Política de Administración de Riesgos en la Gobernación de Caldas

Secretaría de Planeación

Julio 2024

Contenido

Compromiso

La política de Administración del Riesgo de la Gobernación de Caldas representa el compromiso institucional, en relación con la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad de negocio que puedan afectar la planificación estratégica, en el marco del Modelo Integrado de Planeación y Gestión- MIPG.

La Gobernación de Caldas se compromete a administrar y mantener niveles aceptables en los riesgos institucionales de gestión, fiscales, corrupción y seguridad digital, mediante el cumplimiento de la metodología propia para su gestión y las acciones de control, detección, identificación y prevención oportunas que permitan:

1. evitar la materialización de los riesgos
2. corregir de manera inmediata las eventualidades presentadas y
3. mitigar las consecuencias ante posibles materializaciones en los diferentes ambientes institucionales

Introducción

La estructuración del presente documento para la Gobernación de Caldas está basada en la guía para la administración del riesgo vigente y el diseño de controles en entidades públicas v.6 y se establece para asegurar el cumplimiento de la misión institucional y los objetivos estratégicos y de proceso. La política está compuesta por el objetivo, alcance, niveles de aceptación al riesgo, niveles para calificar el impacto, el tratamiento de riesgos, el seguimiento periódico según nivel de riesgo residual y responsabilidad de gestión para cada línea de defensa

La Gobernación de Caldas en atención al artículo 2.2.21.5.4 del Decreto 1083 de 2015, el cual establece:" Administración de riesgos. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y la oficina de control interno, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficina de control interno e integradas de manera inherente a los procedimientos".

Lo anterior permite que los riesgos en el ente territorial se constituyan en parte integral del fortalecimiento de su sistema de control interno, de tal manera que se deben establecer y aplicar políticas de administración del riesgo, el compromiso para gestionar, identificar y tratar los riesgos de gestión, riesgo fiscal, de corrupción y de seguridad digital y definir la política de riesgos como un proceso dinámico, continuo y esencial. Por lo tanto, se deben gestionar herramientas que proporcionen la capacidad y la competencia para diagnosticar, priorizar, monitorear y tratar sus riesgos, teniendo en cuenta los cambios en el ambiente interno y externo, de tal forma que no sea sorprendida por riesgos desconocidos y no controlados.

El presente documento establece los lineamientos para la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad del

negocio que puedan afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos y planes institucionales, tomando como referencia las directrices del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI, los requerimientos de la Guía para la administración del riesgo y el diseño de controles en las entidades públicas – Versión 6 de noviembre de 2022 y el Modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital - MSPI.

Propósito del documento

Establecer el marco general de actuación de todos los servidores públicos de la entidad para la adecuada gestión de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, disminuyendo las potenciales consecuencias negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad

Política de administración de riesgos

La política de administración de riesgos de la Gobernación de Caldas, tiene un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión, la guía para la administración del riesgo y el diseño de controles en entidades públicas, ,con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

Aplica para todos los niveles, áreas y procesos de la Entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

Los riesgos de gestión de proceso que puedan afectar el cumplimiento de la misión y objetivos institucionales.
Los riesgos fiscales impiden el daño sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública.
Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.
Los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

La Gobernación de Caldas determina que el módulo de riesgos del sistema de gestión institucional – SGI –(Plataforma almera), es la herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción y de seguridad digital, para lo cual la secretaría de planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento,

cargue de información y dispone un manual de uso para el servicio de todos los procesos.
El periodo de revisión e identificación de los riesgos institucionales se debe realizar cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción anual, asegurando la articulación de éstos con los compromisos de cada proceso.

Objetivos de la política de riesgos

Objetivo principal

Establecer los lineamientos para la adecuada gestión de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de los objetivos institucionales, disminuyendo las potenciales consecuencias, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad asegurando la satisfacción de las necesidades y expectativas de los grupos de valor.

Objetivos específicos

- Alcanzar los más altos niveles de transparencia y publicación durante administración de riesgos institucionales.
- Garantizar el cumplimiento de los requisitos normativos en cuanto a la administración y gestión de riesgos, protegiendo los recursos públicos a través de acciones que permitan reducir, mitigar o eliminar la materialización de riesgos.
- Contemplar en la metodología de administración de riesgos, acciones para la identificación, análisis, valoración, monitoreo y revisión de los eventos potencialmente negativos.
- Promover desde la planeación estratégica, la construcción y actualización participativa de mapas de riesgos de gestión y de corrupción.
- Desplegar a todos los niveles de la organización, los lineamientos institucionales frente a la gestión del riesgo, fortaleciendo el compromiso de los colaboradores y la cultura de prevención y autocontrol.
- Alcanzar un nivel aceptable de riesgos residuales en todos los procesos, a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional.

Alcance

La presente política de Administración de Riesgos Institucionales abarca el manejo de los riesgos asociados a los procesos y acciones definidos por la entidad y ejecutadas por el talento humano y todos aquellos actores que prestan servicios a través de las diferentes modalidades contractuales en el marco del Modelo Integrado de Planeación y Gestión. Esta política incluye riesgos de gestión, riesgos de corrupción, riesgos de seguridad digital y riesgos fiscales, para los cuales se tendrán en cuenta los lineamientos y metodologías que se definan por parte de la entidad para su respectiva gestión. Aplica a todos los procesos, proyectos, servicios y planes de la entidad territorial, conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa.

Definición de términos

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.

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

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

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

Causa inmediata: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

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

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

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.

Contingencia: posible evento futuro, condición o eventualidad.

Continuidad del negocio: capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.

Control: medida que permite reducir o mitigar un riesgo.

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

CIGD: Comité Institucional de Gestión y Desempeño.

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

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.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Restablecimiento: capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.

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

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

Riesgo Fiscal: efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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.

SGI: Sistema Gestión Institucional, aplicativo propio para la gestión de planeación riesgos e indicadores; para la gobernación de caldas se gestiona en la plataforma almera.

TIC: Tecnologías de la Información y las Comunicaciones.

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

MSPI: El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como

referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Niveles de aceptación del riesgo- Apetito del riesgo

Acorde con los riesgos residuales aprobados por los líderes de procesos y socializados en el comité institucional de coordinación de control interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

La Gobernación de Caldas determina que para los riesgos residuales de gestión,fiscales y seguridad digital que se encuentren en zona de riesgo baja, está dispuesta a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

Contexto Estratégico

A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar en cada vigencia, se analiza el entorno estratégico de La Gobernación de Caldas a partir de los siguientes factores internos, externos y de proceso, para el adecuado análisis de las causas del riesgo y gestión de este.

Tabla 1. Contexto Estratégico Gobernación de Caldas

Contexto Estratégico Gobernación de Caldas		
CONTEXTO EXTERNO	Económicos y Financieros	Recursos de inversión, presupuesto, austeridad del gasto, sistemas de registro, compromisos de gobierno, recursos del Sistema General de Regalías (SGR), disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia, entre otros. Un Estado más flexible, competitivo y cercano.
	Internacional	Un Estado más flexible, competitivo y cercano
		Metodologías agiles para la transformación de servicios
		Modernización del Estado
		Evolución de la tecnología
		Retos de continuidad y permanencia
		Colombia en la OCDE (Organización para la Cooperación y el Desarrollo Económico)
	Político/Gobierno	Cambios de gobierno, legislación, políticas públicas, regulación. promoción de mujeres en cargos directivos. Enfoque del Mérito y desarrollo de competencias del plan de gobierno
	Sociales y culturales	Demografía, responsabilidad social, orden público
	Tecnológicos	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea
	Ambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible, desastres naturales, contaminación, epidemias o pandemias (indisponibilidad de personal clave o imposibilidad de acceso a las instalaciones). Las emergencias epidemiológicas pueden permitir evaluar la capacidad de los planes de contingencia institucionales o la materialización de riesgos de no disponibilidad de personal clave.
	Legales y reglamentarios	Normatividad externa (Leyes, decretos, ordenanzas y acuerdos)

Contexto Estratégico Gobernación de Caldas		
CONTEXTO INTERNO	Comunicación externa	Mecanismos utilizados Para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad
	Financieros	Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada
	Personal	Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional
	Procesos	Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento
	Tecnología	Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información
	Estratégicos	Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo
	Comunicación interna	Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones
CONTEXTO INTERNO DEL PROCESO	Diseño del proceso	Claridad en la descripción del alcance y objetivo del proceso
	Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes
	Transversalidad	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad
	Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos
	Responsables del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso
	Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos
	Activos de seguridad digital del proceso	Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso.

Responsabilidades frente a los Riesgos

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:

Tabla 2. Responsabilidades de las Líneas de Defensa

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Línea Estratégica	**Consejo de Gobierno, Comité de Gestión y Desempeño Institucional**	• Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Asegurar la implementación y desarrollo de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo en diferentes ámbitos institucionales. • Generar recomendaciones de mejora a la política de administración del riesgo para su análisis e inclusión.
	Comité Institucional de Coordinación de Control Interno	• Aprobar la política de administración del riesgo previamente estructurada por parte de la secretaria de Planeación Departamental, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización. • Evaluar la eficacia de la política frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. • Monitorear los riesgos críticos identificados (aquellos definidos en los niveles de severidad Alto y Extremo, independientemente de su nivel de probabilidad), mediante el análisis de eventos o materializaciones u otra información aportada por las instancias de 2ª línea identificadas. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios, a partir

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		de la información aportada por las instancias de 2ª línea identificadas. • Garantizar el cumplimiento de los planes institucionales, estratégicos y sectoriales de la entidad.
Primera Línea	**Secretarios de Despacho**	• Promover al interior de su equipo de trabajo el concepto de "administración de riesgo", iniciando por la socialización de la política, su metodología allí desplegada y el marco de referencia aprobado por la línea estratégica. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo. • Delegar, por parte del secretario de Despacho, en (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos. • Informar a la secretaria de Planeación, los cambios de responsables de reporte en caso de ausentismo laboral. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y su documentación se evidencie en los procedimientos de los procesos. • Revisar de acuerdo con su competencia y alcance la documentación del plan continuidad del negocio. • Reportar en el SGI los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Realizar la medición y análisis a la gestión efectiva de los riesgos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		de los controles y determinar las acciones de mejora a que haya lugar. • Revisar 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. • En caso de materialización de un riesgo identificado, Informar a la secretaria de Planeación (segunda línea) y aplicar las acciones correctivas o de mejora necesarias. • En caso de la materialización de un riesgo no identificado, este debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional, con el acompañamiento de la secretaria Planeación. • Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación. • Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir. • Comunicar al equipo de trabajo los resultados de la gestión del riesgo. • Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento. • Revisar y actualizar el mapa de riesgos con el acompañamiento de la secretaria de Planeación.
	Líderes de Proceso	• Realizar la identificación de los riesgos del proceso. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
	Equipos de Trabajo	• Participar en el diseño de los controles que tienen a cargo. • Ejecutar los controles a su cargo de la forma como están diseñados. • Informar a su superior jerárquico sobre riesgos materializados o posibles situaciones de afectación al proceso, a fin de incorporar las acciones a que haya lugar, incluyendo el informe a la secretaria de Planeación. • Proponer mejoras a los controles existentes.
Segunda Línea	**Secretaría de Planeación**	El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el líder del proceso: • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. Asesorar a la línea estratégica en el análisis del contexto interno y externo, incluyendo su actualización, acorde con los cambios en el entorno, la definición de la política de riesgo, el establecimiento de los riesgos al proceso de direccionamiento acorde con los procesos definidos en la Gobernación de Caldas. • Identificar cambios en el entorno (interno o externo) que afecten el apetito del riesgo en la entidad, para su análisis en el CICCI y se adelanten los ajustes que correspondan a este aparte dentro de la presente política. • Capacitar al grupo de trabajo de cada dependencia en la herramienta SGI para la gestión del riesgo con la asesoría del líder de la política de control interno. • Revisar el adecuado diseño de los controles a través de la metodología aplicada en el sistema de gestión institucional para la mitigación de los riesgos que se han establecido por parte de la primera línea de

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. • Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. • Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad. • Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos registrados en el SGI. • Revisar que el cargue de información en el SGI esté acorde con lo aprobado por el líder del proceso. • Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno. • Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos o proyectos. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Coordinar con los líderes de proceso el responsable de reporte de seguimiento a los riesgos, controles y planes de acción en el aplicativo SGI. • Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. • Comunicar a los líderes de proceso a través de los enlaces los resultados de la gestión del riesgo. • Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso) y generar un reporte ejecutivo que permita establecer alertas a la línea estratégica sobre retrasos, incumplimientos u otras fallas detectadas.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		• Socializar y publicar el mapa de riesgos institucional. • Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados que se adelanten al interior de la entidad. • Revisar 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 logar el cumplimiento a los objetivos. • Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos.
	Secretaria de Planeación	El secretario de Planeación (o a quien delegue), mensualmente consolidará el avance sobre la planeación institucional de manera articulada con los temas asociados a los proyectos de inversión y otros requerimientos externos, generando alertas en semáforo sobre retrasos o posibles incumplimientos; al tiempo articulará la información sobre eventos (materializaciones de riesgo) asociados a los mismos permitiendo el análisis integral de la gestión del riesgo. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el secretario de Planeación como gestor del proceso de direccionamiento estratégico.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
	Secretaria de Planeación - secretaria general - Lideres de los Procesos	• Orientar a la primera línea de defensa para definir la estrategia de continuidad del negocio identificando los escenarios. • Actualizar la documentación que soporta la estrategia de continuidad del negocio. Identificar, valorar, evaluar y gestionar los riesgos de pérdida de continuidad del negocio. • Liderar mesas de trabajo para el análisis de impacto de los escenarios en la continuidad del negocio, documentación de los escenarios de riesgos y definición del plan de continuidad del negocio institucional. • Actualizar, según se requiera, los escenarios de riesgos de continuidad y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad. • Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio.
	Secretaria de Planeación	• Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles y las estrategias de continuidad de negocio asociadas a los escenarios de continuidad de negocio bajo su responsabilidad y los temas a su cargo. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. Participar en las pruebas del plan de continuidad del negocio y en la implementación.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
	Secretaria de Planeación - Unidad de Calidad - Lideres de los Procesos	• Identificar, documentar y formalizar políticas, procedimientos, instructivos y formatos para el adecuado funcionamiento de las labores de dirección de proyectos. • Generar espacios de transferencia y gestión de conocimiento que faciliten el desarrollo de competencias y habilidades en el personal encargado de la gestión de proyectos en la entidad. • Generar espacios de trabajo para que los directores de proyecto compartan recursos de conocimiento para mejorar las posibilidades de éxito de los proyectos. • Apoyar a las dependencias en las actividades de formulación, planificación, seguimiento y control a la ejecución y cierre de los proyectos bajo su responsabilidad, así como la identificación, diseño de controles y gestión de los riesgos de los proyectos y sus seguimientos. • Monitorizar el avance global de los proyectos de la entidad para identificar amenazas y oportunidades que puedan afectar el cumplimiento de los objetivos de proyecto. • Mantener información actualizada sobre el avance, logros, dificultades y necesidades de los diferentes proyectos y presentar informes consolidados para el consejo de gobierno.
Tercera Línea	**Jefatura de Control Interno**	• Revisar 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. • Proporcionar 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. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Asesorar a la primera línea de defensa de forma coordinada con la secretaria de Planeación, en la identificación de los riesgos y diseño de controles.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		• Llevar 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 Auditoria y reportar los resultados al CICCI. • Realizar seguimiento a la implementación de mejoras sobre los lineamientos de continuidad del negocio. • Realizar seguimiento a la implementación de la estrategia de continuidad del negocio y a las pruebas efectuadas. • Recomendar mejoras a la política de operación para la administración del riesgo.

De igual manera, la secretaria de Planeación en coordinación con la Unidad de Calidad de la Secretaría General lleva a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Socializar anualmente la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado.

- Capacitar al grupo de trabajo de cada dependencia en la herramienta SIG para la gestión del riesgo.

- Liderar las mesas de trabajo de identificación del riesgo.

- Liderar las mesas de trabajo para determinación del análisis de impacto del negocio, documentación de los escenarios de riesgo y plan de continuidad de negocio institucional.
- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología.

- Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en el SIG.

- Elaborar el mapa de riesgos de proceso con toda la información respectiva, a partir de la información construida con los equipos de trabajo.

- Documentar los escenarios de pérdida de continuidad de negocio que se utilizan para el desarrollo y prueba del plan de continuidad de negocio.

- Revisar que el cargue de información en el SGI esté acorde con lo aprobado.

- Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso.

Por su parte, los líderes de proceso tienen la responsabilidad de:

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.

- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, monitoreo, reporte y socialización de riesgos asociados.

Nivel de calificación de probabilidad para riesgos de proceso y seguridad digital

Tabla 3. Calificación de probabilidad para riesgos proceso y seguridad digital

Nivel	Probabilidad	Descripción
100%	Muy Alta	La actividad se realiza más de 5000 veces al año.
80%	Alta	La actividad se realiza mínimo 500 veces al año y máximo 5000 veces por año.
60%	Media	La actividad se realiza entre 24 a 500 veces al año.
40%	Baja	La actividad se realiza entre 3 a 24 veces al año.
20%	Muy Baja	La actividad se realiza máximo 2 veces al año.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

Nivel de calificación de probabilidad para riesgos de corrupción

Tabla 4. Calificación de probabilidad para riesgos de corrupción

Nivel	Probabilidad	Probabilidad	Descripción
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

Nivel de calificación de probabilidad para riesgos fiscales

Tabla 5. Calificación de probabilidad para riesgos fiscales

Nivel	Probabilidad	Descripción	Descripción
5	Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
4	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
3	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
2	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
1	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, v6

Niveles de calificación de impacto

La calificación del impacto para los riesgos de gestión y de seguridad de la información se tendrá en cuenta la siguiente escala, de acuerdo con la realidad de Función Pública.

Tabla 6. Calificación de impacto para riesgos de proceso y seguridad digital

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
100%	Catastrófico	Pérdida económica superior a 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel internacional.
80%	Mayor	Pérdida económica de 319 hasta 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial.

60%	Moderado	Pérdida económica de 21 hasta 318 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos.
40%	Menor	Pérdida económica de 11 hasta 20 SMLV	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
20%	Leve	Pérdida económica hasta 10 SMLV	Solo de conocimiento de algunos funcionarios.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

La calificación del impacto para los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración establecida por Secretaria de Transparencia de la Presidencia de la Republica. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 7. Calificación del Impacto para los riesgos de Corrupción

No.	Pregunta: Si el riesgo de corrupción se materializa podría	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		

No.	Pregunta: Si el riesgo de corrupción se materializa podría		Respuesta Si	 No
14	¿Dar lugar a procesos penales?			
15	¿Generar pérdida de credibilidad del sector?			
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?			
17	¿Afectar la imagen regional?			
18	¿Afectar la imagen nacional?			
19	¿Generar daño ambiental?			
Nivel	Descriptor	Descripción	Respuestas afirmativas	
1	Moderado	Genera medianas consecuencias sobre la entidad.	1 a 5	
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11	
3	Catastrófico	Genera consecuencias desastrosas para la entidad.	12 a 19	

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6.

Criterios para la evaluación de impacto de pérdida de continuidad

La determinación de las prioridades de recuperación de servicios en caso de materialización de escenarios de pérdida de continuidad de negocio se realiza mediante la valoración del impacto percibido por los líderes de los procesos. Mediante mesa de trabajo los participantes califican los impactos en cada variable y definen el orden de recuperación de los servicios asignando la secuencia de reactivación de los mismos primero a los servicios con mayor impacto y de manera secuencia a los servicios con menor impacto percibido.

Tabla 8. Criterios para la evaluación de impacto de pérdida de continuidad

Criterio	Descripción
Financiero	Nivel de pérdidas económicas
Reputacional	Nivel de pérdida de la confianza de los grupos de valor en la entidad

Criterio	Descripción
Legal / Regulatorio	Nivel de incumplimiento de normas y regulaciones a las que está sometida la entidad
Contractual	Impactos asociados al incumplimiento de cláusulas en obligaciones contractuales
Misional	Nivel de incumplimiento o impacto percibido por imposibilidad de cumplir los objetivos y obligaciones misionales.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

Acciones ante los riesgos materializados

Ante la materialización de un riesgo se deberá medir el impacto y las consecuencias que puede ocasionar afectaciones a los objetivos de la Entidad, se revisarán y ajustarán los controles asociados determinando el grado de efectividad, eficiencia o eficacia, que garantice la mitigación de la ocurrencia. Para adelantar el análisis del riesgo y sus controles se deben considerar los siguientes aspectos:

Calificación del riesgo: se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.
Bajo el criterio de probabilidad: el riesgo se debe medir a partir de la cantidad de veces que se ejecuta cada una de sus acciones.

Se deberán tomar las medidas encaminadas a prevenir la ocurrencia como primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios

sustanciales por mejoramiento, rediseño o eliminación, resultado de ajustes en los controles y acciones emprendidas.

Acciones a seguir en caso de materialización de riesgos de corrupción

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

Informar a las autoridades de la ocurrencia del hecho de corrupción.
Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

Determinar la efectividad de los controles.
Mejorar la valoración de los riesgos.
Mejorar los controles.
Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
Determinar si se adelantaron acciones de monitoreo.
Revisar las acciones del monitoreo.

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla “acciones de respuesta a riesgos”.

Tabla 9. Acciones de respuesta a riesgos

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	Líder de Proceso	Informar a la Secretaría de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y marcar en el SGI-Almera la alerta de posible materialización. Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. Efectuar el análisis de causas y determinar acciones preventivas y de mejora. Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. Informar a discreción los posibles actos de corrupción al ente de control.

Tipo de Riesgo	Responsable	Acción
Riesgos de Gestión y Seguridad digital	Líder de Proceso	Informar a la Secretaria de Planeación como segunda línea de defensa, el evento o materialización de un riesgo. Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existentes, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. Dar cumplimiento al procedimiento plan de mejoramiento.
Riesgos de Gestión y Seguridad digital	Oficina de Control Interno	Informar al líder del proceso sobre el hecho encontrado Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.
Riesgos de continuidad de negocio	Comité de crisis	Activar el plan de continuidad de negocio

Tabla 10. Seguimiento al mapa de riesgos y controles

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento - Controles
Riesgos de Gestión, Riesgos fiscales y Seguridad digital	Baja	Se realiza seguimiento a los controles con periodicidad anual y se registran sus avances en el módulo de riesgos- SGI.
	Moderada	Se realiza seguimiento a los controles con periodicidad anual y se registran sus avances en el módulo de riesgos- SGI.
	Alta	Se realiza seguimiento a los controles con periodicidad semestral y se registran sus avances en el módulo de riesgos- SGI
	Extrema	Se realiza seguimiento a los controles con periodicidad semestral y se registra en el módulo de riesgos – SGI.
Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento cuatrimestral y se registra en el módulo de riesgos – SGI- Almera.	

Estrategia de seguimiento al plan de acción

Tabla 11. Estrategia de seguimiento al plan de acción

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de Tratamiento – Plan de Acción
Riesgos de Gestión, y	Baja	No se debe realizar plan de acción porque está dentro del nivel de aceptación del riesgo por la Gobernación de Caldas

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de Tratamiento – Plan de Acción
Seguridad digital	Moderada Alta Extrema	El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles. Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.

Anexos

https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

Presentación de PowerPoint (funcionpublica.gov.co)