



2

2da LÍNEA DE DEFENSA

Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

El GIT de Planeación tiene la responsabilidad de monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, acompaña a los procesos en la administración de riesgo y el ahora de la consolidación de los Mapas de Riesgos de Gestión, Corrupción, Seguridad de la Información - Seguridad Digital y de Proyectos, a su vez es el encargado de su publicación.

Para los riesgos de Seguridad de la Información - Seguridad Digital se debe tener el acompañamiento del GIT de Tecnologías de Información.



3

3ra LÍNEA DE DEFENSA

Proporciona información sobre la efectividad del SCI, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. El GIT de Control Interno realiza el seguimiento y la medición de los avances de las acciones de respuesta y evaluación de la efectividad de las políticas.



SC-7328-1



SA-CER 366516



OS - CER 366518



OS-CER 660642



13. NIVELES DE ACEPTACIÓN DEL RIESGO

Para el caso de los riesgos de gestión y de seguridad de la información se consideran **ACEPTABLES** aquellos ubicados en nivel de riesgo bajo.

Los riesgos de corrupción **NO TIENEN** nivel de aceptación.

14. NIVELES PARA CALIFICAR EL IMPACTO

En los riesgos de gestión los niveles para calificar el impacto son:

NIVEL	VALOR DEL IMPACTO	CONSECUENCIAS CUALITATIVAS
INSIGNIFICANTE	1	<ul style="list-style-type: none"> No hay interrupción de las operaciones de la entidad. No se generan sanciones económicas o administrativas. No se afecta la imagen institucional de forma significativa.
MENOR	2	<ul style="list-style-type: none"> Interrupción de las operaciones de la entidad por algunas horas. Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	3	<ul style="list-style-type: none"> Interrupción de las operaciones de la entidad por un (1) día. Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. Reproceso de actividades y aumento de carga operativa. Imagen institucional afectada en el orden nacional o regional por retrasos en la





		<p>prestación del servicio a los usuarios o ciudadanos.</p> <ul style="list-style-type: none"> Investigaciones penales, fiscales o disciplinarias
MAYOR	4	<ul style="list-style-type: none"> Interrupción de las operaciones de la entidad por más de dos (2) días. Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. Sanción por parte del ente de control u otro ente regulador. Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
CATASTRÓFICO	5	<ul style="list-style-type: none"> Interrupción de las operaciones de la entidad por más de cinco (5) días. Intervención por parte de un ente de control u otro ente regulador. Pérdida de información crítica para la entidad que no se puede recuperar. Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. Imagen institucional afectada en el orden nacional o regional

En los riesgos de Seguridad de la Información - Seguridad Digital, los niveles para calificar el impacto son:

NIVEL	VALOR DEL IMPACTO	CONSECUENCIAS CUALITATIVAS
INSIGNIFICANTE	1	<ul style="list-style-type: none"> Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	<ul style="list-style-type: none"> Afectación leve de la integridad. Afectación leve de la disponibilidad.





MODERADO	3	<ul style="list-style-type: none"> • Afectaciones leves de la confidencialidad. • Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	<ul style="list-style-type: none"> • Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	5	<ul style="list-style-type: none"> • Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

En los riesgos de Seguridad de la Información - Seguridad Digital, los niveles para calificar el impacto son:

IMPACTO	DESCRIPTOR
MODERADO	Genera medianas consecuencias sobre la entidad.
MAYOR	Genera altas consecuencias sobre la entidad.
CATASTRÓFICO	Genera consecuencias muy graves para la entidad.

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

15. OPCIONES PARA TRATAMIENTO Y MANEJO DE RIESGOS

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción. En la CGN las opciones apuntarán a la toma de decisiones para:

- **Aceptar el riesgo:** Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo. No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado)
- **Evitar el riesgo:** Cuando los escenarios de riesgo identificados se consideran demasiado extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.
- **Compartir el riesgo:** Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionar, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.
- **Reducir el riesgo:** El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.





Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se está logrando los objetivos estratégicos y de procesos de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control y esto implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales; por lo tanto, se deberá considerar para la implementación de acciones y controles, aspectos como: viabilidad jurídica, técnica, institucional, financiera o económica y análisis costo - beneficio.

16. RECURSOS

En cada uno de los pasos de la administración del riesgo se contemplarán los recursos necesarios para la definición, implementación y efectividad de las acciones que permitan un tratamiento adecuado de los riesgos. Para ello se involucran a los procesos que tengan incidencia en el cálculo, aplicación o solicitud de los recursos: técnicos, financieros y talento humano.

17. DIVULGACIÓN

La Política de Administración del Riesgo, los Mapas de Riesgos: Institucional, Gestión, Corrupción Seguridad de la Información - Seguridad Digital y de Proyectos, se divulgarán a través de la página web de la UAE Contaduría General de la Nación a fin de que todas las partes interesadas se informen de la gestión de riesgos realizada por los procesos.

18. CAPACITACIÓN

La administración del riesgo se considera un tema importante para la entidad, por ello se deberá realizar como mínimo una capacitación anual (interna o externa), que permita fortalecer las competencias de los servidores públicos, y así poder garantizar una





gestión del riesgo coherente y adecuada, dentro de cada uno de los procesos.

19. ACOMPAÑAMIENTO DE PLANEACIÓN

- Brindar los lineamientos para implementar la Política de Administración del Riesgo, la metodología del DAFP y los lineamientos de la metodología general ajustada (MGA WEB) relacionada con los riesgos, en la identificación y tratamiento a los riesgos identificados por los procesos o cuando se formulen proyectos.
- Llevar a cabo las mesas de trabajo para la identificación/validación y seguimiento de la gestión de riesgos e indicadores del proceso.
- Dejar evidencia de los seguimientos realizados, por medio de las ayudas de memoria, en las cuales reposan punto por punto las actividades realizadas.
- Consolidar el mapa de riesgos (gestión, corrupción, seguridad de la información - seguridad digital, proyectos).
- Presentar los mapas de riesgos consolidados para la socialización y aprobación al Comité Institucional de Coordinación de Control Interno CICCI.

20. ACCIONES PARA SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO

Para todos los tipos de riesgos contemplados en los mapas institucionales de riesgos de la CGN, cuando se materialicen, es necesario aplicar las siguientes acciones:

Línea estratégica – Alta Dirección y Comité Institucional de Coordinación de Control Interno.

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 los informes presentados por la segunda y tercera línea de defensa.

Primera línea de defensa – Líderes de proceso, integrantes del Equipo Operativo y colaboradores en general.

- Informar al GIT de Planeación como segunda línea de defensa, sobre la materialización del riesgo.
- 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 defensa.

- 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, para mitigar el impacto y evitar que el riesgo se vuelva a materializar.
- Revisar y ajustar los controles existentes. De ser necesario, establecer nuevos controles asociados al riesgo materializado, teniendo en cuenta el Plan de Mejoramiento definido.
- Revisar y actualizar el Mapa de Riesgos correspondiente, en particular las causas, riesgos y controles, estableciendo acciones preventivas y de mejora.
- Dar cumplimiento estricto al Plan de Mejoramiento propuesto.

Segunda línea de defensa – Grupo Interno de Trabajo de Planeación.

- Revisar el análisis de causas y las acciones correctivas de los Planes de Mejoramiento planteados por la primera línea de defensa, y realizar las recomendaciones que permitan asegurar que los controles estén bien diseñados.
- 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 finalización de la acción, responsable de la acción, seguimiento y el estado.





Tercera línea de defensa – Grupo de Control Interno.

- Revisar las acciones del monitoreo implementadas por la primera línea de defensa.
- Verificar si se ejecutaron las acciones planteadas en el Plan de Mejoramiento y se actualizó el Mapa de Riesgos correspondiente.
- Asegurar que los controles planteados por la primera línea de defensa sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.
- Verificar el cumplimiento del Plan de Mejoramiento y realizar el seguimiento de acuerdo con el procedimiento establecido, cuando la materialización de los riesgos sea identificada en una auditoría realizada por el GIT de Control Interno.

Adicional a las actividades planteadas anteriormente, en el caso de la materialización de los riesgos de corrupción y de seguridad de la información, se deben realizar las siguientes:

RIESGOS DE CORRUPCIÓN

Para los riesgos de corrupción, su materialización puede derivar en acciones legales y pérdida de imagen para la entidad; por lo tanto, las acciones disciplinarias no solo recaen sobre las personas directamente implicadas, sino también sobre los líderes de procesos.

Línea estratégica – Alta Dirección y Comité de Coordinación de Control Interno.

- Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), analiza y determina la aplicabilidad del proceso disciplinario e informa a la instancia respectiva.
- Informar a las autoridades correspondientes de la ocurrencia de un hecho de corrupción.

Segunda línea de defensa – Grupo Interno de Trabajo de Planeación.





- Revisar el Mapa de Riesgos de corrupción, en particular, las causas, riesgos y controles.
- Llevar a cabo un monitoreo de los procesos que han materializado riesgos.
- Consolidar y publicar en la página web de la CGN, el Mapa de Riesgos de corrupción actualizado.

Tercera línea de defensa – Grupo de Control Interno.

- Verificar la efectividad de las acciones planteadas en el Plan de Mejoramiento.
- Actualizar el Mapa de Riesgos de corrupción.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Primera línea de defensa – Líderes de proceso, integrantes del Equipo Operativo y colaboradores en general.

- En caso de materialización de un riesgo de seguridad digital, se debe informar, adicionalmente, al GIT de Apoyo Informático, de acuerdo con lo indicado en los lineamientos para la gestión del riesgo de seguridad digital.
- En la elaboración de los controles para mitigar o tratar el riesgo, se debe tener en cuenta lo indicado en los lineamientos para la gestión del riesgo de seguridad digital.
- Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información 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 seguridad digital.
- 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.





Segunda línea de defensa – GIT de Apoyo Informático y Grupo Interno de Trabajo de Planeación.

- El Coordinador del GIT de Apoyo Informático, como responsable de la seguridad digital de la CGN, deberá supervisar y acompañar el proceso de implementación de los Planes de Mejoramiento, verificando que la primera línea de defensa ejecute las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.
- Efectuar la evaluación de los Planes de Mejoramiento, realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad, y realizar la actualización de los Mapas de Riesgo.
- Actualizar el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar 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.

