Política de Administración de Riesgos

Oficina de Planeación

Versión 4.0

Acta N° 08 del 14 de junio de 2022.
Comité Institucional de Gestión y Desempeño
Acta N° 04 del 14 de junio de 2022.
Comité Institucional de Coordinación de Control interno

Av Calle 26 # 69 - 76 Edificio Elemento Torre 4 (Agua) Piso 17 y 18, Bogotá D.C.
PBX: [571] 3186800 - 3816710 -Línea gratuita de atención ciudadana: 018000-120205
auditoriageneral auditoriagen auditoriagen auditoriageneralcol
participacion@auditoria.gov.co
www.auditoria.gov.co

CONTENIDO

1. DECLARACIÓN INSTITUCIONAL SOBRE EL COMPROMISO FRENTE A LA GESTIÓN DEL RIESGO

La Auditoría General de la República asume el compromiso de administrar en forma adecuada los diferentes tipos de riesgos: de gestión, de corrupción, soborno y de seguridad de la información, asociados a los objetivos institucionales y estratégicos, los planes, los proyectos y los procesos institucionales. Para el efecto se adoptará la metodología propia para su gestión; se determinarán las acciones de control, tanto de detección como preventivas en la debida oportunidad para evitar su materialización. Así mismo, se adelantará la acción correctiva inmediata frente a esta clase de eventualidades con miras a mitigar las posibles consecuencias y disminuir los niveles de riesgo y en lo posible a un rango aceptable.

INTRODUCCIÓN

El presente documento tiene como base la *Guía para la administración del riesgo y el diseño de controles en entidades públicas*, versión 5, diciembre de 2020, del Departamento Administrativo de la Función Pública. Esta política se establece para asegurar el cumplimiento de la misión institucional, de los objetivos estratégicos y de los procesos.

La política de gestión del riesgo está compuesta por objetivo, alcance, niveles de aceptación del riesgo, niveles para calificar el impacto, tratamiento de riesgos, seguimiento periódico según nivel de riesgo residual y responsabilidad de gestión para cada línea de defensa.

PROPÓSITO DEL DOCUMENTO

Establecer el marco general para las funciones, obligaciones y actividades de servidores públicos y contratistas, encaminado tanto a la adecuada gestión de los riesgos como a los escenarios potenciales de falta en la prestación del servicio (funciones constitucionales, legales y reglamentarias).

Son instrumentos de este propósito la identificación de cada riesgo y las acciones necesarias de acuerdo con su calificación, las respuestas oportunas y las estrategias institucionales, a desarrollar frente a situaciones susceptibles de impactar de manera negativa el cumplimiento de la misionalidad y el logro de los objetivos institucionales, para de esta manera disminuir estas consecuencias, reducir las vulnerabilidades ante las amenazas internas y externas y/o mejorar las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten el talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad.

MARCO NORMATIVO Y METODOLÓGICO

AÑO	NORMA	MATERIA
1991	Constitución Política	Consagra principios de la función administrativa y la obligación de establecer el control interno.
2019	Acto Legislativo 4	Reforma el régimen de control fiscal.
1993	Ley 87	Establece normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.

1998	Ley 489	Dicta normas sobre la organización y funcionamiento de las entidades del orden nacional, expide las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política.
2011	Ley 1474	Dicta normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
2015	Ley 1753	Integra en un Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulados con los Sistemas Nacional e Institucional de Control Interno.
2022	Ley 2195	Adopta medidas en materia de transparencia, prevención y lucha contra la corrupción.
2000	Decreto Ley 272	Determina la organización y el funcionamiento de la Auditoría General de la República.
1999	Decreto 2145	Dicta normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del Orden Nacional y Territorial.
2001	Decreto 1537	Reglamenta 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.
2015	Decreto 1083	Único Reglamentario del Sector de Función Pública.
2017	Decreto 1499	Modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
2020	Decreto 403	Dicta normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.
2013	ISO 27001	Gestión de la seguridad de la información.
2015	ISO 14001	Gestión de los riesgos medioambientales.
2016	ISO 37001	Sistemas de gestión antisoborno.
2018	Guía DAFP	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - versión 4 - octubre de 2018
2020	Guía DAFP	Guía de Auditoría Interna basada en riesgos para entidades públicas - versión 4 - julio de 2020.
2020	Guía DAFP	Guía para la Gestión por Procesos en el marco del Modelo Integrado de Planeación y Gestión - MIPG - versión 1 - julio de 2020.
2020	Guía DAFP	Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 5 - diciembre de 2020.
2019	Manual DAFP	Manual Operativo del Modelo Integrado de Planeación y Gestión Consejo para la Gestión y Desempeño Institucional - versión 3 - diciembre de 2019.

GLOSARIO

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenaza: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

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

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección y el órgano de Gobierno que no sería posible el logro de los objetivos de la entidad.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo

CIGD: Comité Institucional de Gestión y Desempeño.

CICCI: Comité Institucional de Coordinación de Control Interno

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Contingencia: posible evento futuro, condición o eventualidad.

Control: Medida que permite reducir o mitigar un riesgo

Crisis: ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de riesgo: Son las fuentes generadoras de riesgos.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de Riesgos: documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.

MIPG: Modelo Integrado de Planeación y Gestión

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.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales, como la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

Riesgo residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

SIA POAS: Sistema Integral de Auditoría, aplicativo propio para la gestión de la planeación estratégica, los riesgos, los planes de mejora y los indicadores.

Soborno: Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directamente o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona

Nota 1 Lo anterior es una definición genérica. El significado del término “soborno” es el definido por las leyes antisoborno aplicables a la organización y por el sistema de gestión antisoborno diseñado por la organización. (ISO 37001:2016)

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

2. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgos de la Auditoría General de la República, se define por parte de la Alta Dirección de la entidad a través del Comité Institucional de Gestión y Desempeño, acorde con la dimensión de Direccionamiento Estratégico y de Planeación del Modelo Integrado de Planeación y Gestión – MIPG y con la participación del Comité Institucional de Coordinación de Control Interno.

Como base para su formulación se empleó la *Guía para la administración del riesgo y el diseño de controles en entidades públicas*, versión 5, diciembre de 2020, del Departamento Administrativo de la Función Pública.

La administración de riesgos en la Auditoría General de la República, se lleva a cabo a través del módulo de "Administración de Riesgos" del Sistema de Información SIA POAS, herramienta que permite a los líderes de proceso, con el apoyo de la Oficina de Planeación, efectuar la identificación de los riesgos, sus controles y valoración. Así mismo, éste sistema de información, facilita la formulación del Plan de Acción, cuando corresponda, y el seguimiento a las acciones planeadas.

Posteriormente la Oficina de Control Interno, adelanta, como parte de sus funciones, la evaluación de los controles y de las acciones de los planes formulados, con el fin de verificar su efectividad.

La Oficina de Planeación identificará los requerimientos funcionales y revisará en forma periódica su adecuado funcionamiento, así como el cargue de información y la disposición de un manual de uso para el servicio de todos los procesos.

En cada vigencia deberá cumplirse la revisión e identificación de los riesgos institucionales, con base en la metodología vigente. La Oficina de Planeación, una vez definido el Plan Operativo Anual, verificará que las acciones de control estén articuladas con los compromisos de cada proceso.

2.1 OBJETIVO

La política de administración de riesgos busca el cumplimiento de la misión institucional y del plan estratégico institucional, mediante la formulación de controles efectivos y acciones de mitigación para los riesgos identificados en la entidad.

2.2 ALCANCE

La política será aplicable a los once (11) procesos institucionales, así como a los planes y proyectos de la entidad, de conformidad con cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y las correspondientes a las líneas de defensa.

2.3 IDENTIFICACIÓN DE RIESGOS

Para la identificación de riesgos, a continuación, se enuncian las tipologías que se adoptarán en la Auditoría General de la República:

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 pesar de que la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* de diciembre de 2020, no especifica esta tipología, la Auditoría General de la República

recoge el concepto de la guía anterior y lo incorpora en su política, con el fin de ejercer la administración integral de los diferentes riesgos, incluyendo los de corrupción que hacen parte de su Plan Anticorrupción y de Atención al Ciudadano - PAAC.

Soborno: Efecto sobre la incertidumbre o posible hecho de soborno. Esta tipología se adopta en el contexto del Sistema de Gestión Antisoborno bajo la norma ISO 37001:2016 el cual esta implementando la Auditoría General de la República,

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos.

Fraude Externo: Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad)

Fraude interno: Pérdida debida a actos de fraude, actuaciones irregulares, comisión de hechos delictivos, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad, en las cuales está involucrado por lo menos un participante interno de la organización, cometido en forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Fallas tecnológicas: Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

Relaciones laborales: Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

Usuarios, productos y prácticas: Fallas por negligencia o de naturaleza involuntaria, de las obligaciones frente a usuarios, que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos fijos / eventos externos: Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos o eventos externos como atentados, vandalismo o perturbación del orden público.

2.4 VALORACIÓN DE RIESGOS

Determinación de la probabilidad de los riesgos:

La probabilidad se define de acuerdo con la frecuencia en que se lleva a cabo la actividad generadora del riesgo así:

	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%

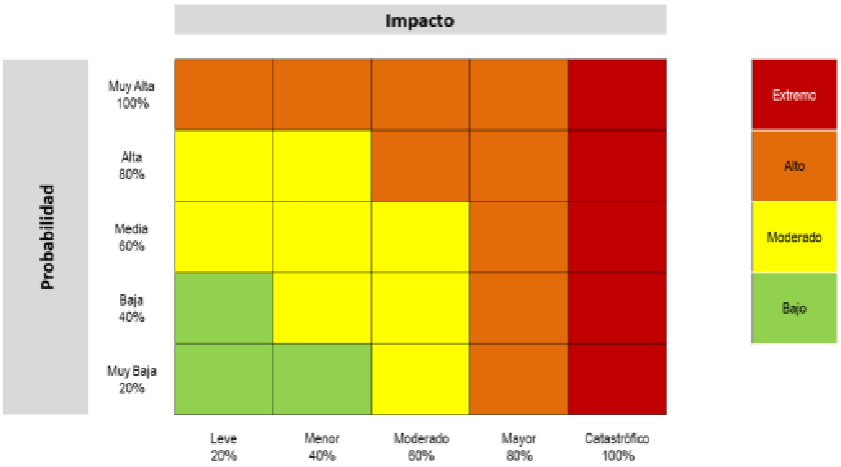
Determinación del impacto de los riesgos:

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Posteriormente se definen los criterios de los cinco (5) niveles, a saber: leve, menor, moderado, mayor y catastrófico.

Como lo menciona la Guía de la Función Pública, "Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo."

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún 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 proveedores.
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 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 publicitario sostenido a nivel país

Como resultado se obtiene el nivel de RIESGO INHERENTE:



De acuerdo con el resultado, los líderes de procesos deben identificar los controles existentes o formular nuevos controles con el fin de reducir la probabilidad o el impacto.

Según el resultado de los controles aplicados se obtiene el RIESGO RESIDUAL, identificado con el mismo mapa de calor presentado anteriormente.

2.5 ESTRATEGIAS PARA TRATAMIENTO DE RIESGOS

Con el resultado del RIESGO RESIDUAL, se definen las siguientes acciones**, por parte de la Función Pública en su metodología son.**

EVITAR. Decisión que se adopta cuando después de un análisis se considera que el riesgo es demasiado alto y lo mejor es NO asumir la actividad que genera el riesgo y por tanto plantear una diferente.

ACEPTAR. Se determina para los riesgos cuyo resultado, una vez aplicados los controles, se encuentra en el nivel de RIESGO RESIDUAL LEVE, MENOR o MODERADO. Estos riesgos requieren monitoreo y seguimiento periódico cuatrimestral por parte de los líderes de procesos.

REDUCIR. Se determina para los riesgos cuyo resultado, una vez aplicados los controles, se encuentran en el nivel ALTO o CATASTRÓFICO. Estos riesgos requieren monitoreo y seguimiento periódico cuatrimestral por parte de los líderes de procesos y, además, exigen la formulación de plan de acción.

Para los riesgos de corrupción, incluidos los riesgos de soborno, no hay aceptación. De otra parte, para los riesgos de corrupción y soborno que se encuentren en un nivel residual Leve o Menor se continuarán aplicando los controles existentes sin necesidad de formular un plan de acción y para los que se encuentren por encima del nivel Menor se formulará plan de acción consistente en la definición de acciones para reducir el nivel del riesgo.

Este plan deberá formularse a través del SIA POAS, en el módulo administración de riesgos, y recogerá la siguiente información

Riesgo	Acción	Responsable	Fecha Inicio	Fecha Cierre	Indicador

2.6 ROLES Y RESPONSABILIDADES

Se definen desde las líneas de defensa y se determinan para la AGR, así:

LINEA DE DEFENSA	ROL	RESPONSABLE
LÍNEA ESTRATÉGICA	**Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento.** Someter a la aprobación del Comité de Gestión y Desempeño Institucional, Comité Institucional de Coordinación de Control Interno - CICCI la política de administración del riesgo previamente estructurada por parte de la Oficina de Planeación, como segunda línea de defensa en la entidad. Hacer seguimiento para su posible actualización; y evaluar su eficacia frente a la gestión del riesgo institucional.	Comité Institucional de Gestión y desempeño. Comité Institucional de Coordinación de Control Interno - CICCI.
LÍNEA ESTRATÉGICA	Recomienda mejoras a la política de operación para la administración del riesgo.	Comité Institucional de Gestión y Desempeño - CGDI.
	Identifica, analiza y valora riesgos para cada proceso institucional.	

PRIMERA LÍNEA DE DEFENSA	Diseña, implementa y monitorea los controles y los gestiona de manera directa. Formula plan de acción a los riesgos, (determina acciones, responsables y fechas de cumplimiento de las acciones). Orienta el desarrollo e implementación de políticas y procedimientos internos y asegura que sean compatibles con las metas y objetivos de la entidad. Desarrolla ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio. Reporta en el SIA POAS, los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. Formula acciones de mejoramiento.	Líderes de los once (11) procesos institucionales. Gerencias seccionales.
SEGUNDA LÍNEA DE DEFENSA	**Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.** Asesora a la línea estratégica en el análisis y definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. Revisa el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. Verifica que las acciones de control se diseñen conforme a los requerimientos de la metodología. Hace seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos. Revisa que el cargue de información en el SIA POAS esté acorde con lo aprobado por el líder del proceso. Acompaña y orienta a los líderes de procesos en la identificación, valoración y evaluación del riesgo. Socializa y publica el mapa de riesgos. Revisa las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y lograr el cumplimiento a los objetivos. Supervisa, en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se	Oficina de Planeación. Servidores de la Oficina de Planeación. Contratistas de apoyo a la gestión de la Oficina de Planeación.

	apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. Evalúa que la gestión de los riesgos esté acorde con la presente política de la entidad y que sean gestionados por la primera línea de defensa.	
	Proporciona información sobre la efectividad del Sistema de Control Interno, a través del enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.	
	Monitorea la gestión de riesgo y control ejecutada por la primera línea de defensa complementando su trabajo.	
TERCERA LÍNEA DE DEFENSA	Revisa los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. Proporciona aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.	Oficina de Control Interno Funcionarios de la Oficina de Control Interno Auditores Internos o quien haga sus veces
	Asesora a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles.	
	Lleva a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditorías internas y reporta los resultados al CICCI.	
	Realiza seguimiento a la implementación de mejoras sobre los lineamientos de continuidad del negocio.	
	Recomienda mejoras a la política de operación para la administración del riesgo.	

Fuente: Adaptada de la Política de Administración de Riesgos en Función Pública. DAFP. Versión 15

2.7 SEGUIMIENTO Y EVALUACIÓN DEL MAPA DE RIESGOS Y CONTROLES

Los líderes de proceso monitorean constantemente los controles definidos para los riesgos y las acciones del plan de acción, cuando haya lugar. Además registran con periodicidad cuatrimestral en el SIA POAS el seguimiento de los mismos.

La Oficina de Control Interno lleva a cabo el seguimiento a la administración del riesgo, de conformidad con lo indicado en los documentos "*Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces*" y "*Estrategias para la Construcción del Plan Anticorrupción y de atención al ciudadano*" del Departamento Administrativo de la Función Pública, y como se determina en el título precedente de Roles y Responsabilidades.

La Oficina de Control Interno presentará un informe cuatrimestral sobre los resultados de la evaluación de la efectividad del Sistema de Control Interno - SCI, acorde con la evaluación de los controles definidos en los mapas de riesgos y de los riesgos de procesos, en el cual se consigne, cuando sea el caso, la materialización, la creación, la modificación o la eliminación de alguno de los riegos.