ANEXO 2 POLITICA DE ADMINISTRACIÓN DE RIESGOS

1. Política administración del Riesgo

La política de administración de riesgos de la Gobernación de Boyacá, tiene un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión -MIPG-, la guía de 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.

2. Compromiso Frente a la Administración de los Riesgos Institucionales

"La Gobernación de Boyacá dando cumplimiento a su misionalidad se compromete a controlar los riesgos que puedan afectar el cumplimiento de los objetivos institucionales en el marco de los planes, procesos y proyectos, así como a identificar las oportunidades que se presenten para mejorar la prestación de los servicios diseñando e implementando herramientas y estrategias de gestión que respondan a las necesidades de sus grupos de valor, contando con la participación activa de los lideres de los procesos o Subprocesos del Sistema Integrado de Gestión y de sus equipos de trabajo"

3. Objetivos

3.1 Objetivo General

Identificar, valorar y reducir los riesgos en todos los procesos y/o subprocesos de la Gobernación de Boyacá, a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional y los objetivos estratégicos vigentes.

3.2 Objetivos Específicos:

1. Contribuir al cumplimiento de la misión institucional y objetivos de los procesos y/o subprocesos de la Gobernación de Boyacá.
2. Establecer la administración de riesgos como una herramienta confiable para la planeación institucional y soportar la toma de decisiones.
3. Fortalecer el compromiso de todos los servidores públicos y contratistas de la Gobernación de Boyacá, con el oportuno tratamiento de los riesgos mediante controles y acciones encaminadas a prevenir los efectos adversos y la materialización de los riesgos.
4. Proteger los recursos de la Gobernación de Boyacá, resguardándolos contra la materialización de los riesgos.

5. Prevenir la Ocurrencia de Riesgos y mitigar el impacto de su materialización a través de controles y planes de acción.
6. Priorizar la prevención de Riesgos asociados a las actividades críticas de los procesos y subprocesos de la Gobernación de Boyacá.
7. Asegurar la continua prestación de los trámites y servicios a cargo de la Gobernación.

4. Alcance

La Política para la Administración del Riesgo en la Gobernación de Boyacá aplica a todos los procesos, subprocesos, sectoriales, proyectos, servicios y planes de la entidad, conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa, involucra el contexto estratégico, la identificación, valoración, tratamiento, monitoreo, seguimiento, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- 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 digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

5. Política Operativa para la Administración de Riesgos

5.1 Metodología Aplicada

La metodología está definida en los documentos: Manual para la administración de riesgos de gestión y de corrupción E-DO-DM-M-004, procedimientos: “Administración de Riesgos” E-DO-DM-P-002 y "Gestión de activos de Tecnologías de la Información" A-AD-TI-P-008, de la Gobernación de Boyacá; los cuales se ajustan a los parámetros del Modelo Integrado de Planeación y Gestión – MIPG-, la guía de administración del riesgo y el diseño de controles en entidades públicas (Versión No.5 de 2020) y demás herramientas diseñadas por el Departamento Administrativo de la Función Pública – DAFP, lo establecido en la Norma Técnica Colombiana NTC-ISO 31000: 2018.

El registro de la información concerniente al contexto estratégico, identificación, valoración, análisis y evaluación de los riesgos, se realiza en el Módulo Riesgos DAFP de la herramienta tecnológica ISOLUCIÓN, su operatividad se da por medio de la presente Política de Administración de riesgos, documentada en el Manual para la administración de riesgos de gestión y de corrupción E-DO-DM-M-004, procedimiento: “Administración de Riesgos” E-DO-DM-P-002. En caso de fallas de en el módulo de riesgos DAFP, se deben registrar la información relacionada con la administración de riesgos en la Ficha técnica Matriz de Gestión del Riesgo y asociarse como ficha técnica a cada subproceso.

5.2 Periodicidad para la administración de los riesgos

Identificación y actualización: El periodo identificación y actualización de los riesgos de los procesos y/o subprocesos de la entidad, debe realizarse una vez al año, atendiendo la metodología vigente, asegurando la articulación de éstos con los compromisos de cada proceso.

Monitoreo y seguimiento a los riesgos: El periodo para el monitoreo y seguimiento a los riesgos debe realizarse de manera cuatrimestral conforme a lo definido en la presente política - numeral 8 “Monitoreo y Seguimiento a los Riesgos”.

5.3 Responsabilidades

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

Tabla 1. Responsabilidades frente a las actividades de Riesgo. Fuente. Gobernación de Boyacá

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Línea Estratégica	Comité de Gestión y Desempeño Institucional	○ Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. ○ Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. ○ Recomendaciones de mejoras a la política de operación para la administración del riesgo.
	Comité Institucional de Coordinación de Control Interno	○ Someter a aprobación del Gobernador del Departamento de Boyacá la política de administración del riesgo previamente estructurada por parte de la Oficina Asesora de Planeación y Métodos de Gestión, 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. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. ○ Revisar la política de administración del riesgo por lo menos una vez al año para su actualización y validar su eficacia a la gestión del riesgo institucional. se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta.

		○ Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. ○ Analizar los riesgos, vulnerabilidades, amenazas institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. ○ Garantizar el cumplimiento de los planes de la entidad.

Primera Línea	Líderes de Subproceso Responsable del proyecto Servidores en general	○ Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración de riesgo” la política, metodología y 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 subproceso y realizar seguimiento al mapa de riesgo del subproceso a cargo. ○ 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 subprocesos. ○ Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. ○ Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. ○ Informar a la Oficina Asesora de Planeación y Métodos de Gestión (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo y aplicar las acciones correctivas necesarias. ○ Realizar monitoreo y seguimiento a las acciones correctivas establecidas para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces. ○ En caso de la materialización de un riesgo no identificado, este debe ser gestionado en el aplicativo isolucion y ser incluido en el mapa de riesgo institucional. El líder del subproceso debe:

		○ 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. ○ Revisar y actualizar el mapa de riesgos con el acompañamiento de la Oficina Asesora de Planeación y Métodos de Gestión. Los servidores en general deben: ○ Participar en el diseño de los controles que tienen a cargo. ○ Ejecutar el control de la forma como está diseñado. ○ Proponer mejoras a los controles existentes. ○ Monitorear los controles definidos para cada riesgo El responsable del proyecto debe: ○ Realizar la identificación de los riesgos del proyecto. ○ 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.
		○ Asesorar a la línea estratégica en el análisis del contexto interno y externo, la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual.

Segunda Línea	Oficina Asesora de Planeación y Métodos de Gestión	○ Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del CICCI. ○ Capacitar al grupo de trabajo de cada dependencia en la herramienta isolucion para la gestión del riesgo. ○ Revisar 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. ○ 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 subprocesos registrados en Isolucion. ○ Revisar que el cargue de información en Isolucion esté acorde con lo aprobado por el líder del subproceso. ○ 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 de Gestión y Desempeño Institucional. ○ 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 subprocesos o proyectos. ○ Acompañar, orientar y entrenar a los líderes de subprocesos en la identificación, análisis, valoración y evaluación del riesgo. ○ Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su subproceso. ○ Comunicar a los líderes de subproceso 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

		subprocesos (mapa de riesgo del subproceso). o Gestionar la publicación del mapa de riesgos institucional. o Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. o 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 lograr el cumplimiento a los objetivos. o Informar a la primera línea de defensa correspondiente (líder del subproceso) la materialización de un riesgo no identificado, el cual debe ser gestionado en el aplicativo Isolucion y ser incluido en el mapa de riesgo institucional. o 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. o Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de subprocesos. o Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean gestionados por la primera línea de defensa. o Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos en el CICCI.
		o Acompañar a los líderes de subprocesos 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.

	Secretaria de TIC	○ 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.
Tercera Línea	Oficina de Control Interno de Gestión	○ 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 Oficina de Planeación, en la identificación de los riesgos y diseño de controles. ○ Recomendar mejoras a la política de operación para la administración del riesgo.

5.4 Clasificación de los riesgos

Con el fin de mantener una terminología común para las actividades de gestión de riesgos, la
Entidad establece la siguiente clasificación de riesgos:

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 debido 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

1 participante interno de la organización, son realizadas de 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 negligentes o involuntarias de las obligaciones frente a los usuarios y 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/eventos externos como atentados, vandalismo, orden público.

5.5 Criterios para evaluar el Impacto de Riesgos de Gestión, Riesgos de Seguridad de la Información y Riesgos de Corrupción.

A continuación, se presentan los niveles de calificación del Impacto de los riesgos de gestión y de seguridad de la información en la Gobernación de Boyacá, conforme a la Guía para la administración del riesgo y el diseño de controles en entidades públicas V5 2020 emitida por el Departamento Administrativo de la Función Pública.

Criterios para evaluar Riesgos de Gestión incluye los riesgos de seguridad digital:

Criterios para definir el nivel de 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%

Criterios para definir el nivel de impacto

	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

Criterios para evaluar Riesgos de Corrupción:

Criterios para definir el nivel de probabilidad:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
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.

Criterios para definir el nivel de probabilidad:

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

Nivel de impacto MAYOR

Probabilidad para riesgos de gestión, fraude y seguridad de la información

Se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo?. La probabilidad de ocurrencia está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad corresponde al número de veces que se pasa por el punto de riesgo en el período de 1 año (frecuencia con la que se lleva a cabo una actividad en 1 año).

**En materia de tecnología (incluye disponibilidad de aplicativos) se debe tener en cuenta que 1 hora de funcionamiento = 1 vez.

Probabilidad para riesgos de corrupción

Se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo?. La probabilidad de ocurrencia está asociada a hechos que se han materializado o frente a los cuales se cuenta con un historial de situaciones o eventos asociados al riesgo.

Nota: Para el tratamiento de los riesgos de corrupción sin importar la zona los responsables de procesos y/o subprocesos deben generar, formular, hacer tratamiento y seguimiento a una acción preventiva a través del software del sistema de gestión.

6. Evaluación del Riesgo

En esta etapa se busca confrontar los resultados del análisis de riesgo inicial (riesgo inherente) frente a los controles establecidos, con el fin de determinar la zona o nivel de riesgo final (riesgo residual). La evaluación del riesgo requiere el diseño y la valoración de los controles.

Los controles son aquellas medidas orientadas a reducir o mitigar un riesgo, y se clasifican primariamente de la siguiente manera:

Preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Detectivo: control accionado durante la ejecucion del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Adicionalmente, se cuenta con tematicas generales asociadas a los controles como se muestra en la siguiente tabla, las cuales facilitan el proceso de diseño y redacción de los mismos.

GESTIÓN	Evaluación de desempeño
	Monitoreo y revisión de informes de gestión o reportes
	Seguimiento a indicadores de gestión por procesos, planes, programas, proyectos
	Monitoreo y revisión de riesgos
	Seguimiento a bases de datos
	Seguimiento a instrumentos de planificación de largo, mediano y corto plazo
	Validación de información por parte de un sistema o aplicativo
OPERATIVOS	Aplicación de listas de chequeo, formatos estandarizados
	Capacitación/ divulgación/ socialización
	Validación de información por parte de una persona o comité (revisión, comparación, verificación, validación, inspección, conciliación)
	Copias de seguridad, contingencias y respaldo de información, planes de continuidad del negocio
	Custodia apropiada de la información
	Seguros o pólizas
	Realización de visitas en sitio
	Segregación de funciones
LEGALES	Actualización de normatividad
	Seguimiento al cumplimiento de normas o tiempos de respuesta

Fuente: Elaboración propia

7. Niveles de aceptación de Riesgos o Apetito de Riesgo

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
RIESGOS DE GESTIÓN **Y** **RIESGOS DE CORRUPCIÓN**	***BAJA***	Se *asumirá* el riesgo y se administra por medio de actividades propias desarrolladas dentro de un proceso o subproceso realizando un monitoreo al riesgo y registrando sus avances en el formato respectivo. *Ningún riesgo de corrupción podrá ser aceptado;* para evitar su materialización por parte del proceso de donde se origina el riesgo debe formular, implementar y hacer seguimiento a una acción preventiva.
	MODERADA	Éste es *reducido* mediante la aplicación de los controles y el fortalecimiento a estos, así como el monitoreo y seguimiento periódico al

		riesgo y registrando los avances en los respectivos formatos.
	ALTA Y EXTREMA	Se deben adoptar medidas para reducir la probabilidad u ocurrencia del riesgo mediante el fortalecimiento de controles, y para evitar su materialización debe formular, implementar y hacer seguimiento a una acción preventiva; así mismo, se debe realizar monitoreo y seguimiento periódico al riesgo y registrar sus avances en el respectivo formato.

8. Monitoreo y Seguimiento a los Riesgos

8.1 Monitoreo de la Línea Estratégica

La Alta Dirección y el Comité Institucional de Coordinación de Control Interno (CICCI), definen el marco general para la gestión del riesgo y el control, verifican el cumplimiento de los lineamientos establecidos de la presente política, analizan el resultado de las evaluaciones de la gestión del riesgo elaboradas por la segunda y tercera línea de defensa y definen los ajustes o modificaciones a que haya lugar, monitorean permanentemente los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI, y monitorean el estado de los riesgos con el fin de identificar cambios sustantivos que afecten el funcionamiento de la Gobernación de Boyacá y que permitan la oportuna toma de decisiones.

8.2 Monitoreo de la Primera Línea de Defensa

Es la actividad realizada por los líderes de procesos, planes y proyectos y sus equipos de trabajo, mediante la cual se actualizan los mapas de riesgos a su cargo y se monitorea que se estén ejecutando los controles y los planes de acción establecidos para la mitigación de los riesgos.

La actualización de los mapas de riesgos de gestión, corrupción y seguridad de la información se debe realizar a más tardar el 31 de enero de cada vigencia, y se podrán realizar los ajustes y modificaciones necesarias orientadas a su mejoramiento durante el año de vigencia. Esta actividad tiene los siguientes propósitos:

- ⇒ Identificar nuevos riesgos
- ⇒ Identificar nuevas causas generadoras o efectos con la materialización de los riesgos.
- ⇒ Identificar nuevos controles o actualizaciones en el diseño y valoración de los existentes.
- ⇒ Identificar nuevas acciones para abordar riesgos u oportunidades (planes de acción).

⇒ Reportar los avances en el sitio destinado para tal fin, con la debida identificación de los soportes para cada una de las actividades propuestas para mitigar los riesgos.

El monitoreo tiene como propósito revisar la ejecución consistente de los controles establecidos para la mitigación de los riesgos y de los planes de acción propuestos para el tratamiento de los mismos. En esta actividad, también se identifica si se materializaron o no riesgos de gestión, corrupción y seguridad de la información. En caso que el tratamiento a los riesgos no sea efectivo durante todo el año, dichos riesgos pasarán automáticamente para el siguiente año, si la actividad que conlleva al riesgo se sigue realizando.

La primera línea de defensa debe reportar a la Oficina Asesora de Planeación y Métodos de Gestión, un informe sobre la actualización y el monitoreo realizado en los riesgos de gestión, corrupción y seguridad de la información a su cargo, teniendo en cuenta las siguientes fechas de control.

1. Con corte al 30 de abril. El envio del informe debe realizarse dentro de los tres (3) primeros dias del mes de mayo.
2. Con corte al 31 de agosto. El envio del informe debe realizarse dentro de los tres (3) primeros dias del mes de septiembre.
3. Con corte al 31 de diciembre. El envio del informe debe realizarse dentro de los tres (3) primeros dias del mes de enero.

8.3 Monitoreo de la Segunda Línea de Defensa

Teniendo en cuenta que la segunda línea de defensa está conformada por la Oficina Asesora de Planeación y Métodos de Gestión, supervisores e interventores de contratos y responsables de cada uno de los Sistemas de Gestión, el monitoreo funcionara de la siguiente manera:

- Monitoreo por parte de la Oficina Asesora de Planeación y Métodos de Gestión, mediante el cual se brinda apoyo metodológico a la primera línea de defensa para la identificación, análisis evaluación y tratamiento de los riesgos de gestión, corrupción y seguridad de la información. En esta etapa también se efectúa monitoreo con un mínimo de tres veces al año.

  La Oficina Asesora de Planeación, a partir de los avances reportados por la primera línea de defensa, identificará las necesidades de revisión, actualización o mejora en los mapas de riesgos, teniendo en cuenta los siguientes aspectos:

  ⇒ La incidencia de los riesgos en el logro de los objetivos
  ⇒ La apropiada valoración del riesgo.
  ⇒ Necesidades de creación, eliminación o modificaciones a los mismos para mejorar su eficacia.
  ⇒ Generar alertas tempranas que permitan prevenir la materialización de los riesgos.

⇒ Posibles riesgos emergentes o nuevos riesgos, que se identifican en los seguimientos realizados o como resultados de las auditorías.

- Monitoreo por parte de los responsables de cada uno de los Sistemas de Gestión, mediente la cual se brinda apoyo metodologico a la primera linea de defensa para la identificación, analisis, evaluación y tratamiento de los riesgos o eventos propios de cada sistema. Incluyendo el apoyo en la evaluación de la gestión del riesgo, conforme a los lineamientos definidos en la presente politica.

- Monitoreo por parte de supervisores e interventores de contratos, mediante la cual se efectúa el seguimiento a las matrices de riesgos de los contratos a su cargo, teniendo en cuenta las normas en materia de contratación, así como los lineamientos, directrices y herramientas de Colombia Compra Eficiente.

- Monitoreo por parte del banco de proyectos a los riesgos asociados a los mismos.

8.4 Seguimiento de la Tercera Línea de Defensa

Es la etapa realizada por la Oficina de Control Interno, donde se valora de manera independiente la gestión de riesgos, verificando la efectividad de los controles, mediante actividades de evaluación y seguimiento.

La Oficina de Control Interno, realiza el seguimiento a la gestión de riesgos de acuerdo con los siguientes ciclos de control establecidos en el Plan Anticorrupción y de Atención al Ciudadano:

1. Con corte al 30 de abril. El envio del informe debe realizarse dentro de los diez (10) primeros dias del mes de mayo.
2. Con corte al 31 de agosto. El envio del informe debe realizarse dentro de los diez (10) primeros dias del mes de septiembre.
3. Con corte al 31 de diciembre. El envio del informe debe realizarse dentro de los dies (10) primeros dias del mes de enero.

La Oficina de Control Interno, dentro de su función asesora presentará, luego de los respectivos seguimientos sus resultados de retroalimentación a los responsables de los procesos y subprocesos, con el fin que ellos emprendan las acciones necesarias; y en caso en que se requiera, presenten propuestas de mejoramiento y tratamiento a las situaciones detectadas.

9. Fuentes de Materialización de los Riesgos

A continuación se presentan las principales fuentes de materialización de los riesgos en la Gobernación de Boyacá, sin perjuicio de otras fuentes inherentes a la gestión de riesgos en la entidad, de acuerdo con los roles y responsabilidades definidos bajo el modelo de líneas de defensa.

- Si la Oficina de Control Interno en desarrollo de sus roles de evaluación a la gestión del riesgo, evaluación y seguimiento establecidos en el Decreto 648 de 2017, identifica la ocurrencia del riesgo o posible materialización del mismos.

- Si la Oficina de Control Interno identifico que la ocurrencia del riesgo afecta el cumpliemiento de las metas y objetivos de la Gobernación de Boyacá.

- Si la ocurrencia del riesgo corresponde a un hecho que haya sido cuestionado por algun ente de control externo, por lo mensos en una ocasión.

- Eventos adversos que puedan presentarse e inciden en el cumplimiento de los objetivos estrategicós y del proceso.

- Actividades que hacen parte del flujo del proceso y que son vulnerables creando amenazas frente al cumplimiento del objetivo del mismo.

- Peticiones, quejas, reclamos, denuncias.

- Actos decisorios en materia disciplinaria por acción, omisión o extralimitación de funciones de los servidores públicos de la Gobernación de Boyacá.

- Monitoreos realizados por la primera y la segunda línea de defensa.

9.1 Lineamientos para el manejo de los riesgos materializados

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar acciones descritas en la siguiente tabla:

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	Líder de Proceso y Subproceso	○ Informar a la Oficina Asesora de Planeación y Métodos como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y reportar en el aplicativo Isolucion el evento materializado. ○ 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. i) Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. ii) Efectuar el análisis de causas y determinar acciones preventivas y de mejora.

		iii) Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	○ Informar al líder del subproceso 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. ○ Reporta el riesgo materializado (corrupción) en la plataforma SACI (Sistema de Alertas de Control Interno) de la Contraloría General de la Republica.
Riesgos de Gestión y Seguridad digital	Líder de Proceso	○ Informar a la Oficina Asesora de Planeación y Métodos de Gestión 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 e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento y actualizar el mapa de riesgos.

	Oficina de Control Interno	○ Informar al líder del subproceso 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.

9.2 Incumplimiento de la Política

El incumplimiento de la política descrita anteriormente se clasificará de dos (2) formas: por acción o por omisión, que serán determinadas por la Tercera línea de Defensa (Oficina de Control Interno de Gestión) dando cumplimiento a la responsabilidad de evaluar la gestión de riesgos de la Gobernación de Boyacá. Tanto el código de integridad como el código disciplinario serán parámetros para determinar la aplicación de sanciones en los casos a que haya lugar.

Notas:

1. Si como resultado de las auditorias de gestión se evidencia la materialización de algún riesgo, este manejo debe darse desde el plan de mejoramiento de determinado hallazgo sin necesidad de generar una nueva acción correctiva en la herramienta ISOLUCIÓN.
2. Si se trata de un riesgo materializado se debe tomar una acción correctiva.
3. Si como resultado del seguimiento a riesgos se evidencia la materialización de un riesgo previamente definido por varios procesos de la entidad. Se debe generar la acción correctiva en ISOLUCIÓN desde el proceso de donde se origina el riesgo y los controles para el manejo de éste.
4. Los responsables de proceso y subproceso deben informar al subproceso Direccionamiento y Mejoramiento de Métodos y sistemas de Gestión, sobre la materialización del riesgo y registrar la acción correctiva en ISOLUCIÓN e iniciar con el respectivo tratamiento.

Aprobó: Comité Institucional de Control Interno
Reviso: Juan Carlos Silva Cárdenas - OAPMG
Elaboro: Diego Alejandro Lancheros Ruiz - OAPMG