Guía Metodológica para la Gestión del Riesgo

CÓDIGO: E-SGI-G003
VERSIÓN: 003
FECHA: 30/06/2021

Índice de contenido

Índice de figuras

Índice de tablas

1. Desarrollo

La gestión de riesgos propende por identificar y mitigar la ocurrencia de desviaciones que afecten la misión, visión y los objetivos estratégicos y de proceso del Instituto de Hidrología, Meteorología y Estudios Ambientales (Ideam). Por lo anterior, se han definido los elementos para la administración de riesgos con base en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas", del Departamento Administrativo de la Función Pública.

1.1 Objetivo

Establecer un esquema para ejercer una correcta y eficiente administración de los riesgos del Instituto, mediante la implementación de políticas, procedimientos y controles que permitan mitigar la probabilidad de ocurrencia de los eventos que afecten los objetivos estratégicos institucionales. Como consecuencia, dicho esquema de acciones se debe orientar hacia la calidad de los procesos y la eficiencia de sus servidores para apoyar la toma de decisiones por parte de la alta dirección.

1.2 Alcance

Abarca tanto los procesos definidos en el "Modelo de gestión por procesos" como las tareas desarrolladas por los servidores públicos que hacen parte de las sedes central, aeropuertos, estaciones y áreas operativas del Ideam. Incluye la identificación de los riesgos de corrupción y de operaciones estadísticas y estratégicas; la seguridad digital operativa o de gestión. Abarca la identificación, el análisis, la valoración, el tratamiento y monitoreo por parte de la Oficina Asesora de Planeación y el seguimiento de riesgos por parte de Control Interno.

1.3 Política de administración del riesgo

El Ideam es una institución pública de apoyo técnico y científico que genera conocimiento, produce información en hidrología, meteorología y estudios ambientales de manera confiable, consistente y oportuna. Facilita la definición y ajustes de la política ambiental en Colombia y la toma de decisiones por parte de los sectores público, privado y de la ciudadanía en general. En su quehacer adopta las medidas para administrar los riesgos de corrupción, seguridad digital y estratégicos, con el fin de establecer controles efectivos que se orienten a mitigar la ocurrencia de eventos que afecten los objetivos estratégicos de la entidad.

Por lo anterior, se establece que los riesgos de corrupción que la entidad identifique en los diferentes procesos tendrán la connotación de "no aceptables" y su tratamiento se orientará a reducir el riesgo. Para los demás tipos de riesgos se aceptarán aquellos cuya zona de riesgo final se encuentre valorada en "bajo". La descripción, monitoreo y seguimiento de estos

riesgos podrán ser consultados en la página web de la entidad, en el enlace de transparencia y acceso a la información pública de acuerdo con el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015, a más tardar el 31 de enero de cada año.

La entidad se compromete a establecer canales y herramientas que promuevan valores encaminados a controlar y a responder frente a los acontecimientos y potenciales acciones de riesgos de corrupción, de operatividad y de proceso de seguridad digital. Estos compromisos serán posibles con la participación de los servidores públicos y demás colaboradores. Por último, dado que la estructura por procesos es dinámica y cambiante en el tiempo, los instrumentos diseñados para la administración del riesgo son susceptibles de mejora y serán revisados permanentemente.

1.4 Marco normativo

La gestión de los riesgos en el Instituto se enmarca en el siguiente conjunto de normas que rigen la administración del riesgo como apoyo al buen gobierno corporativo y mejoresmedidas de control en las entidades.

Constitución Política de Colombia de 1991, artículo 209. La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.
Constitución Política de Colombia, artículo 269. En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas.
Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
Ley 489 de 1998. Estatuto Básico de Organización y funcionamiento de la administración pública.
Decreto 2145 de 1999. Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del Orden Nacional y territorial y se dictan otras disposiciones. Modificado parcialmente por el Decreto 2593 del 2000.
Directiva Presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.
Decreto 1537 de 2001. Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado.

Ley 872 de 2003. Establece el Sistema de Gestión de la Calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios.
Decreto 943 de 2014. Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
NTCPE 1000 2017.Norma Técnica de la Calidad del Proceso Estadístico. Requisitos de Calidad para la Generación de Estadísticas. DANE-ICONTEC.
NTCPE 1000-2020. Norma Técnica de la Calidad del Proceso Estadístico. Requisitos de Calidad para la Generación de estadísticas. DANE-ICONTEC.

1.5 Términos y definiciones[1]

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Riesgo de gestión: Posibilidad que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencia.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de sus objetivos.

Activo: En el contexto de seguridad digital, hace referencia a 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.

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Vincula al modelo de seguridad y privacidad de la información (MSPI)[2], el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la Dirección para modificar su probabilidad o impacto.

Riesgo de corrupción: Posibilidad que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado.

[1] Tomado de "Guía de administración del riesgo y el diseño de controles en entidades públicas". V5 2020.
[2] Tomado de: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

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

1.6 Roles y responsabilidades

Los roles y las responsabilidades en la gestión del riesgo son de carácter integral y diferenciado, y participan todos los niveles de la gestión institucional. De esta manera se asegura el logro, anticipándose y minimizando los riesgos que pueden afectar a la entidad. Esta gestión se desarrolla mediante las líneas de defensa estratégica y de responsabilidad de la gestión del riesgo y control.

Tabla 1. Líneas de defensa en el Modelo Estándar de Control Interno

Línea de defensa	Conformada por	Funciones
Línea de defensa estratégica	Dirección general, Comité Institucional de Control Interno	Emitir, revisar, validar y supervisar el cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad. Fortalecer el Comité Institucional de Coordinación deControl Interno, incrementando su periodicidad para las reuniones. Evaluar el funcionamiento del Esquema de Líneas de Defensa, incluyendo la línea estratégica. Definir líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. Definir y evaluar la "Política de administración del riesgo". La evaluación debe considerar su aplicación en la entidad, los cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes. Evaluar la política de gestión estratégica del talento humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar).

Línea de defensa	Conformada por	Funciones
Primera línea de defensa	Servidores en sus diferentes niveles, líderes o responsables de proceso	Mantener controles internos efectivos; por consiguiente, identificar, evaluar, controlar y mitigar los riesgos. Aspectos que debe tener en cuenta la línea de defensa: El conocimiento y la apropiación de políticas, procedimientos, manuales, protocolos y otras herramientas que faciliten tomar acciones para el autocontrol en sus puestos de trabajo. La identificación de riesgos y el establecimiento de controles, así como el seguimiento, acorde con su diseño, con el fin de evitar la materialización de estos. El seguimiento a los indicadores de gestión institucionales y de los procesos, según corresponda. La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. La coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la segunda línea de defensa.
Segunda línea de defensa	Jefe de Oficina Asesora de Planeación, líderes o coordinadores de contratación, financiera y de TIC	Asegurar los controles y procesos de gestión del riesgo de la primera línea de defensa para que sean apropiados y funcionen correctamente. Supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas para adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos. Asegurar que los controles y procesos de gestión del riesgo de la primera línea de defensa sean apropiados y funcionen correctamente. Supervisar la implementación eficaz de prácticas de gestión de riesgo. Consolidar y analizar la información sobre temas fundamentales para la entidad, como base para tomar decisiones y acciones preventivas necesarias que eviten materializaciones de riesgos. Trabajar junto a las oficinas de control interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno. Asesorar a la primera línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos. Establecer los mecanismos para la autoevaluación

Línea de defensa	Conformada por	Funciones
		requerida: auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora.
Tercera línea de defensa	Oficina de Control Interno	Evaluar de manera independiente y objetiva los controles de segunda línea de defensa para asegurar su efectividad y cobertura; así mismo, evaluar los controles de primera línea de defensa que no se encuentren cubiertos y los que inadecuadamente son cubiertos por la segunda línea de defensa. A través de su rol de asesoría, dar orientación técnica y hacer recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces, con enfoque hacia el cumplimento efectivo de los objetivos. Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. Asesorar proactiva y estratégicamente a la Alta Dirección y a los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. Formar a la Alta Dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. Informar los hallazgos y proporcionar recomendaciones de forma independiente.

Fuente: *Manual operativo MIPG*, marzo, 2021.

1.7 Contexto de la organización

El inicio en la administración de los riesgos está dado por la identificación del contexto, normatividad, planes y programas que se desarrollan en el marco de la plataforma estratégica de la entidad. El contexto de la organización comprende la estructura institucional, cultura organizacional, objetivos del proceso, procedimientos relacionados, sistemas de información, recursos humanos y económicos con respecto a condiciones externas económicas, sociales, culturales, políticas, legales, ambientales o tecnológicas que inciden en su gestión. Comprender el contexto permite conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

1.8 Objetivos de proceso

El objetivo del proceso debe dar respuesta a los interrogantes: qué, cómo, para qué, cuando y cuánto. La entidad debe analizar los objetivos estratégicos y revisar que se encuentren

alineados con la misión, la visión institucional, y los objetivos de procesos.

1.9 Matriz de riesgos

El formato E-SGI-F006 "mapa de riesgos" es la herramienta que el instituto definió en su Sistema de Gestión para consignar la información que da cuenta del desarrollo de cada una de las etapas de la presente metodología, y en la que los líderes de proceso deben diligenciaro actualizar el mapa, de acuerdo con las indicaciones y lineamientos definidos en esta *Guía*. Todo lo anterior, con la asesoría y revisión de la Oficina Asesora de Planeación, y a partir de las orientaciones metodológicas establecidas en las guías o herramientas dispuestas para tal fin por el Departamento Administrativo de la Función Pública (DAFP), la Secretaría de Transparencia de la Presidencia de la República y las que puedan ser aplicables en lo que concierne a la administración de riesgos, acorde a la dinámica y necesidades de la entidad.

1.10 Descripción de metodología administración de riesgos

La estructura de la metodología aplicada para la administración de riesgos en el formato de riesgos E-SGI-F006 "mapa de riesgos" se establece de la siguiente manera:

1.10.1 Tipo de riesgo

Tabla 2. Descripción de tipos de riesgo

Tipo	Descripción
Estratégico	Se asocia con la manera que se administra la entidad. Se enfoca a asuntos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, el diseño y la conceptualización de la entidad por parte de la dirección general.
Imagen	Está relacionado con la percepción, reputación y confianza por parte de la ciudadanía hacia la entidad.
Operativo	Corresponde a los riesgos o posibilidad de ocurrencia que afecten los procesos de la entidad, provenientes del funcionamiento y operatividad de los sistemas de información, de la estructura de la entidad y de la articulación interdependencias.
Financiero	Aquellos riesgos o posibilidades de ocurrencia que afecten los estados financieros; esto es, todo lo relacionado con el manejo de recursos, presupuesto, ejecución presupuestal, estados financieros, costos, pagos, excedentes de tesorería, manejo de bienes, entre otros que perjudiquen la sostenibilidad del Instituto.
Cumplimiento	Se asocia con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
Tecnología	Están relacionados con el uso de la tecnología en la entidad para

Tipo	Descripción
	satisfacer sus necesidadesactuales y futuras, y el cumplimiento de la misión.
Corrupción	Se asocia al uso del poder para desviar la gestión de lo público hacia el beneficio privado.
Seguridad digital	Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de los objetivos institucionales y afectar la autonomía, principios e integridad de la entidad. Incluye aspectos relacionados con el ambiente físico y digital, y con las personas.
Operaciones estadísticas	Se asocian a los riesgos que se identifican en el cumplimiento e implementación de la NTCPE 1000 2017. "Norma técnica de la calidad del proceso estadístico". Requisitos de calidad para la generación de estadísticas. DANE-ICONTEC NTCPE 1000-2020. "Norma técnica de la calidad del proceso estadístico". Requisitos de calidad para la generación de estadísticas. DANE-ICONTEC.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

1.10.2 Impacto: Análisis de las consecuencias que puede ocasionar a la organización, la materialización del riesgo, en términos de afectación de la reputación, afectación económica o ambas.

1.10.3 Causas inmediatas: Son aquellos factores que generan el riesgo; por ejemplo, falta de procedimientos, falta de capacitación, daño de equipos, caída de redes y daños a activos fijos, entre otros.

1.10.4 Causa raíz: Es la causa principal que origina el riesgo. Los controles se orientarán a mitigar esta causa.

1.10.5 Descripción del riesgo: Consolida el análisis de impacto, causa inmediata y causa raíz. El riesgo se debe redactar en términos de probabilidad.

1.10.6 Clasificación del riesgo: Agrupa el riesgo identificado en criterios.

1.10.7 Valoración del riesgo: Se busca establecer la probabilidad de ocurrencia y el impacto de materialización del riesgo.

1.10.7.1. ***Probabilidad*****:** Se busca establecer la probabilidad y el impacto. Puesto en otros términos, lo que generará como resultado el riesgo residual. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año, lo cual establece determinar la frecuencia con la que se lleva a cabo una actividad.

1.10.7.2. ***Impacto:*** Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles, se debe tomar el nivel más alto**.**

Tabla 3. Criterios para definir la probabilidad

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas 2020.

Tabla 4. Criterios para definir el impacto

	Afectación Económica (o	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de provedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

1.10.7.3. *Definición de impacto para riesgos de corrupción*

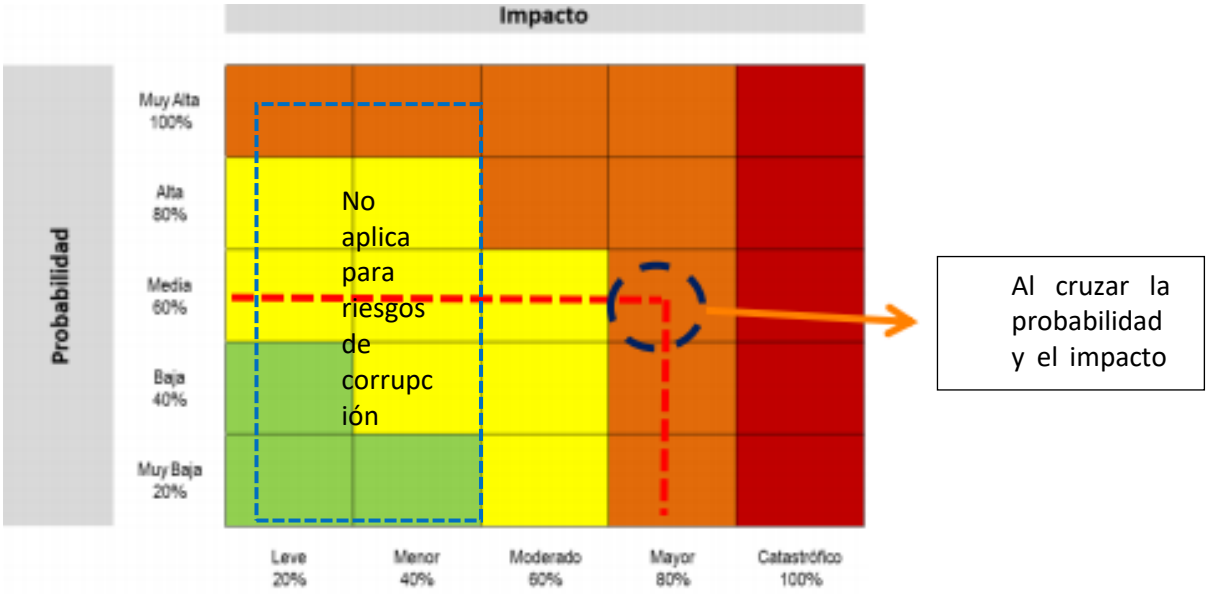
La definición de los riesgos de corrupción se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Se realiza a partir de la respuesta Sí/No a las siguientes preguntas, posteriormente se cuenta el número de respuestas positivas y se verifica con la tabla de validación.

1.10.8 Evaluación de riesgos

A partir del análisis de la probabilidad y sus consecuencias, se establece la zona de riesgo inherente. El riesgo inherente se ubica en 4 zonas de severidad: bajo, moderado, alto y extremo.

Figura 1. Mapa de calor riesgo inherente



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

Apetito al riesgo: El apetito al riesgo será definido por cada proceso de acuerdo con el nivel de impacto que genere su materialización. En general, se aceptan los riesgos cuyo nivel de riesgo final sea bajo e incluya controles de prevención, detección y corrección.
Tolerancia al riesgo: La tolerancia al riesgo se define en cada proceso de acuerdo con los porcentajes de desviación máxima identificados. La tolerancia a los riesgos de gestión, estratégicos y de seguridad digital se califica con nivel alto cuando la valoración esté determinada por el impacto, no por la probabilidad. En riesgos de corrupción no aplica el apetito ni la tolerancia al riesgo.

La evaluación del riesgo se realiza de acuerdo con los resultados que se obtengan en la matriz, teniendo en cuenta la valoración del riesgo residual:

- Si el riesgo se ubica en la zona de riesgo baja la entidad puede asumirlo, esto debido a que se encuentra en un nivel en el que puede ser controlado sin necesidad de tomar medidas

adicionales a las establecidas.

- Si el riesgo se ubica en las zonas moderada o alta, se deben tomar medidas de control adicionales a las actuales que conduzcan a disminuir la probabilidad o la consecuencia o ambas. En lo posible, los riesgos se deben llevar a la zona baja.
- Si el riesgo se ubica en la zona de riesgo extrema, se deben eliminar las causas que generan el riesgo e implementar controles preventivos para evitar la probabilidad de ocurrencia y disminuir el impacto. La decisión debe ser asumida por la Dirección General.

1.10.9 Descripción de controles

Los controles orientados a atacar la causa raíz para prevenir la materialización del riesgo tienen en cuenta que cada líder de proceso o su representante deben definir, implementar y monitorear los controles establecidos.

Para establecer el control se tendrá en cuenta:

- La identificación del cargo que es responsable del control.
- La acción del control se redacta como verbo en infinitivo.
- El complemento o los detalles que identifican el objeto de control.

Tabla 5. Tipología de control y ejecución

Tipo de control	Descripción	Forma de ejecución
Prevención	Control establecido en la entrada del proceso y antes de que se realice la actividad originadora del riesgo.	Manual / automático
Detección	Se identifica durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.	Manual / automático
Corrección	Control accionado en la salida del proceso y después de que se materializa el riesgo.	Manual / automático

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

Tabla 6. Tributos informativos del control

Atributo	Descripción
Documentación	Controles que están documentados en el proceso, ya sea en manuales, procedimientos.
Frecuencia	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.
Evidencia	El registro de evidencias permite probar la ejecución del control.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

Una vez se establecen los controles, se da un movimiento en los ejes de probabilidad o impacto, de acuerdo con el tipo de control aplicado. Los controles de prevención y detección atacan la probabilidad de ocurrencia; y, los controles de corrección atacan el impacto una vez se ha materializado el riesgo. En caso de no contar con controles de corrección, el impacto residual es el mismo calculado inicialmente. Es importante señalar que en este caso no será posible su movimiento en la matriz para el impacto.

El nivel de riesgo final es el resultado del movimiento en los ejes de acuerdo con el tipo de control aplicado.

1.10.10 Estrategia para combatir el riesgo

Consiste en la decisión frente al nivel de riesgo final.

Reducir: Cuando se considera que el riesgo final es alto y se determina tratarlo mediante la mitigación (deducción del riesgo) no es necesario aplicar un control adicional, o la transferencia (tercerizar o trasladar el riesgo), en este la responsabilidad económica recae en el tercero, pero la responsabilidad reputacional no se transfiere.

Aceptar: Una vez analizado el nivel de riesgo se toma la decisión de asumirlo. Es decir, se asume cuando en el documento E-SGI-F006 "Matriz de riegos", la calificación del riesgo, posterior a la aplicación de controles es baja.

Evitar: Si se considera que el riesgo es muy alto se define no asumir la actividad que genera el riesgo.

1.10.11 Plan de tratamiento

El plan de tratamiento describe el modo en que se estructurarán y se llevarán a cabo las actividades complementarias a los controles en la administración de riesgos.
Responsable: Define el líder, el apoyo y los miembros del equipo de gestión de riesgos para cada tipo de actividad del plan de gestión de los riesgos, y explica sus responsabilidades.
Cronograma de implementación de acciones: Se establecen las fechas de inicio y de

terminación para la implementación de las acciones de control. Estos seguimientos se deben hacer dependiendo del nivel de evaluación del riesgo.

Indicador para la evaluación de las acciones implementadas: Se definen los indicadores para medir la eficacia de las acciones implementadas.

1.10.12 Riesgo de corrupción

El riesgo de corrupción es la posibilidad de que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado. A diferencia de los riesgos estratégicos, digitales y de gestión, el impacto de los riesgos de corrupción se valora por medio de las siguientes preguntas:

Tabla 7. Criterios para definir el impacto en riesgos de corrupción

Formato para determinar el impacto de los riesgos de corrupción				
Núm.	Factor	Pregunta: si el riesgo de corrupción se materializa podría:	RESPUESTA	
			Sí	No
1	Recursos	¿Generar pérdida de recursos económicos?		
2	Estrategia	¿Afectar el cumplimiento de misión de la entidad?		
3		¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
4		¿Afectar la generación de los productos o la prestación de servicios?		
5	Imagen/ reputación	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6		¿Generar pérdida de credibilidad del sector?		
7		¿Afectar la imagen?		
8		¿Afectar la imagen nacional?		
9	Ciudadanía	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
10		¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
11	Operacional/ organizacional	¿Afectar al grupo de funcionarios del proceso?		
12		¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
13	Legales	¿Generar intervención de los órganos de control, de la Fiscalía o de otro ente?		
14		¿Dar lugar a procesos sancionatorios?		
15		¿Dar lugar a procesos disciplinarios?		
16		¿Dar lugar a procesos fiscales?		
17	Información	¿Dar lugar a procesos penales?		
18		¿Generar pérdida de información de la entidad?		

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

El impacto de los riegos de corrupción se clasifica por el número de respuestas afirmativas (Sí), así:

Tabla 8. Definición del impacto en riesgos de corrupción por número de respuestas afirmativas

Impacto del riesgo	Número de respuestas afirmativas
Moderado	1 a 5 respuestas
Mayor	6 a 11 respuestas
Catastrófico	12 a 18 respuestas

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020*.

1.10.13 Riesgo de seguridad digital

Estriba en una 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, para lo cual se deben identificar los riesgos que afecten o vulneren las siguientes propiedades de la información:

Tabla 9. Propiedades de la información

Propiedades de la información	Descripción
Confidencialidad	Propiedad de la información que la hace no disponible; es decir, que no puede ser divulgada a individuos, entidades o procesosno autorizados.
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Integridad	Propiedad de exactitud y completitud.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.*

1.10.14 Revisión y evaluación

La evaluación y revisión del riesgo es responsabilidad de la primera línea de defensa, la cual debe:

- Garantizar que los controles son eficaces tanto en el diseño como en la operación.
- Obtener información adicional para valorar el riesgo.
- Analizar y aprender lecciones.
- Verificar, atender e informar la materialización del riesgo.

Como parte del seguimiento a los controles, la primera línea de defensa reportará a la segunda línea de defensa cuatrimestralmente las actividades de control desarrolladas, junto con las evidencias soporte.

Con respecto a los cambios en el contexto estratégico del Instituto o a los cambios en la ejecución de los procesos o procedimientos, estos se deben revisar y actualizar en el mapa de riesgos de gestión, corrupción y seguridad de la información, de lo contrario se verificará que ningún hecho afecte la operación del Instituto.

Un aspecto fundamental para la administración del riesgo son las capacitaciones, las cuales se realizarán unavez al año (interna o externamente), de tal manera que permitan fortalecer las competencias de los servidores públicos, y así garantizar una gestión del riesgo coherente y adecuada dentro de los procesos.

1.10.15 Monitoreo

De acuerdo con la cultura del autocontrol, los responsables de los procesos junto con su equipo realizarán anualmente la elaboración del mapa de riesgos de corrupción y son ellos quienes realizarán el monitoreo y la evaluación permanente al mismo, en los plazos establecidos.
La Oficina Asesora de Planeación revisará que se cumpla con la presente metodología y liderará la consolidación de la información y su publicación. Para lo cual, publicará el mapa de riesgos de corrupción anualmente antes del 31 de enero de cada año y realizará el monitoreo cuatrimestral a la gestión del riesgo.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del mapa de riesgos de corrupción en la página web de la entidad.
- Hacer seguimiento a la gestión del riesgo.
- Revisar los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

- Generar un informe sobre el resultado del monitoreo a los riesgos.

1.10.16 Seguimiento de riesgos

La Oficina de Control Interno realiza el seguimiento de manera independiente y objetiva al cumplimiento tanto de los objetivos institucionales como de los procesos. Asimismo, entrega su informe, de acuerdo con el programa de auditorías, al Comité Institucional de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno. A la par, cuatrimestralmente realiza seguimiento a la gestión del riesgo, basándose en la revisión y resultados del monitoreo a los riesgos identificados y gestionados de la entidad. Las fechas de seguimiento serán las adaptadas por el Ideam para cumplir con las definidas a continuación:

Tabla 10. Fechas de seguimiento a riesgos de la entidad

Seguimiento	Fecha	Publicación
1.er seguimiento	Corte al 30 de abril	Dentro de los diez (10) primeros días del mes de mayo.
2.º seguimiento	Corte al 31 de agosto	Dentro de los diez (10) primeros días del mes de septiembre.
3.er seguimiento	Corte al 31 de diciembre	Dentro de los diez (10) primeros días del mes de enero.

Fuente: *Guía para la gestión del riesgo de corrupción, 2015*.

1.10.17 Materialización del riesgo

En caso de materialización del riesgo, las acciones para seguir irán encaminadas hacia el análisis de causas y ajustes necesarios a la matriz de riesgos. De igual manera se tomarán las siguientes medidas:

Riesgo de corrupción: Informar a las autoridades de la ocurrencia de este hecho; revisar el mapa de riesgos,en particular las causas y los controles; y, realizar un monitoreo permanente para evitar la recurrencia.

Riesgo de gestión y seguridad digital: Hacer una descripción detallada de lo ocurrido y del impacto generadoen el proceso; revisar las causas y los controles. Realizar el análisis del riesgo teniendo en cuenta que varía laprobabilidad; redefinir acciones que eviten la materialización del riesgo y actualizar el mapa de riesgos; y, realizar un monitoreo permanente.

La materialización del riesgo se deberá reportar a la segunda línea de defensa, que a su vez hará lo propioal Comité Institucional de Coordinación de Control Interno, en caso de que la materialización del riesgo haya afectado el cumplimiento de objetivos de la entidad.

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

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el mapa de riesgos de corrupción, en particular las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4) Realizar un monitoreo permanente.

Para los riesgos de corrupción, su materialización puede derivar en acciones legales y pérdida de imagen para el instituto, estas acciones disciplinarias no solo caerán en las personas implicadas, sino también en los líderes de los procesos.

1.10.18 Actualización a la matriz de riesgo

Cuando el equipo responsable del proceso, producto del seguimiento y la revisión quisiera ajustar la redacción de un riesgo, incluir o eliminar algún riesgo identificado al inicio de la vigencia, el responsable del proceso deberá remitir un correo electrónico al jefe de la Oficina Asesora de Planeación con copia al profesional asignado, en el que se indique la justificación por la cual requiere que se realice la inclusión, modificación o eliminación del riesgo. La Oficina Asesora de Planeación realizará el análisis de esa información y generará sus observaciones, las cuales pueden ser aprobadas o no, dependiendo de la justificación aportada. Si los ajustes proceden dará respuesta favorable al proceso vía correo electrónico y se ajustará la matriz de riesgos institucional.

En caso de que sea eliminado un riesgo no se remueve de la matriz de riesgos, este quedará en estado finalizado, manteniendo el número consecutivo asignado, de tal manera que el riesgo mantenga su codificación y se pueda llevar trazabilidad de este.

1.10.19 Comunicación y consulta

El consolidado de los mapas de riesgo se publicará en la página web de la entidad, *link* de transparencia, numeral 6.4 "Planeación".

Se deberá realizar la socialización del mapa de riesgos de corrupción de la entidad a servidores públicos, contratistas y ciudadanía en general, de forma previa a su publicación, con el fin de recibir observaciones para su mejora.

Es responsabilidad de los líderes de proceso la socialización de los resultados obtenidos entre los miembros de su equipo y es responsabilidad de cada servidor consultar permanentemente los riesgos documentados a fin de tener reconocimiento de las situaciones de riesgo existentes y de las nuevas condiciones.

Este documento fue aprobado en sesión del 24 de Junio de 2021, del Comité Institucional de

Coordinación de Control Interno.

2. DOCUMENTOS RELACIONADOS

República de Colombia. Departamento Administrativo de la Función Pública. (2020). *Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020, versión 5*. Bogotá: Departamento Administrativo de la Función Pública, Dirección de Gestión y Desempeño Institucional.

3. BIBLIOGRAFÍA

República de Colombia. Departamento Administrativo de la Función Pública. (2020). *Guía para la administración del riesgo y el diseño de controles en entidades públicas 2020, versión 5*. Bogotá. Departamento Administrativo de la Función Pública, Dirección de Gestión y Desempeño Institucional.

4. CONTROL DE CAMBIOS

Versión	Fecha	Descripción
001	27/08/2019	Creación del documento.
002	19/03/2021	Actualización de la política de administración del riesgo y guía incluyendo los criterios de la guía del DAFP.
003	30/06/2021	Actualización del alcance en el cual se incluyen operaciones estadísticas De igual manera, se actualizan el marco normativo y los roles de las líneas de defensa de acuerdo con el Manual de MIPG, 2021.

ELABORÓ	REVISÓ	APROBÓ
ANA MILENA ÁLVAREZ Contratista Oficina Asesora de Planeación	TELLY DE JESÚS MONTH Jefe Oficina Asesora de Planeación	COMITÉ INSTITUCIONAL DE CONTROL INTERNO