MINISTERIO DE CIENCIA TECNOLOGÍA E INNOVACIÓN

GUÍA PARA LA GESTIÓN DEL RIESGO Y LAS OPORTUNIDADES

TABLA DE CONTENIDO

INTRODUCCIÓN

Las Entidades públicas existen con el fin último de generar resultados que atiendan los planes de desarrollo, garanticen los derechos y resuelvan las necesidades y problemas de sus grupos de interés, grupos de valor y ciudadanos en general, con integridad y calidad en el servicio, generando valor público. En su camino cotidiano se enfrentan con la falta de certeza en diversos ámbitos, por lo que el reto de toda Entidad consiste en determinar cuanta incertidumbre se puede y se desea aceptar mientras se genera valor público, que realmente permita la obtención de los resultados planificados.

Al operar en ambientes donde factores como la globalización, los cambios políticos, económicos, tecnológicos, ambientales, legales, sociales y culturales, los mercados cambiantes, la competencia y la dinámica interna de sus propios procesos, crean incertidumbre, se debe considerar que estos eventos, implican riesgos que pueden representar tanto amenazas como oportunidades para la Entidad. En este sentido, el Ministerio de Ciencia, Tecnología e Innovación incorpora esfuerzos que permitan el cumplimiento de su misión institucional y la generación de acciones coherentes que permitan el logro de los objetivos propuestos; para ello, ejecuta diferentes actividades enmarcadas bajo una gestión por procesos que puede verse afectada por la presencia de riesgos, por tanto se hace necesario contar con una herramienta encaminada a administrar y prevenir la ocurrencia de riesgos que puedan generar efectos negativos al interior de la Entidad y que al mismo tiempo permita potencializar las oportunidades identificadas. Una adecuada administración de los riesgos permite a la alta dirección tratar la incertidumbre de una manera eficaz y por tanto generar con mayor certeza valor público a la gestión institucional.

La presente guía es un instrumento de tipo preventivo para identificar, analizar, evaluar, tratar, comunicar, monitorear, revisar y realizar seguimiento a los riesgos de gestión, corrupción, calidad estadística, seguridad digital y riesgos de tecnologías de la información, con el fin de optimizar y enfocar los esfuerzos institucionales en acciones estandarizadas que permitan abordar y tratar los riesgos identificados en forma eficaz y efectiva en coherencia con los objetivos y metas institucionales, potencializando las oportunidades identificadas.

1. OBJETIVO GENERAL

Definir los lineamientos para la implementación y desarrollo de la política de administración del riesgo y la gestión de las oportunidades del Ministerio de Ciencia, Tecnología e Innovación, a través de un conjunto de lineamientos orientados a un adecuado control y gestión riesgos de gestión, corrupción, calidad estadística, seguridad digital y de tecnologías de la información, identificados en cada uno de los procesos que hacen parte del Sistema de Gestión Organizacional, así como de la gestión articulada de las oportunidades a fin de garantizar el cumplimiento de la misión y objetivos estratégicos de la Entidad.

1.1 OBJETIVOS ESPECÍFICOS

- Generar una visión sistémica de la administración de los riesgos de la Entidad, evidenciada en un ambiente de control adecuado y un direccionamiento estratégico que fije una orientación clara y planeada sobre las actividades de control y seguimiento para abordar las amenazas y oportunidades identificadas.

- Proteger los recursos de la Entidad, resguardándolos contra la materialización de los riesgos valorados como amenazas de corrupción, de seguridad digital o de gestión.

- Implementar y fortalecer dentro de los procesos y procedimientos controles, que permitan evitar, reducir o mitigar, las vulnerabilidades o potenciales amenazas que se puedan presentar.

- Involucrar y comprometer a todos los servidores de la Entidad en la búsqueda de acciones encaminadas a gestionar los riesgos de los procesos en los cuales participa.

- Aumentar la probabilidad de alcanzar los objetivos y proporcionar a la administración un aseguramiento razonable con respecto al logro de estos.

- Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan a la Entidad, tener una seguridad razonable en el logro de sus objetivos, bajo el cumplimiento de normas, leyes y regulaciones aplicables.

- Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los colaboradores de la Entidad.

2. ALCANCE

Esta guía define los lineamientos para la gestión y control de los riesgos de gestión, corrupción y seguridad digital de la Entidad partiendo desde la política de administración del riesgo, la construcción del mapa de riesgos, la comunicación, consulta y divulgación de los riesgos existentes, su priorización, seguimiento, monitoreo, revisión y actualización para la gestión integral de los riesgos.

Se incluyen los lineamientos para la gestión de los riesgos de toda naturaleza, así como las directrices para la gestión de las oportunidades con el fin de garantizar un manejo sistemático, articulado y transversal en todos los procesos y funciones del Ministerio de Ciencia, Tecnología e Innovación.

3. LA GESTIÓN DEL RIESGO EN EL MARCO DEL MIPG

De acuerdo con el Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, el Decreto 1083 de 2015, Decreto único del Sector Función Pública, modificado por el Decreto 1499 de 2017, establece el Modelo Integrado de Planeación y Gestión - MIPG, el cual surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo Sistema de Gestión, y de la articulación de este con el Sistema de Control Interno.

El MIPG Es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio. MIPG opera a través de un conjunto de 7 dimensiones que agrupan las políticas de gestión y desempeño institucional (Talento Humano, Direccionamiento estratégico y Planeación, Gestión con valores para resultados, Evaluación de resultados, Información y comunicación, Gestión del conocimiento y Control Interno), implementadas de manera articulada e intercomunicada, permitirán que MIPG funcione.

De esta manera, en el Ministerio este modelo concentra las prácticas y procesos que adelanta la entidad para transformar insumos en resultados que produzcan los impactos deseados en materia de CTeI, esto es, una gestión y un desempeño institucional que generan valor público[1].

En la siguiente figura se muestra la estructura del MIPG, conformado por 7 dimensiones y 19 políticas de gestión y desempeño. Resaltado en óvalos de color rojo y letra azul las dimensiones y políticas directamente relacionadas con la gestión del riesgo en la entidad.

De acuerdo con el MIPG, el Ministerio a partir del ejercicio de planeación institucional, define los planes de acción anual, e incluye iniciativas o acciones para la gestión de los riesgos que pueden afectar el cumplimiento de las metas de la entidad y los controles para su mitigación. Los planes e iniciativas asociadas a la gestión del riesgo se pueden consultar en el aplicativo ***GINA, módulo Planes***. Según lo anterior, la gestión del riesgo en la entidad es una tarea propia del equipo directivo del Ministerio que se desarrolla desde el ejercicio de Direccionamiento Estratégico y de Planeación. En este punto, se emiten lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

El Modelo también contiene la política de administración de riesgos, la cual se entiende como la declaración de dirección y las intenciones generales de la entidad con respecto a la gestión del riesgo y establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos. Para definir la Política de Gestión del Riesgo, el Ministerio tuvo en cuenta el alcance de la misma, que abarcar todos los procesos y áreas de la entidad.

[1] Manual Operativo MIPG V04. Función Pública marzo 2021. Disponible en: https://www.funcionpublica.gov.co/documents/28587410/34112007/Manual+Operativo+MIPG.pdf/ce5461b4-97b7-be3b-b243-781bbd1575f3.

Por otra parte, uno de los planes que se integra en el MIPG y que involucra acciones transversales de integridad en sus componentes es el ***Plan Anticorrupción y de Atención al Ciudadano –PAAC,*** que contiene la estrategia de lucha contra la corrupción y de atención al ciudadano del Ministerio, en cumplimiento de lo establecido en el artículo 73 de la Ley 1474 de 2011. El PAAC tiene un carácter preventivo para el control de la gestión y se encuentra integrado por cinco componentes independientes que cuentan con parámetros y un soporte normativo propio: cinco componentes obligatorios son: (i) Mapa de riesgos de corrupción. (ii) Estrategia anti-trámites. (iii) Rendición de cuentas. (iv) Mecanismos para mejorar la atención al ciudadano, y (v) Mecanismos para la transparencia y el acceso a la información. Un sexto componente, que no es obligatorio: Iniciativas adicionales, en el que las entidades podrán incluir políticas, estrategias, mecanismos o prácticas que se consideren convenientes para combatir la corrupción. El PAAC del Ministerio se encuentra disponible para consulta en la sección de ***Transparencia y Acceso a la Información Pública*** de la página Web de la entidad, en el siguiente enlace: https://minciencias.gov.co/transparencia-accesoainformacionpublica.

En materia de Seguridad Digital, de acuerdo con el Documento CONPES 3854 de 2016 la entidad ha implementado lineamientos en materia de Seguridad Digital, orientados a fortalecen las capacidades institucionales para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital. Para su implementación se han definido los ***Riesgos de Seguridad Digital***.

Finalmente, en coherencia con la Dimensión de Control Interno del MIPG, el Ministerio tiene establecida la ***Política de Control Interno,*** para determinar acciones, métodos y procedimientos de control y de gestión del riesgo, así como mecanismos para la prevención y evaluación de éste. Esta Política se articula con el Modelo Estándar de Control Interno MECI, que se fundamenta en cinco componentes, a saber: (i) ambiente de control, (ii) Evaluación del riesgo, (iii) actividades de control, (iv) información y comunicación y (v) actividades de monitoreo.

Nota: Para efectos de la implementación de la metodología de gestión del riesgo en el Ministerio de Ciencia, Tecnología e Innovación, la entidad ha adoptado la "***Guía para la administración del riesgo y el diseño de controles en entidades públicas",*** de la Función Pública en su versión vigente disponible en el siguiente enlace:

https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238

4. BENEFICIOS DE LA GESTIÓN DE RIESGOS

La gestión de los riesgos institucionales da acceso a los siguientes beneficios inherentes:

- **Alinea el riesgo y la estrategia:** en su evaluación de alternativas estratégicas, la dirección considera los riesgos priorizados por la Entidad, estableciendo los objetivos correspondientes y desarrollando mecanismos para gestionar las oportunidades o amenazas asociadas.

- **Mejora las decisiones de respuesta a los riesgos:** La metodología de gestión de riesgos institucionales proporciona rigor para identificar las posibles oportunidades o amenazas que hacen parte del que hacer institucional y seleccionar entre las posibles alternativas de respuesta a las amenazas o a las oportunidades, la más viable y efectiva para alcanzar los resultados esperados.

- **Reduce las sorpresas y las pérdidas operativas:** La gestión de los riesgos mejora la capacidad de la Entidad para identificar las amenazas o vulnerabilidades que pueden afectar su gestión y establecer respuestas, reduciendo las sorpresas y las pérdidas asociadas.

- **Identifica y gestiona la diversidad de riesgos para toda la Entidad:** Cada Entidad se enfrenta a riesgos que inciden de manera negativa o positiva en el desempeño de sus procesos y en el logro de los resultados planificados; la gestión de riesgos facilita respuestas eficaces e integradas a los impactos interrelacionados de dichos riesgos.

- **Provee respuestas integradas a múltiples riesgos:** La ejecución de los procesos conllevan riesgos inherentes, para lo cual la gestión de los riesgos favorece la elaboración de soluciones integradas para administrarlos, bajo la premisa de optimizar los recursos disponibles y garantizar la coherencia en las respuestas institucionales, en el momento de abordar las posibles vulnerabilidades o amenazas, así como las oportunidades identificadas.

- **Permite aprovechar las oportunidades:** mediante la consideración de una amplia gama de potenciales eventos, la dirección está en posición de identificar y aprovechar las oportunidades de modo proactivo, a fin de potencializar los efectos deseables.

- **Enfoque preventivo:** la gestión del riesgo permite la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a sus grupos de valor en aspectos fundamentales frente a la generación de valor público.

5. DEFINICIONES

Aplican todas las definiciones contenidas en la ***"Guía para la administración del riesgo y el diseño de controles en entidades públicas"***, de la Función Pública en su versión vigente disponible en el siguiente enlace:

https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238

De igual forma, aplican las definiciones del ***Glosario del MIPG***, emitido por la Función Pública, el cual está disponible en el siguiente enlace:

https://www.funcionpublica.gov.co/documents/28587410/34112007/2023-03-21_Manual_operativo_mipg_5V.pdf/dbe560cc-e81d-bd7b-b23f-075184e029c6?t=1679509602732

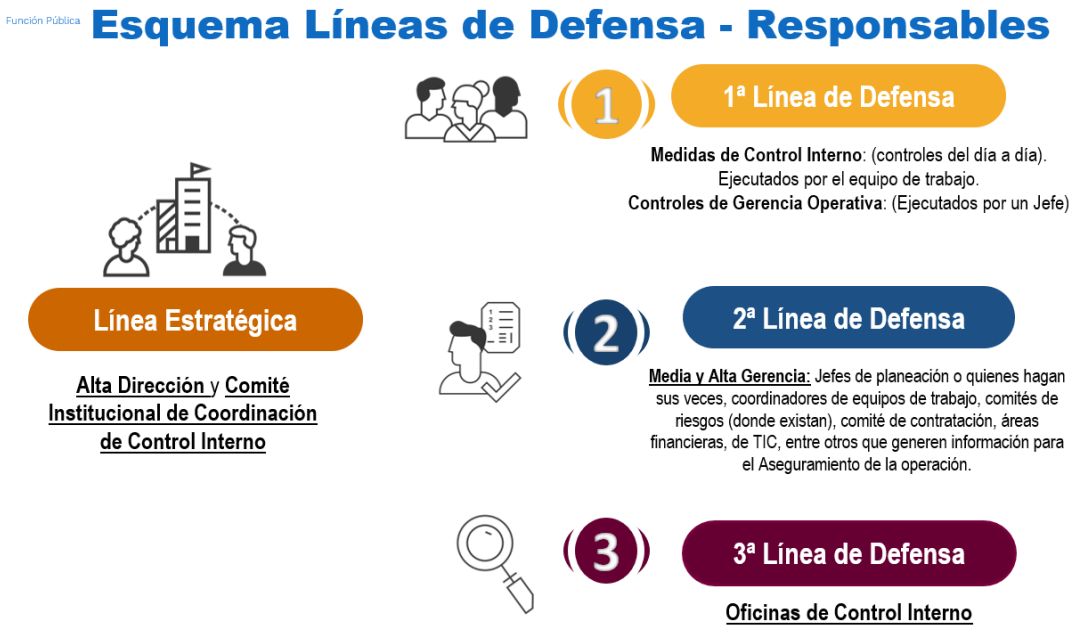
6. MARCO LEGAL

Aplica el marco Legal contenido en el Manual Operativo del MIPG, Políticas Planeación Institucional y Control Interno.

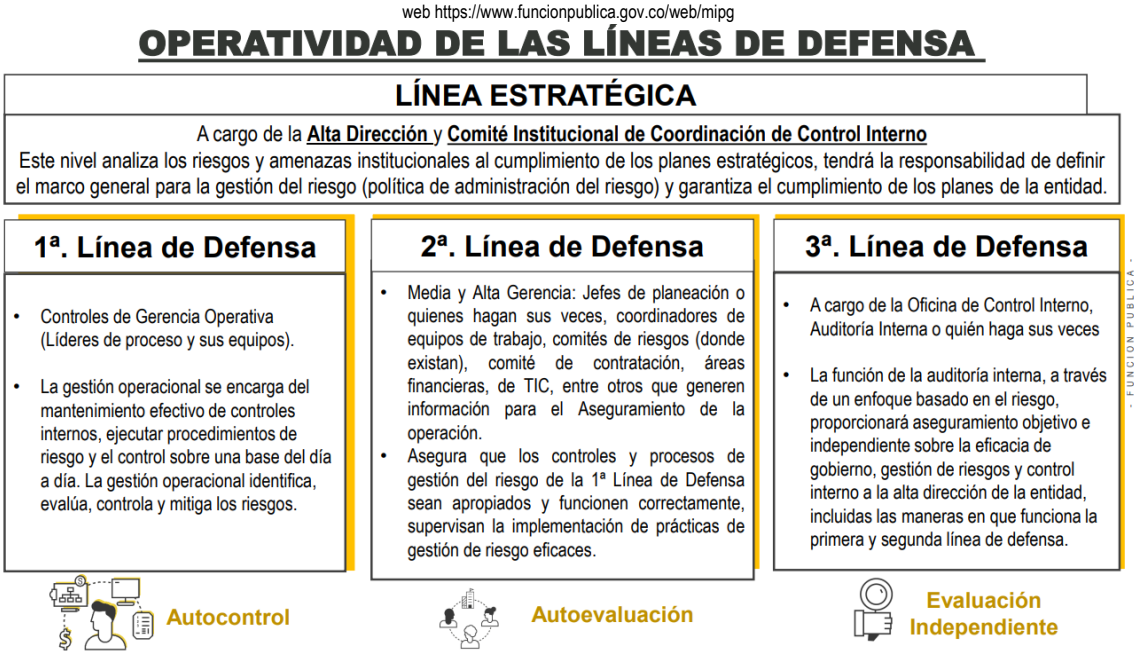
Aplican las normas identificadas en el Normograma de la entidad, Proceso Gestión de la Innovación Institucional (riesgos de gestión y corrupción) y Gestión Tecnologías de la Información y las Comunicaciones (riesgos de Seguridad Digital), disponible en GINA, módulo documentos.

7. ROLES Y RESPONSABILIDADES

La gestión del riesgo está alineada con los requisitos de la dimensión del Modelo Integrado de Planeación y Gestión – MIPG de "Direccionamiento Estratégico" y de "Control interno", que se desarrolla con el Modelo Estándar de Control, Interno - MECI a través de un esquema de líneas de defensa a través del cual se asignan responsabilidades y roles, el cual se distribuye en diversos servidores de la Entidad como se ilustra a continuación:



Fuente: OAPII (2022) basados en la información de la guía para la administración del riesgo y el diseño de controles en Entidades públicas y los documentos soporte dispuestos la página web https://www.funcionpublica.gov.co/web/mipg



Fuente: OAPII (2022) basados en la información de la guía para la administración del riesgo y el diseño de controles en Entidades públicas y los documentos soporte dispuestos la página web https://www.funcionpublica.gov.co/web/mipg

8. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

El Ministerio de Ciencia, Tecnología e Innovación, aplica la definida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública, disponible en el siguiente enlace:

https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238

Por otra parte, la Entidad cuenta con la plataforma tecnología – Suite Visión Empresarial – GINA, la cual, mediante su módulo de riesgos, consolida y controla la administración de los riesgos en cada uno de los procesos de la Entidad. Dicha aplicación se encuentra alineada con la metodología establecida en la mencionada Guía.

9. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Con el fin de lograr los objetivos establecidos en su planeación estratégica y misionalidad, el Ministerio de Ciencia, Tecnología e Innovación, se compromete a instaurar y conservar un sistema que permita y garantice la identificación, registro, análisis, evaluación, monitoreo y control de los riesgos inherentes al desarrollo de la misión y el cumplimiento de los objetivos institucionales, promoviendo la eficacia y eficiencia administrativa, así como la transparencia de la Entidad.

9.1 Lineamientos de la Política de Administración del Riesgo:

- ✓ Corresponde a la Oficina Asesora de Planeación e Innovación Institucional y la Oficina de Control Interno, impulsar a nivel institucional una cultura de gestión del riesgo coherente con el Modelo Integrado de Planeación y Gestión, el Modelo Estándar de Control Interno – MECI, el Modelo de Seguridad y Privacidad de la Información y las Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

- ✓ Para facilitar el cumplimiento de los propósitos y requerimientos del Sistema de Administración de Riesgos (SAR), se mantendrá adecuada la estructura organizacional, el modelo de operación por procesos y los roles, responsabilidades y autoridades de cada uno de los servidores públicos y contratistas de la Entidad.

- ✓ Con el fin de asegurar la comunicación y consulta, así como el establecimiento de roles, responsabilidades y autoridades en la gestión del riesgo la Entidad cuenta con un Equipo de Líderes y responsables de procesos, que esencialmente apoyan al área responsable del Sistema de Administración de Riesgos en la recolección y evaluación de la información sobre riesgos en cada una de las dependencias y procesos de la Entidad.

- ✓ Para el tratamiento de riesgo la Entidad ejecutará acciones para evitar, reducir, transferir o asumir el riesgo calificado como amenaza; para el caso de las oportunidades se promoverán las acciones para aumentar los resultados esperados. Dichas opciones establecen las orientaciones para que los líderes, responsables de procesos y en general las áreas de la Entidad, formulen las acciones que conforman el plan manejo del riesgo.

- ✓ Las disposiciones aplicables para la gestión del riesgo institucional se encuentran en el Procedimiento de "Identificación**,** Análisis, Valoración, Seguimiento y Evaluación del Riesgo" D102PR03 y en la Guía para la Gestión del Riesgo y las oportunidades del Ministerio de Ciencia, Tecnología e Innovación" D102PR03G01.

- ✓ La consolidación de los riesgos identificados y el seguimiento a los mismos se llevará a cabo a través del módulo "Gestión del Riesgo" del aplicativo GINA (Gestión Integrada Nuestra Aliada).

9.2. Monitoreo y revisión:

Una vez se han implementado el plan de manejo del riesgo para la vigencia, se debe realizar un monitoreo a través de seguimientos programados, evaluaciones o auditorías con el fin de evaluar la **eficacia** de las acciones tomadas para abordar los riesgos y si estás han impactado (**efectividad**), en términos de:

- ✓ La disminución de la valoración del riesgo (calificación del riesgo residual).
- ✓ Logro de los objetivos institucionales concertados en el Plan Estratégico Institucional (PEI) y Plan de Acción Institucional (PAI).
- ✓ Logro de los objetivos de los procesos.
- ✓ Cumplimiento en las características de calidad definidas para los bienes y servicios que la Entidad suministra. (Las características de calidad se encuentran definidas en los documentos del proceso, así como en las regulaciones normativas aplicables).
- ✓ Los Líderes de procesos, como primera línea de defensa, reportan el estado de avance del tratamiento de los riesgos a cargo. La consolidación de los riesgos en todos los niveles será reportada por la Oficina Asesora de Planeación e Innovación Institucional como segunda línea de defensa hacia la alta dirección.
- ✓ En el caso de los riesgos de seguridad de la información se debe reportar en el mapa y planes de tratamiento correspondientes.
- ✓ El Oficial de Seguridad apoyará y acompañará a las diferentes líneas de defensa tanto para el reporte como para la gestión y el tratamiento de estos riesgos.
- ✓ El monitoreo y revisión de los riesgos se desarrolla a través de los "Roles y Responsabilidades" descritos en el numeral 6 de la presente guía.

La Oficina de Control Interno a partir de los avances reportados por los responsables de la gestión de los riesgos, debe generar un informe en el cual debe identificar las necesidades de revisión, actualización o mejora en el mapa de riesgos, teniendo en cuenta los siguientes aspectos:

- ✓ La incidencia de los riesgos en el logro de los objetivos
- ✓ La apropiada valoración del riesgo
- ✓ Necesidades de creación, eliminación o modificaciones a los mismos para mejorar su eficacia
- ✓ Alertas tempranas que permiten prevenir la materialización de los riesgos
- ✓ Posibles riesgos emergentes o nuevos riesgos, que se identifican en los seguimientos realizados o como resultados de auditorías

El análisis se realiza sobre el cumplimiento de las acciones propuestas para abordar los riesgos, las cuales deberán estar sustentadas a través de evidencia objetiva (cumplimiento de actividades planificadas en las iniciativas estratégicas, actas, listados, correos, documentos, indicadores, imágenes, etc.), cargada en "GINA" por los Líderes y Responsables de proceso como sustento para dar cuenta de los avances efectivos en la mitigación del riesgo.

Los jefes de Oficina o directores pueden revisar los informes realizados y generar las observaciones pertinentes, asegurando que se implementan las acciones correctivas a que haya lugar. (Ver procedimiento de "Acciones de Mejora" D102PR02 y de "Control de Salidas o Servicios No Conformes" D102PR04).

9.3. Lineamientos para el manejo de riesgos materializados:

A partir de la vigencia 2022, el Equipo de Calidad de la Oficina Asesora de Planeación e Innovación Institucional desarrolló una matriz de consolidación de los riesgos materializados, la cual se reporta a la Oficina de Control Interno y a partir del mes de agosto de la vigencia 2022, se realizó un ajuste al módulo de riesgos de la plataforma GINA, con el fin que cada responsable designado por proceso realice directamente el reporte en la plataforma con el fin de mejorar la evidencia y trazabilidad de los riesgos materializados al interior de la Entidad y fortalecer el rol de la primera línea de defensa en la entidad.

En los casos que el riesgo materializado sea de corrupción, la Oficina de Control Interno debe asegurar que se adelanten las siguientes acciones:

1. Informar a las autoridades de la ocurrencia del hecho de corrupción, si es del caso.
2. Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles.
3. Verificar si se tomaron las acciones de mejora, las cuales deben estar cargadas en la plataforma GINA.
4. Realizar un monitoreo permanente hasta tanto el hecho que lo causo se cierre.

En todos los casos (corrupción, gestión o seguridad digital) las acciones adelantadas en caso de materialización del riesgo se deben centrar implementar acciones de mejora, las cuales deben estar cargadas en la plataforma GINA y de igual forma evaluar los siguientes aspectos:

1. Acciones encaminadas a determinar la efectividad de los controles.
2. Acciones encaminadas a mejorar la valoración de los riesgos.
3. Acciones encaminadas a mejorar los controles.
4. Analizar el diseño e idoneidad de los controles, si son adecuados para prevenir o mitigar los riesgos.
5. Determinar si se adelantaron acciones de monitoreo.
6. Realizar un monitoreo permanente hasta tanto el hecho que lo causo se cierre.

Por último, a partir de la vigencia 2022, se creó un nuevo indicador denominado "Riesgos Materializados", dispuesto en la plataforma GINA, asociado al proceso de Gestión de la Innovación Institucional.

10. GESTION DE LOS RIESGOS DE SEGURIDAD DIGITAL

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

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: "Integridad, confidencialidad o disponibilidad". Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Le corresponde a la primera línea de defensa identificar los activos en cada proceso.

10.1.Identificación de los activos de seguridad de la información

Un activo, es cualquier elemento que tenga valor para la Entidad, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: aplicaciones de la Entidad, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO que utiliza la Entidad para funcionar en el entorno digital. Así la Entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital[2].

Los activos de Información la Entidad pueden ser consultados con el Oficial de Seguridad en la "Matriz de inventarios de activos de información de TI" D103M02F01. Para realizar la identificación de activos relacionados con seguridad de la información, deberá tenerse en cuenta la sección 3.1.6 del a Anexo 4 "Modelo nacional de gestión de riesgo de seguridad de la información en Entidades públicas", del Ministerio de Tecnologías de la Información y las Comunicaciones.

10.2.Identificación del riesgo de seguridad de la información

En la identificación de las amenazas es necesario tener en cuenta cuáles y cuantos activos de información tiene cada proceso bajo su responsabilidad. Es importante considerar que las amenazas pueden causar daño temporal o permanente a los activos, procesos y sistemas de soporte de la Entidad. Algunas amenazas pueden afectar a más de un activo y pueden causar diferentes impactos dependiendo de los activos que se vean afectados. (Ver "Manual de inventario de activos, clasificación y publicación de la información" Código D103M02).

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

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

De acuerdo a lo definido en la "Guía para la administración del riesgo y el diseño de controles en Entidades públicas" versión 05, para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 "Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas" donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla 5. Tabla de amenazas comunes
- Tabla 6. Tabla de amenazas dirigida por el hombre
- Tabla 7. Tabla de vulnerabilidades comunes

Las vulnerabilidades, son fallas o debilidades que afectan la confidencialidad, integridad y disponibilidad de los sistemas. La identificación podrá obtenerse de pruebas de vulnerabilidad, visitas, entrevistas y/o basados en los criterios que la Entidad vea necesarios. Asimismo, es importante tener en cuenta que, la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control

Las posibles amenazas y vulnerabilidades que ocasionan la aparición de un riesgo sobre un activo de información se relacionan a continuación, teniendo en cuenta el tipo de activo:

[2] FUNCIÓN PÚBLICA. Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Bogotá, 2020. Página. 75
[3] Ibíd. Página. 78

Tabla 1. Ejemplos Vulnerabilidades y Amenazas por tipo de activo

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
HARDWARE	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de temperatura	Pérdida del suministro de energía
	Almacenamiento de medios sin protección	Hurto de medios o documentos
SOFTWARE	Ausencia de parches de auditoria	Abuso de derechos
	Ausencia de documentación	Error en el uso
	Tablas de contraseñas sin protección	Falsificación de derechos
	Ausencia de control de cambios eficaz	Manipulación con software
RED	Arquitectura de red insegura	Espionaje remoto
	Envío de contraseñas en texto claro	Espionaje remoto
	Gestión inadecuada de la red	Saturación del sistema de información
PERSONAL	Ausencia de personal	Incumplimiento en la disponibilidad del personal
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de políticas para el uso correcto del correo electrónico	Uso no autorizado del equipo
ENTIDAD	Ausencia de auditorias	Abuso de derechos
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de derechos
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos para el manejo de la información	Error en el uso

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

10.3. Valoración del riesgo de seguridad de la información:

Para esta etapa se deben aplicar los lineamientos de medición de la probabilidad e impacto definidos en la sección 10.1 de la presente guía.

10.4. Controles asociados a la seguridad de la información:

Para mitigar/tratar los riesgos de Seguridad de la información el Ministerio de Ciencia, Tecnología e Innovación aplica los criterios establecidos para la definición de controles del Anexo A de la norma ISO 27001:2013, los cuales también se encuentran en estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”.

Así mismo debe asegurar que cada riesgo cuente con mínimo dos indicadores que permitan evaluar la eficacia y efectividad de los planes de tratamiento implementados de la siguiente manera:

- **Un (1) Indicador de eficacia** que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada proceso de la Entidad.

- **Un (1) Indicador de efectividad** para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

11. GESTIÓN DE RIESGOS DE TI

Los lineamientos desarrollados en este ítem aplican para los proyectos del Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI.

El proceso de identificación y gestión de los Riesgos de TI debe asegurar que no exceden el apetito ni la tolerancia al riesgo institucional de acuerdo con lo definido en el numeral 7.2 Apetito del Riesgo, del presente documento, y deben tratarse los riesgos residuales priorizados, con el fin de optimizar los recursos disponibles y enfocar los esfuerzos institucionales, según lo definido en el numeral 10.3 Tratamiento del Riesgo (medidas de respuesta).

Un escenario de riesgo describe un evento relacionado con TI que puede llevar a un impacto en la Entidad. Para que los escenarios de riesgo sean completos y se puedan utilizar en análisis de riesgos, deben contener los siguientes componentes, que se muestran en la tabla a continuación.

Tabla 2. Componentes del Escenario de Riesgos de TI

Escenario del Riesgo	**Actor**	• Interno (funcionarios, contratistas) • Externo (aliado estratégico o proveedor de TI)
	Tipo de amenaza	• Malicioso • Accidental • Fracaso • Natural
	Acción	• Divulgación • Interrupción • Modificación • Robo • Destrucción • Diseño ineficaz • Ejecución ineficaz • Regulación • Uso inadecuado
	Activo / Recurso	• Personas • Ministerio • Procesos • Infraestructura (Instalaciones, Infraestructura de TI)

		• Arquitectura de Componentes Institucionales (Información, Tecnología, Aplicaciones)

Fuente: Elaboración propia según ISACA (2009)

En relación con los riesgos de TI se deben llevar a cabo las siguientes actividades:

a) Evaluar la gestión de riesgos:

- Establecer el nivel de riesgos de TI que la Entidad está dispuesta a asumir para el cumplimiento de los objetivos estratégicos (apetito del riesgo).
- Evaluar factores de riesgos de TI con anterioridad a la toma de decisiones estratégicas, y dar a conocer a la alta dirección, para que éstas se tomen siendo conscientes de los posibles riesgos.
- Evaluar si el uso de las TI tiene una evaluación y valoración del riesgo adecuada.
- Evaluar actividades de gestión del riesgo de TI para garantizar su alineación con las capacidades institucionales.

b) Orientar la gestión de riesgos:

- Promover una cultura de gestión de riesgos de TI
- Identificar de manera proactiva los riesgos de TI, las oportunidades e impactos potenciales para la Entidad.
- Orientar la integración de la gestión de riesgos de TI y la operación y toma de decisiones institucional.
- Elaborar el plan de comunicación y planes de acción de gestión de riesgos de TI
- Definir y orientar la implementación de mecanismos de respuesta ante riesgos de TI cambiantes, y su notificación.
- Los riesgos de TI, las oportunidades, los problemas y preocupaciones pueden ser notificados por cualquier persona y en cualquier momento.
- El riesgo de TI debe ser gestionado de acuerdo con las políticas definidas para tal fin.
- Identificar objetivos e indicadores claves de gobierno y gestión de riesgos, y definir métodos para su medición.

c) Supervisar la gestión de riesgos

- Supervisar la gestión del riesgo de TI
- Supervisar metas y métricas de gobierno y gestión de riesgos de TI respecto a los objetivos institucionales.
- Informar problemas en la gestión de riesgos al comité institucional definido para tal fin (Comité de gestión y desempeño sectorial e institucional)

Para gestionar los riesgos TI se tiene en cuenta los conceptos del marco de gestión de riesgos TI y el libro de Procesos catalizadores del marco COBIT 5. A fin de identificar, valorar y tratar riesgos de TI en el mapa de riesgos de TI con código D102PR03F01 Identificación y Valoración de Riesgos publicado en el sistema GINA, siguiendo los lineamientos definidos en el numeral 16 para la actualización del mapa de riesgos.

11.1. Roles y Responsables

Rol	Responsables
Evaluar	Comité de Gestión y Desempeño Sectorial e Institucional, Oficina Asesora de Planeación e Innovación Institucional (Encargado de realizar seguimiento a riesgos institucionales), Oficina de Tecnologías y Sistemas de Información
Orientar	Oficina Asesora de Planeación e Innovación Institucional (Encargado de realizar seguimiento a riesgos institucionales), Oficina de Tecnologías y Sistemas de Información
Supervisar	Comité de Gestión y Desempeño Sectorial e Institucional, Oficina de Tecnologías y Sistemas de Información, líderes de proceso

12. GESTION DE LOS RIESGOS DEL SISTEMA DE SEGURIDAD Y SALUD EN EL TRABAJO

La identificación y gestión de los Riesgos del Sistema de Seguridad y Salud en el Trabajo, se realiza mediante la aplicación del procedimiento de "Identificación de peligros, valoración de riesgos y determinación de controles" (A201PR07), a través del cual se identifican los peligros y valorar los riesgos para las operaciones y actividades que generen situaciones adversas que puedan poner en riesgo la salud y seguridad de los servidores públicos, contratistas y visitantes del Ministerio de Ciencia, Tecnología e Innovación, estableciendo los controles para prevenir accidentes de trabajo, enfermedades laborales y pérdidas materiales.

Para el registro de los riesgos identificados se utiliza la "Matriz de Identificación de Peligros y Valoración de Riesgos" (A201PR07AN01).

13. GESTIÓN DE LOS RIESGOS EN LOS PROCESOS DE CONTRATACIÓN

Atendiendo los lineamientos establecidos en el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación", de Colombia Compra Eficiente, y en el "Manual de Contratación" (A206MO1) actualizado, para la administración del riesgo en los procesos de contratación, los responsables de la elaboración de los estudios previos, junto con el grupo interdisciplinario responsable de la parte técnica, financiera y jurídica del proyecto deberán atender los siguientes pasos:

- Establecer el contexto.
- Identificar y clasificar los riesgos.
- Evaluar y calificar los riesgos.
- Asignación y tratamiento de los riesgos.
- Monitorear los riesgos.

Para desarrollar cada uno de los pasos enunciados anteriormente se debe tener en cuenta lo establecido en el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación", publicado en la página web de Colombia Compra Eficiente, en el siguiente enlace: https://www.colombiacompra.gov.co/manuales-guias-y-pliegos-tipo/manuales-y-guias

Para la valoración del riesgo se debe consultar el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación", en el enlace: https://www.colombiacompra.gov.co/manuales-guias-y-pliegos-tipo/manuales-y-guias

De acuerdo con lo definido en al Manual de Contratación (A206MO1), los estudios y documentos previos son el soporte para elaborar el proyecto de pliegos, los pliegos de condiciones, y el contrato. Deben contener los siguientes elementos:

(i) La descripción de la necesidad que se pretende satisfacer con el Proceso de Contratación.

(ii) El objeto a contratar, con sus especificaciones, las autorizaciones, permisos y licencias requeridos para su ejecución, y cuando el contrato incluye diseño y construcción, los documentos técnicos para el desarrollo del proyecto.

(iii) La modalidad de selección del contratista y su justificación; incluyendo los fundamentos jurídicos.

(iv) El valor estimado del contrato y la justificación de este. Cuando el valor del contrato esté determinado por precios unitarios, se debe incluir la forma como se calculó y soportar los cálculos de presupuesto en la estimación de aquellos.

(v) Los criterios para seleccionar la oferta más favorable.

(vi) El análisis de Riesgo y la forma de mitigarlo.

(vii) Las garantías que se exigirán en el proceso de Contratación.

(viii) La indicación de si el proceso de contratación está cobijado por un Acuerdo Comercial.

(ix) Análisis del sector desde la perspectiva legal, comercial, financiera, organizacional, técnica y de análisis de riesgo.

La elaboración de los estudios y documentos previos será responsabilidad de la dirección técnica o área que requiere la contratación directamente o a través de las coordinaciones creadas para apoyar el ejercicio de las funciones asignadas.

14. RIESGOS RELACIONADOS CON CALIDAD ESTADÍSTICA

El Ministerio de Ciencia, Tecnología e Innovación en cumplimiento del Plan de Trabajo para la implementación de la Política de Gestión de la Información Estadística del MIPG y teniendo en cuenta los requisitos de la Norma Técnica de la Calidad del Proceso Estadístico NTCPE 1000:2020, emitida por el Departamento Nacional de Estadística y como miembro del Sistema Nacional de Estadística, se encuentra implementando los requisitos de esa norma para las operaciones estadísticas bajo responsabilidad de la entidad, que se encuentran incluidas en Plan Estadístico Nacional.

En el marco del cumplimiento de esta norma técnica, el Ministerio ha identificado dentro del Mapa de Riesgos, aquellos que tienen relación directa y podrían afectar la calidad de las operaciones cubiertas por el alcance de la NTCPE 1000:2020, siendo los siguientes:

a) **Gestión de la Planeación Institucional:**

R17- Posibilidad de afectación reputacional por reportes o respuesta a requerimientos internos o externos sobre información estadística oficial de la Entidad sin calidad ni oportunidad, debido a las falencias de los reportes y análisis cargados en GINA, por parte de las áreas técnicas.

R70 - Posibilidad de Daño en la Data o en la información del Ministerio debido a interrupciones del servicio por cortes de electricidad, fallos de hardware, daño de los sistemas de climatización del datacenter y daño y/o descarga de las baterías del equipo UPS, daños provocados por mal funcionamiento de los equipos tecnológicos, ataques cibernéticos, etc. Afectando el principio de Integridad.

R59 - Posibilidad de afectación económica y reputacional debido a la toma de decisiones unilaterales y no participativa para la obtención de un beneficio en favor de un tercero que no refleja el interés institucional y puede generar un detrimento patrimonial.

b) Gestión de la Innovación Institucional:

R19 Posibilidad de afectación reputacional por incumplimiento de requisitos aplicables al SGC debido a desconocimiento de requisitos por parte de los responsables, debilidades en la consulta de información para la toma de decisiones, ausencia o debilidad en los lineamientos, subregistros y debilidades en la formación de planes de mejora.

R20 Posibilidad de afectación reputacional y económica por incertidumbre, reprocesos y desgaste administrativo, debido a la duplicidad de esfuerzos para el cumplimiento de requisitos relacionados con el Sistema de Gestión de la Calidad y el Modelo Integrado de Planeación y Gestión, generando ineficacia de las acciones, de los indicadores y/o procedimientos implementados por los líderes y responsables de proceso.

R30 Posibilidad de afectación reputacional por el favorecimiento a particulares debido conflictos de interés no identificados

c) Gestión de Tecnologías y Sistemas de Información:

R22 Posibilidad de afectación reputacional por la capacidad en la interoperabilidad de los sistemas de información que permitan responder a las necesidades operativas y de acceso a la información de los grupos de valor y de interés.

R75 Posibilidad de afectación de reputación Institucional, debido a Incumplimiento en las políticas de TI y seguridad y privacidad de la información

d) Gestión de las Comunicaciones:

R3 Posibilidad de afectación reputacional por manipular la información de la Entidad de forma inapropiada revelando u ocultando datos que son relevantes hacia los grupos de valor y grupos de interés de la Entidad, con el fin de obtener un beneficio directo o indirecto a quien la manipuló.

e) Gestión del Conocimiento para la CTeI:

R29 Posible pérdida reputacional por debilidades en lineamientos de política para la caracterización de las capacidades de CTeI de actores del SNCTI generados por baja capacidad al interior del Ministerio, debilidades en los sistemas de información y alto volumen de requerimientos de información.

R69 Posibilidad de indisponibilidad de la información, debido a interrupciones del servicio por cortes de electricidad, fallos de hardware, daño de los sistemas de climatización del datacenter y daño y/o descarga de las baterías del equipo UPS, daños provocados por mal funcionamiento de los equipos tecnológicos, ataques cibernéticos. etc.

R68 Posibilidad de Acceso indebido o mal intencionado a las plataformas tecnológicas del Ministerio, generando perdida o alteración de información, debido a las vulnerabilidades de las plataformas tecnológicas del Ministerio.

R70 Posibilidad de Daño en la Data o en la información del Ministerio debido a interrupciones del servicio por cortes de electricidad, fallos de hardware, daño de los sistemas de climatización del datacenter y daño y/o descarga de las baterías del equipo UPS, daños provocados por mal funcionamiento de los equipos tecnológicos, ataques cibernéticos, etc. Afectando el principio de Integridad.

R74 Posibilidad de Daños o fallas en la infraestructura del datacenter del Ministerio por eventos relacionados con la infraestructura física como: (Derrumbes, Incendios, Inundaciones, entre otros) afectando la disponibilidad, confidencialidad e integridad de la información del Ministerio, debido a daños o fallas en la infraestructura tecnológica y física del datacenter.

f) Trámites y Servicios:

R1 Posibilidad de afectación reputacional y económica en la que puede incurrir la entidad a respuestas de PQRDS que no cumplan con los atributos de pertinencia, calidad y oportunidad y que incumplan con los tiempos establecidos en la normatividad vigente para su contestación.

g) Evaluación y Control:

R77 Posibilidad de afectación reputacional por incumplimiento del Plan Anual de Auditorías, Evaluaciones y Seguimientos de la vigencia, debido a la no asignación de los recursos financieros, insuficiente personal de planta y un óptimo manejo de información física y electrónica, que garantice la adecuada respuesta a requerimientos de la Entidad.

h) Talento Humano:

R37 Posibilidad de afectación reputacional por formular un programa de capacitación que no responda a las necesidades de la Entidad debido a que no se tuvo en cuenta las necesidades de capacitación de los procesos.

R38 Posible afectación reputacional por pérdida del conocimiento o memoria institucional debido a que los Servidores Públicos o Contratistas terminan su vinculación o relación contractual con la Entidad sin realizar su debida entrega.

i) Gestión Contractual:

R11 Posibilidad de afectación reputacional por orientar en beneficio propio o de un tercero la contratación de la Entidad.

R12 Posibilidad de afectación reputacional y/o económica por autorizar pagos o emitir avales debido al incumplimiento de las obligaciones contractuales.

R52 Posibilidad de afectación económica por celebrar contratos o convenios ó iniciar su ejecución, sin cumplir con los requisitos legales.

j) Gestión documental:

R48 Posibilidad de afectación reputacional por pérdida de la información institucional debido a la inadecuada administración de los archivos de la Entidad.

Los riesgos anteriormente mencionados se encuentran disponibles para consulta en la Plataforma Tecnológica GINA, Módulo Riesgos y se han documentado aplicando los criterios definidos en la presente Guía.

15. ACTUALIZACIÓN DEL MAPA DE RIESGOS

El mapa de riesgos es revisado y actualizado cuando el proceso presente cambios en su objetivo, alcance y/o actividades, o cuando el contexto estratégico presente un cambio significativo que requiera la revisión completa de los riesgos gestionados, teniendo como mínimo una revisión y/o actualización anual a partir de última fecha de revisión.

Los riesgos identificados podrán ser actualizados de forma individual, cuando así se requiera, tomando como insumos las necesidades de ajuste identificadas en auditorías internas, revisión por la dirección, auditorías externas o resultado de las acciones de seguimiento y autocontrol ejecutadas por los líderes y responsables de proceso.

La actualización o ajuste estará a cargo de los líderes y responsables de procesos (primera línea de defensa), quienes con el acompañamiento de la Oficina Asesora de Planeación e Innovación Institucional y basados en las acciones de seguimiento o autocontrol al proceso, las recomendaciones de seguimiento generadas por la Oficina de Control Interno, auditorías internas, revisión por la dirección o auditorías externas procederán a realizar los ajustes de los riesgos a su cargo.

Con el fin de facilitar la formulación de los riesgos se utilizarán los siguientes formatos, que contienen los aspectos para tener en cuenta "Identificación y valoración de riesgos" D102PR03F01 para el caso de los riesgos de corrupción, gestión y seguridad digital. Para el caso de los riesgos de seguridad y salud en el trabajo su identificación se debe realizar de acuerdo con lo definido en el Formato "Identificación de peligros y valoración de riesgos de seguridad y salud en el trabajo" A201M02F01, su gestión se encuentra en la "Matriz de Gestión de Riesgos de Seguridad y Salud en el Trabajo" (A201PR07AN01).

16. METODOLOGÍA PARA LA GESTIÓN DE LAS OPORTUNIDADES

Con el fin de realizar la gestión de las oportunidades, una vez realizada su identificación en la definición del Contexto Estratégico en la Entidad se realiza su análisis a fin de proponer iniciativas estratégicas que permitan abordar las oportunidades y promover el logro de los objetivos estratégicos de la Entidad. Los líderes y responsables de proceso son los responsables de proponer las iniciativas estratégicas que desde los programas a cargo permitan maximizar las oportunidades identificadas y de este modo asegurar el cumplimiento de los resultados planificados.

Así mismo, los líderes y responsables de proceso deben realizar el reporte de los avances en el desarrollo de la iniciativa estratégica propuesta, de conformidad con los plazos establecidos y los lineamientos para el reporte definidos en la "Guía para la Planeación, Seguimiento y Evaluación de la Gestión" D101PR01G01 y la "Guía de reporte y seguimiento a la gestión" D101PR01G02.

La Oficina Asesora de Planeación e Innovación Institucional es la instancia responsable de brindar asesoría técnica para la definición y articulación de oportunidad priorizada con la iniciativa propuesta por el Líder o Responsable del proceso, garantizando su coherencia con los objetivos y metas definidos en el Plan Estratégico Institucional (PEI) y Plan de Acción Institucional (PAI).

Trimestralmente la Oficina Asesora de Planeación e Innovación Institucional, consolida el avance en las iniciativas propuestas a través del seguimiento al Plan de Acción Institucional e Innovación Institucional, socializando los resultados en el Comité Ministerial y/o Comité de Gestión y Desempeño Sectorial e Institucional, a fin de facilitar la toma de decisiones frente a los avances obtenidos. La evaluación de la eficacia de las acciones tomadas para abordar las oportunidades se realiza teniendo en cuenta el resultado obtenido en las metas programáticas y estratégicas a las cuales aporta la iniciativa propuesta.

En conclusión, las oportunidades de la Entidad se encuentran directamente articuladas con las iniciativas estratégicas desarrolladas en el Plan Estratégico Institucional (PEI) y Plan de Acción Institucional (PAI) vigentes.

17. COMUNICACIÓN Y CONSULTA

Teniendo en cuenta que la comunicación y consulta con las partes involucradas tanto internas como externas debe tener lugar durante todas las etapas del proceso para la gestión del riesgo y las oportunidades, el Ministerio de Ciencia, Tecnología e Innovación determina las siguientes actividades para asegurar una adecuada divulgación y participación:

- ✓ La Ata Dirección establecerá y actualizará la Política de Gestión de Riesgos, asegurando su socialización en todos los niveles de la Entidad a través de los Comités Estratégicos y de Gestión, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

- ✓ El mapa de Riesgos del Ministerio de Ciencia, Tecnología e Innovación deberá ser divulgado y estará cargado en la plataforma GINA / Módulo de Riesgos para consulta de la Comunidad del Ministerio de Ciencia, Tecnología e Innovación. A partir de esto, los funcionarios y colaboradores podrán revisar y retroalimentar en términos de aportar su conocimiento en la identificación, análisis y valoración del riesgo, así como en la ejecución de las acciones definidas para el tratamiento de los riesgos priorizados.
- ✓ Los líderes y responsables de cada proceso (Directores Técnicos/ Jefes de Oficina / Responsables de Equipo o Grupo de Trabajo), deben divulgar y sensibilizar al interior de sus dependencias el mapa de riesgos junto con el plan de manejo y políticas de operación que se derivan, reportando a la segunda línea sus avances y dificultades.
- ✓ La Oficina Asesora de Planeación e Innovación Institucional y la Oficina de Control Interno, impulsarán a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.
- ✓ Las acciones de tratamiento de los riesgos priorizados que involucren partes interesadas o terceros serán dadas a conocer, por parte de los líderes y responsables de cada proceso.
- ✓ La consolidación del Mapa de Riesgos de Corrupción le corresponde realizarla al jefe de planeación o quien haga sus veces, quien servirá de facilitador en el proceso de Gestión de Riesgos de Corrupción con las dependencias.
- ✓ La consulta y divulgación del Mapa de Riesgos de Corrupción a partes interesadas y comunidad en general se realizará a través de su publicación en la página web de la Entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.
- ✓ Para la gestión de las oportunidades se debe asegurar el reporte periódico del avance en la ejecución de las iniciativas estratégicas, por parte de los líderes y responsables de proceso (Directores Técnicos/ Jefes de Oficina / Responsables de Equipo o Grupo de Trabajo).
- ✓ La Oficina Asesora de Planeación e Innovación Institucional consolidará trimestralmente el avance en la ejecución de las iniciativas, socializando los resultados a través del Comité Ministerial y/o de Gestión y Desempeño Sectorial e Institucional. La consulta y divulgación del avance de las iniciativas a las partes interesadas y comunidad en general se realizará a través de la publicación de los seguimientos al Plan de Acción Institucional (PAI), en la página web de la Entidad.
- ✓ Los riesgos de seguridad digital deberán ser reportados a las autoridades o instancias respectivas que el gobierno disponga, para lo cual el oficial de seguridad asegurará su monitoreo periódico.
- ✓ Le corresponde a la Oficina de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la Entidad, para lo cual, debe dar a conocer a toda la Entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

18. ALINEACIÓN CON LA POLÍTICA DE LUCHA CONTRA LA CORRUPCIÓN Y DE EFICIENCIA ADMINISTRATIVA

Teniendo en cuenta que el Gobierno Nacional viene impulsando y desarrollando diferentes políticas públicas con miras a disminuir los niveles de corrupción en todos los ámbitos. La Secretaría de Transparencia de la Presidencia de la República en cumplimiento del artículo 73 de la Ley 1474 de 2011 diseñó una metodología para que todas las Entidades determinen su Plan Anticorrupción y de Atención al ciudadano, la cual contempla como uno de sus componentes el levantamiento de los mapas de riesgos asociados a posibles hechos de corrupción.

Entendiendo que los riesgos de corrupción se convierten en una tipología de riesgos que debe ser controlada por la Entidad, éstos deben incorporarse en primera instancia en el mapa de riesgos del proceso, sobre el cual se han identificado, de modo tal que el responsable o líder del mismo pueda realizar el seguimiento correspondiente, en conjunto con los riesgos de gestión propios del proceso, evitando que se generen mapas separados de gestión y de corrupción, lo que promueve que el responsable tenga una mirada integral de todos los riesgos que pueden llegar a afectar el desarrollo de su proceso.

En este sentido, es importante precisar que el seguimiento a los riesgos de corrupción en primer lugar es responsabilidad de los líderes de los procesos en los cuales fueron identificados, así mismo de la Oficina de Asesora de Planeación e Innovación Institucional quien realiza seguimiento y finalmente de la Oficina de Control Interno quien es la encargada de evaluar la efectividad de los controles y determinar si se han materializado o no este tipo de riesgos.

En todos los casos se debe asegurar la gestión de riesgos de corrupción, a fin de evitar que se impacten los resultados del Plan Estratégico Institucional (PEI) y Plan de Acción Institucional (PAI).

19. CONTROL DE LAS SALIDAS NO CONFORMES

En el Ministerio de Ciencia, Tecnología e Innovación, la no conformidad que se presenta en un producto o servicio prestado, debido al no cumplimiento de la característica de calidad definida en los procedimientos, normas legales y demás documentos del proceso, se relaciona directamente con la materialización de un riesgo.

De esta manera, es importante revisar la matriz "Matriz de identificación del producto o servicio no conforme" (D102PR04AN01), la cual establece que si se detecta la materialización del riesgo es necesario analizar su efecto y generar acción correctiva, de ser requerido.

El tratamiento respectivo del Producto y Servicio No Conforme se realiza de acuerdo con lo establecido en el procedimiento de "Control de Salidas o Servicios No Conformes" (D102PR04).

BIBLIOGRAFÍA

BRITISH STANDARD. Information Technology – Security Techniques – Information Security Risk Management. ISO/IEC 27005. 2008.

COSO, COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. (2017). Enterprise Risk Management. Integrating with Strategy and Performance. Durham: Association of International Certified Professional Accountants.

COSO, FLAI, PRICE WATERHOUSE COOPERS (2005). Administración de Riesgos Corporativos –Marco Integrado (Técnicas de aplicación).

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA -DAFP (2022). Guía para la administración del riesgo y el diseño de controles en Entidades Públicas. Versión 06. Disponible en: https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238

Instituto de Auditores Internos de Colombia. (2017). MARCO INTERNACIONAL PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORÍA INTERNA. Bogotá D.C. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad

THE INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS -INTOSAI (2000). Guía para las normas de control interno del sector público.

CONTROL DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la Modificación
00	2020-03-30	Todos	Se crea el documento en el Ministerio de Ciencia, Tecnología e Innovación.
01	2021-04-26	3, 4, 7, 8, 9, 10, 11, 12 Control de cambios	Se ajustan los lineamientos de acuerdo con lo definido en la versión 5 del documento "Guía para la administración del riesgo y el diseño de controles en Entidades Públicas" emitida por el Departamento Administrativo de la Función Pública. Se ajusta la instancia de aprobación del Comité de Gestión y Desempeño Institucional y Sectorial al Comité de Coordinación de Control Interno.
02	2022-10-04	Todos	Se articulan los contenidos de la Guía con los lineamientos del Manual Operativo del MIPG V04. Precisar los lineamientos de manejo, monitoreo y materialización de riesgos que se encuentran desarrollados en la Entidad para la vigencia 2022. Se ajustó el documento con el fin de referenciar los lineamientos dispuestos en la guía para la administración del riesgo y el diseño de controles en entidades públicas al igual que la cartilla del Modelo Integrado de Planeación y Gestión. Se depuró el documento para evitar que fuera una transcripción guía para la administración del riesgo y el diseño de controles en entidades públicas. Se incluyeron criterios para la gestión del riesgo de TI y calidad estadística.
03	2023-11-29	13. Todos	Para los Riesgos Relacionados con Calidad Estadística, se elimina la denominación del año. Se actualizan los enlaces que redireccionan a las versiones de los documentos vigentes del DAFP

Versión 01

Elaboró	Revisó	Aprobó
Nombre: Adriana Pereira Oviedo Lorena Arias Puentes Laura Jimena Cuellar	**Nombre:** Adriana Pereira Oviedo	**Nombre:** Comité Institucional de Coordinación de Control Interno
Cargo: Contratistas Oficina Asesora de Planeación e Innovación Institucional	**Cargo:** Contratista Oficina Asesora de Planeación e Innovación Institucional – Líder Sistema de Gestión	**Cargo:** Comité Institucional de Coordinación de Control Interno

Versión 02

Elaboró	Revisó	Aprobó
Nombre: Luis Felipe Giraldo Romero Gloria Rocío Pereira Oviedo Erika Chacón Gamba	**Nombre:** Gloria Rocío Pereira Oviedo Erika Chacón Gamba	**Nombre:** Sandra Lucía Lozano Vargas
Cargo: Contratista Oficina Asesora de Planeación e Innovación Institucional Líder Calidad Oficina Asesora de Planeación e Innovación Institucional Contratista Oficial de Seguridad	**Cargo:** Contratista Oficina Asesora de Planeación e Innovación Institucional – Líder Sistema de Gestión Contratista Oficial de Seguridad - Oficina Tecnología y Sistemas de Información.	**Cargo:** Jefe Oficina Asesora de Planeación e Innovación Institucional (E)

Versión 03

Nombre: Pedro Antonio Pardo Lagos Leidy Liliana Ríos Martínez Martha Lucía Quintero García	**Nombre:** Leidy Liliana Ríos Martínez Martha Lucía Quintero García	**Nombre:** Leidy Liliana Ríos Martínez
Cargo: Contratistas Oficina Asesora de Planeación e Innovación Institucional	**Cargo:** Contratistas Oficina Asesora de Planeación e Innovación Institucional	**Cargo:** Contratista Oficina Asesora de Planeación e Innovación Institucional