Tabla de Contenido

1. OBJETIVOS

Describir la metodología y proporcionar las herramientas necesarias para gestionar y administrar los riesgos, desde la identificación, el análisis, la valoración y tratamiento que facilitará la toma oportuna de decisiones por parte de la alta dirección; así como de las acciones realizadas por los servidores responsables de gestionar, hacer seguimiento y monitoreo a la administración de riesgos de gestión de nuestra Entidad.

2. ALCANCE

Aplica a todos los procesos del Sistema Integral de Gestión y Control (SIGC) para orientar la administración y mitigación de riesgos de gestión.

Implica la actualización de la Política para la Administración de Riesgos, el análisis del contexto estratégico, la caracterización de las partes interesadas e identificación de los riesgos de gestión; finaliza con el seguimiento, evaluación, plan de tratamiento de los mismos y la actuación oportuna en caso de la materialización de riesgos.

3. DEFINICIONES

Administración del Riesgo: Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye en el cumplimiento de los objetivos de la entidad.

Acción Correctiva: Conjunto de actividades concatenadas tomadas para eliminar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.

NOTA 1: Existe diferencia entre corrección y acción correctiva.

NOTA 2: Puede darse más de una causa para una no conformidad.

NOTA 3: La acción correctiva se toma para evitar que algo vuelva a producirse, mientras que la acción preventiva se toma para prevenir que algo suceda.

Acción Preventiva: Conjunto de acciones tomadas para prevenir o eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.

NOTA 1: Puede haber más de una causa para una no conformidad potencial.

NOTA 2: La acción preventiva se toma para prevenir que algo suceda, mientras que la acción correctiva se toma para evitar que vuelva a producirse.

Actividades de Control: Son las acciones establecidas a través de políticas (establecen las líneas generales del control interno) y procedimientos (son los que llevan dichas políticas a la práctica) que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Activo: Todo aquello que tiene valor para la Gobernación de Cundinamarca. 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.

Análisis de Riesgos: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

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

Confidencialidad: Propiedad que la información no se pone a disposición i se divulga a personas, entidades o procesos no autorizados.

Consecuencias: 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.

Control: Medida tomada para mitigar o gestionar el riesgo y para que la probabilidad de que el negocio /proceso logre sus metas y objetivos sea mayor. Los controles son políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Controles Automáticos: Utilizan herramientas tecnológicas como sistemas de información o software, diseñados para prevenir, detectar o corregir errores o

deficiencias, sin que tenga que intervenir una persona en el proceso.

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

Control Preventivo: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

Control Detectivo: Controles que se generan durante la ejecución del proceso. Detectan la situación no deseada o riesgo para que se corrija y se tomen las acciones correspondientes.

Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

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

Evento: Incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

Frecuencia: Periodicidad con que ha ocurrido un evento.

Identificación del Riesgo: Descripción de la situación no deseada.

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

Integridad: Propiedad de exactitud y precisión.

Mapa de riesgos Institucional: Contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos. Hacen parte de este mapa todos los riesgos que afectan la entidad en su conjunto, los riesgos identificados en los procesos misionales, los riesgos de seguridad de la información y los riesgos de corrupción.

Mapa de riesgos por proceso: Representación final de la probabilidad e impacto de uno o más riesgos de un proceso.

Materialización de riesgo: Un riesgo materializado determina que el riesgo deja de ser una probabilidad y se convierte en un siniestro real y concreto.

Monitorear: Comprobar, supervisar, observar, o registrar la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios. En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo permanente a los riesgos.

Políticas de Riesgo: Son los criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad, en función de su evaluación.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo, estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. Esta puede ser medida con criterios de Frecuencia (Número de eventos en un periodo determinado) o Factibilidad (Se analiza la presencia de factores internos y externos que pueden propiciar el riesgo).

Probabilidad Inherente: Será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Proceso de Gestión de Riesgos para la Seguridad de la Información: Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de establecimiento del contexto, evaluación de los riesgos (identificación, análisis, valoración) tratamiento, aceptación, comunicación y consulta, vigilancia y examen de los riesgos para la seguridad de la información.

Riesgo: Hace referencia al evento que podría ocurrir, positivo o negativo, que tenga un impacto directo sobre el logro de los objetivos. También se define como un hecho una acción u omisión que podría afectar la capacidad de la organización para lograr sus objetivos de proceso, de negocio o estrategias. Considera la ocurrencia latente o potencial de acontecimientos negativos o inesperados, así como la ausencia o sub-aprovechamiento de oportunidades. Los riesgos positivos se tratarán como oportunidades para el Sistema de Gestión.

Riesgo Ambiental: Eventos que pueden ocasionar incumplimientos en el tratamiento de los aspectos ambientales, objetivos ambientales y demás directrices para prevenir impactos adversos al medio ambiente por las actividades que adelantan las dependencias y entidades de la Gobernación de Cundinamarca.

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

Riesgo de Fraude: (externo): Pérdida derivada de actos de fraude por personas ajenas a la Entidad.

Riesgo de 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.

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

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo de Seguridad de la Información: Posibilidad que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como la combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Emergente: Un riesgo altamente incierto que está en evolucionando con el potencial de graves consecuencias/impactos.

> **Nota 1:** El término "evolucionando" se refiere a los cambios en la comprensión del riesgo en relación con las fuentes de riesgo, los eventos, los efectos/consecuencias, la probabilidad y/o el conocimiento previo.

Riesgo Inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para para modificar su probabilidad o impacto, es el nivel de riesgo propio de la actividad. La combinación de la probabilidad con el impacto, nos permite determinar el nivel de riesgo inherente dentro de unas escalas de severidad.

Riesgo Residual: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento, es decir, el resultado de aplicar la efectividad de los controles al riesgo inherente.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

4. PRINCIPIOS DE LA GESTIÓN DE RIESGOS[1]

El propósito de la administración del riesgo es la creación y la protección del valor. Mejorar el desempeño, fomentar la innovación y contribuir al logro de objetivos de la GOBERNACIÓN DE CUNDINAMARCA.

Los principios descritos proporcionan orientación sobre las características de una gestión del riesgo eficaz y eficiente, comunicando su valor y explicando su intención y propósito. Los principios son el fundamento de la gestión del riesgo y se deberían considerar cuando se establece el marco de referencia y los procesos de la gestión del riesgo de la entidad. Estos principios habilitan a la entidad para gestionar los efectos de la incertidumbre sobre sus objetivos.

a) Integrada

La gestión del riesgo es parte integral de todas las actividades de la organización.

b) Estructurada y exhaustiva

Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

c) Adaptada

El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.

d) Inclusiva

La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una

1 Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC. Norma Técnica Colombiana NTCISO31000. 2018

mayor toma de conciencia y una gestión del riesgo informada.

e) Dinámica

Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.

f) Mejor información disponible

Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.

g) Factores humanos y culturales

El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.

h) Mejora continua

La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

5. LÍNEAS DE DEFENSA

De acuerdo a lo establecido en el numeral 8 de la Política para la Administración de Riesgos de la Gobernación.

6. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas, tanto internas como externas, debería tener lugar durante todas las etapas del proceso para la gestión del riesgo.[2]

Es así como desde la Dirección de Desarrollo Organizacional se ejecuta el Programa de Apropiación del SIGC con el fin de comunicar a todos los servidores

2 Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC. Norma Técnica Colombiana NTCISO31000. 2018.

Públicos su rol en la gestión de riesgos. Así mismo todo lo referente a la gestión de riesgos se encuentra publicado en el software o herramienta utilizada para consulta de los servidores y partes interesadas.

La comunicación de riesgos es una actividad para lograr un acuerdo sobre la forma de gestionar los riesgos intercambiando y/o compartiendo información sobre el riesgo entre los responsables de la toma de decisiones y otras partes interesadas. La información incluye entre otras cosas, la existencia, la naturaleza, la forma, la probabilidad, la gravedad, el tratamiento y la aceptación de riesgos.

La comunicación eficaz entre las partes interesadas es importante, ya que puede repercutir considerablemente en las decisiones que se adopten. La comunicación garantiza que los responsables de la aplicación de la gestión de riesgos y los que tienen un interés personal comprendan la base sobre la que se adoptan las decisiones y por qué se requieren determinadas medidas. La comunicación es bidireccional.

7. ROLES Y RESPONSABLES

De acuerdo a lo establecido en el numeral 8 de la Política para la Administración de Riesgos de la Gobernación.

8. POLÍTICAS DE OPERACIÓN

La gestión de riesgos se realiza acorde a la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el DAFP, versión 5, 2020; y a la Política para la Administración de Riesgos definida por la Gobernación.

También se tienen en cuenta los lineamientos definidos en las normas NTC ISO 31000 – Gestión del Riesgo. Principios y directrices y NTC ISO 27005 – Gestión de Riesgos para la Seguridad de la Información.

La formulación de los riesgos de gestión se realizará a más tardar el 30 de abril de cada vigencia, teniendo en cuenta el Contexto Estratégico y Partes Interesadas.

Los riesgos se identifican, analizan y valoran en el formato Identificación de Riesgos de Gestión.

Si como resultado de auditorías, autoevaluaciones, revisiones, seguimientos o

verificaciones se detectan riesgos emergentes o necesidades de actualizar el mapa de riesgos de gestión, se debe gestionar una solicitud a la Dirección de Desarrollo Organizacional (para riesgos de Gestión) siguiendo el procedimiento Control de la información documentada.

9. NORMATIVIDAD APLICABLE

Política para la Administración del Riesgo de la Gobernación de Cundinamarca.

Constitución Política de Colombia. Arts. 1 y 209. 7 de julio de 1991.

Estatuto Anticorrupción, Ley 1474 de 2011

Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones

Ley 489 de 1998: Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional

Decreto 1499 de 2017: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Función Pública.

Guía para la Gestión del Riesgo de Corrupción. Secretaría de Transparencia. 2015

Decreto Nacional 648 de 2017. Por medio del cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector Función Pública.

Decreto Nacional 338 de 2019. Por medio del cual se modifica el Decreto 1083 de 2015, Reglamentario Único del Sector Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción.

Guía de Roles de las Unidades u Oficinas de Control Interno, Auditoría Interna o quien haga sus veces. Diciembre de 2018.

Decreto Ordenanzal 437 de 2020. "Por medio del cual se establece la estructura de la administración pública departamental, se define la organización interna y las funciones de las dependencias del sector central de la administración pública de Cundinamarca y se dictan otras disposiciones".

Decreto departamental No. 338 de 2018 por el cual se expide el decreto único del Sistema Integral de Gestión y Control del nivel central de la Administración Central o por el decreto que lo sustituya o complemente.

NTC ISO 9001:2015 Sistema de Gestión de la Calidad. Requisitos.

NTC ISO 14001:2015. Sistemas de Gestión Ambiental. Requisitos con orientación para su uso.

NTC ISO 27001: 2013. Sistemas de Gestión de Seguridad de la Información.

NTC ISO IEC 27005:2020. Gestión de Riesgos para la Seguridad de la Información.

NTC ISO 31000:2018 Gestión del riesgo. Principios y Directrices.

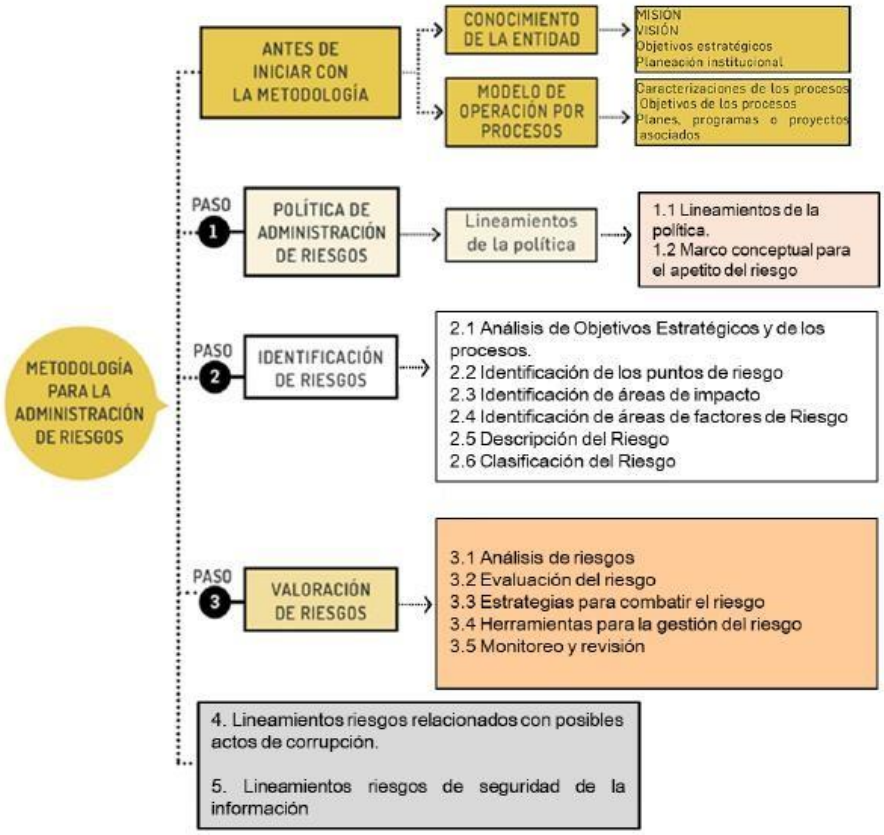
NTC ISO 45001:2018 Sistema de Gestión de Seguridad y salud en el Trabajo.

NTC ISO 17025:2017 Requisitos generales para la competencia de los laboratorios de ensayo y calibración

Política para la Administración del Riesgo de la Gobernación de Cundinamarca.

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP, versión 5, 2020. El Departamento Administrativo de la Función Pública en este documento pone a disposición de las entidades nacionales y territoriales la metodología para la administración del riesgo.

10. METODOLOGÍA PARA LA ADMINISTRACION DEL RIESGO



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP, versión 5, 2020, Figura 4, Pág. 20

10.1. ALCANCE, CONTEXTO Y CRITERIOS

La gestión de riesgos en la Gobernación de Cundinamarca está dentro del marco de los procesos del Sistema Integral de Gestión y Control cuyo alcance es: Diseño y ejecución de las políticas públicas departamentales para la Promoción del Desarrollo Económico, Social, Político y Territorial.

La gestión de riesgos permite establecer el lineamiento estratégico que orienta las decisiones de la Entidad Pública frente a los riesgos que pueden afectar el cumplimiento de sus objetivos, producto de la observación, distinción y análisis del conjunto de circunstancias internas y externas que puedan generar eventos que originen oportunidades o afecten el cumplimiento de su función, misión y objetivos institucionales.

10.1.1. CONTEXTO ESTRATÉGICO Y PARTES INTERESADAS

Para determinar las Partes Interesadas se debe utilizar el formato "Partes Interesadas" el cual constituye la metodología de trabajo que cada proceso debe seguir para el análisis e identificación de las personas u organizaciones que pueden afectar, verse afectados, o percibirse como afectados por una decisión o actividad.

Para determinar el Contexto se debe utilizar el formato "Contexto Estratégico" el cual constituye la metodología de trabajo que cada proceso debe seguir para el análisis de factores internos y factores externos que tienen incidencia en los procesos, en el SIGC y en la entidad en general.

Cada proceso debe realizar la revisión y actualización de estos formatos trimestral.

10.2. RIESGOS DE GESTIÓN

10.2.1. Identificación, Análisis y Valoración de Riesgos de Gestión

Para efectuar la identificación, análisis y valoración de riesgos se cuenta con el formato "Identificación de Riesgos" el cual constituye la metodología de trabajo que cada proceso debe seguir para la administración de sus riesgos. Dicho formato se debe conservar adjunto en la caracterización del proceso en el software o herramienta utilizada.

10.2.1.1. Identificación de Riesgos de Gestión

Partiendo del análisis del contexto estratégico en el que opera la Entidad, la caracterización de cada uno de los procesos (contemplando su objetivo y alcance), el análisis de los factores internos y externos que pueden generar riesgos; se identifican los riesgos que se encuentren o no bajo el control de la Entidad con el fin de conocer los eventos potenciales que puedan afectar el logro de los objetivos.

Se deben tener en cuenta los siguientes insumos:

- El análisis del contexto estratégico.
- Caracterización de los procesos
  - Objetivo y alcance
  - Los productos y servicios que entrega el proceso
  - Las actividades que realiza el proceso
  - Las no conformidades que ha tenido el proceso en cuanto a cantidad,

problemas más recurrentes y dificultades para emprender acciones de mejora.
    - Los indicadores (de proceso y de Plan de Desarrollo) que no cumplen con las metas planteadas.
    - Riesgos materializados en las vigencias anteriores.
    - Las salidas no conformes que se han reportado en el proceso.
- Los resultados generales de las auditorias tales como lecciones aprendidas, observaciones, hallazgos, sugerencias, oportunidades de mejora, etc. La Primera Línea de Defensa debe realizar un análisis de los hallazgos para establecer posibles riesgos no identificados que evidencian materialización con los hallazgos, este análisis debe ser validado desde la Segunda Línea de Defensa.
- Factores Internos y externos que puedan generar riesgos.

Para los laboratorios de Salud Pública y laboratorio de Rentas es importante considerar los riesgos de imparcialidad, así como los vinculados a los procesos analíticos del laboratorio (Muestreo, Traslado de las muestras, Recepción, Ensayo, Elaboración de Informe, disposición de las muestras procesadas).

La identificación del riesgo se da en tres fases:

10.2.1.1.1. Análisis de Objetivos Estratégicos y de los Procesos:

Este es un paso muy importante teniendo en cuenta que los riegos que se identifiquen deben tener impacto en el cumplimiento de los objetivos estratégicos o del proceso.

La Entidad debe analizar y revisar que los objetivos estratégicos estén alineados con la misión y visión institucional, deben contener cómo mínimo las siguientes características: ser específicos, medibles, alcanzables, relevantes y proyectados en el tiempo. Los objetivos de los procesos deben ser analizados y revisados teniendo en cuenta las anteriores características y adicionalmente se debe revisar que estos contribuyan a los objetivos estratégicos.

Es importante tener en cuenta que el riesgo va ligado completamente al objetivo del proceso, actividades, productos y servicios del proceso por esta razón para un proceso misional su riesgo no sería el tener personal insuficiente, o que no se contrate, ya que el objetivo de los procesos misionales de la Gobernación no es contratar ni contar con cierta cantidad de personal.

10.2.1.1.2. Identificación de los Puntos de Riesgo:

Actividades dentro del flujo del proceso en donde existe evidencia o se tienen indicios que pueden ocurrir eventos de riesgo operativo y se debe mantener bajo control para que el proceso cumpla con su objetivo.

10.2.1.1.3. Identificación áreas de impacto:

Las áreas de impacto son las consecuencias económicas o reputacionales a las que están expuestas las entidades, en caso de la materialización de un riesgo.

10.2.1.1.4. Identificación de áreas de factores de riesgos:

Son las fuentes generadoras de riesgos, cada entidad de acuerdo a su complejidad propia y otros aspectos pertinentes del contexto debe analizarlos e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo.

10.2.1.1.5. Descripción del riesgo:

Debe contener todos los detalles necesarios, debe ser fácil de entender tanto para los involucrados en el proceso como para personas ajenas al mismo.

La Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Versión 5 del DAFP propone la siguiente estructura que facilita la redacción y claridad del riesgo, debe iniciar con la frase POSIBILIDAD DE y se analizar los siguientes aspectos:

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP, versión 5, 2020, Figura 10, Pág. 32

Impacto: Consecuencias que la materialización del riesgo puede ocasionar a la Entidad.

Causa Inmediata: Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, estas NO constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, son las razones por las cuales puede presentarse el riesgo, son las bases para la definición de controles en la etapa de valoración del riesgo. Es importante tener en cuenta que pueden existir más de una causa o sub causas que puedan ser analizadas para un mismo riesgo.

La estructura sugerida evita que se presente subjetividad en la redacción de los riesgos, permitiendo que se entienda la forma en la que se manifiesta el riesgo, así como sus causas, lo cual es esencial para la definición de controles en la etapa de valoración del riesgo.

Ejemplo[3]:

Proceso: Gestión de recursos
Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.
Alcance: Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requerida bajo especificaciones técnicas y normativas establecidas.

Redacción inicia con:	¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de	afectación económica	por multa y sanción del ente regulador	debido a adquisición de bienes y servicios fuera de los requerimientos normativos
	Impacto	Causa Inmediata	Causa Raíz

Para una adecuada redacción del riesgo se debe evitar:

3 Tomado de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, DAFP 2020

- Describir omisiones o desviaciones del control como riesgos (Ej: errores en la liquidación de la nómina por falla en los procedimientos existentes).
- Describir causas como riesgos (Ej: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación)
- Describir riesgos como la negación de un control (Ej: retrasos en la prestación del servicio por no contar con digiturno para la atención)
- No existen riesgos transversales, lo que pueden existir son causas transversales (Ej: pérdida de expedientes)

10.2.1.1.6. Clasificación del riesgo:

Para la identificación de los riesgos de gestión y con el objeto de incorporar toda clase de riesgo asociado con el proceso, se debe tener en cuenta la siguiente clasificación dada por el Departamento Administrativo de la Función Pública a través de la Guía para la Administración del Riesgo versión 5:

- ☐ **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 estos.
- ☐ **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.

10.2.2. Valoración del Riesgo de Gestión

10.2.2.1. Análisis de Causas de los Riesgos

El análisis de causas pretende determinar todos aquellos motivos, escenarios, debilidades, o amenazas que pueden desencadenar en materialización (ocurrencia) del riesgo. Para realizar dicho análisis debemos preguntarnos porque puede presentarse el riesgo identificado.

Para los laboratorios de Salud Pública y de Rentas se debe tener en cuenta el impacto potencial que afecte la validez de los resultados.

Causas comunes que podría tener cualquier riesgo[4]:Causa
Información no disponible o inoportuna
Deficiencias en la planeación
Insuficiente capacitación
Uso inadecuado de los métodos o herramientas empleadas en el proceso
Caídas de los sistemas de información
Criterios no unificados o estandarizados
No aplicación de los lineamientos del proceso
Débil interacción o fallas en la comunicación entre las dependencias de la Gobernación

10.2.2.2. Análisis de Riesgos de Gestión

El análisis de riesgos permite establecer la probabilidad de ocurrencia de los mismos y determinar sus consecuencias o impactos, valorándolos y evaluándolos a fin de establecer los criterios para su tratamiento.

10.2.2.2.1. Probabilidad de Ocurrencia

La calificación de la posibilidad de ocurrencia del riesgo se encuentra asociada a la exposición al riesgo del proceso o actividad analizada. Por lo anterior la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año. Esta metodología está orientada a eliminar la subjetividad que afecta usualmente esta clase de análisis.

De acuerdo con lo anterior, es posible establecer que la exposición al riesgo está asociada al proceso o la actividad que se está analizando, es decir al número de veces que se pasa por el punto de riesgo en el periodo de un año.

4 El listado de causas comunes es producto del ejercicio de identificación de riesgos de los procesos que hacen parte del Sistema Integral de Gestión y Control de la Gobernación de Cundinamarca

Probabilidad de Ocurrencia			
Nivel	**Descriptor**	**Frecuencia de la Actividad**	**Probabilidad**
1	Muy baja	El evento que conlleva al riesgo, ocurre como máximo 2 veces por año.	20%
2	Baja	El evento que conlleva al riesgo, ocurre de 3 a 24 veces por año	40%
3	Media	El evento que conlleva al riesgo, ocurre de 24 a 500 veces por año	60%
4	Alta	El evento que conlleva al riesgo, ocurre mínimo 500 veces al año y máximo 5000 veces por año	80%
5	Muy Alta	El evento que conlleva el riesgo, ocurre más de 5000 veces por año	100%

Nota: Tomados de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP, versión 5, 2020.

El líder de proceso y su equipo de mejoramiento deben calificar la probabilidad de ocurrencia según el conocimiento y su experticia, definiendo cuantas veces se desarrolla la actividad para el nivel de probabilidad y a través de la tabla ubicando el nivel correspondiente. Esta actividad se realiza utilizando la Hoja "Calificación Probabilidad" del formato Identificación de Riesgos.

10.2.2.2.2. Determinar el Impacto

Los criterios establecen los niveles de impactos económicos y reputacionales como variables principales clasificados de la siguiente manera:

Criterios de Impacto		
Descriptor	**Afectación Económica**	**Reputacional**
Leve – 20%	Afectación menor a 10 SMLMV.	No se afecta la imagen institucional de alguna área de forma significativa.

Criterios de Impacto		
Descriptor	**Afectación Económica**	**Reputacional**
Menor – 40%	Entre 10 y 50 SMLMV	Afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o deproveedores. Imagen institucional afectada localmente por retrasos en laprestación del servicio a los usuarios o ciudadanos.
Moderado - 60%	Entre 50 y 100 SMLMV	Afecta la imagen de la entidad con algunos usuariosde relevancia frente al logro de los objetivos. Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Mayor – 80%	Entre 100 y 500 SMLMV	Afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, departamental o municipal. Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio alos usuarios o ciudadanos.
Catastrófico – 100%	Mayor a 500 SMLMV	Afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenible a nivel país. Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

Para abordar los riesgos de los laboratorios, el impacto está relacionado principalmente con el criterio reputacional, dado que se encuentra asociado al impacto potencial sobre la validez de los resultados de los ensayos.

El líder y su equipo de mejoramiento del proceso deberán establecer el nivel de impacto de acuerdo a la tabla establecida, con el fin de realizar un análisis objetivo. Esta actividad se realiza utilizando la Hoja "Calificación Probabilidad" del formato Identificación de Riesgos.

Es importante resaltar que en la actualidad el criterio experto, es decir el conocimiento y experticia de los líderes, gestores y usuarios expertos de los equipos de mejoramiento de los procesos del SIGC, es fundamental para la definición de aspectos tales como: número de veces que ocurre un evento, cadena de valor del proceso y la definición de controles.

10.2.3. Evaluación de Riesgos de Gestión

10.2.3.1. Calificación Riesgo Inherente

La zona de riesgo donde se ubica el riesgo inicial (inherente) se determina combinando la probabilidad de ocurrencia y el impacto. Existen 4 zonas de severidad definidas en la matriz de calor.

Matriz de Calor Inherente	Impacto				
Probabilidad					
Muy Alta 100%					
Alta 80%					
Media 60%					
Baja 40%	R1				
Muy Baja 20%					
	Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Zona de riesgo	Color
Muy Alta	**Rojo**
Alta	**Naranja**
Moderada	**Amarillo**
Baja	**Verde**
Muy Baja	**Verde**

La valoración de riesgos es el producto de confrontar los resultados del análisis del riesgo con los controles identificados. Para adelantar esta etapa se hace necesario identificar controles existentes para el riesgo.

Los controles son políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos por debajo del nivel asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Para cada causa debe existir un control.
- Cada causa tiene que tener un análisis individual y se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).
- Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

10.2.3.2. Diseño de Controles[5]

- Paso 1: Responsable

Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable

5 Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4 DAFP 2018

de su ejecución.

Cuando un control se hace de manera manual (ejecutado por personas) es importante establecer los diferentes aspectos del responsable de su realización tal y como se evidencia en la siguiente tabla:

Nombre del Responsable	Cargo Responsable	Área o Dependencia Responsable	Jefe del Área del Responsable

Cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es importante establecer como responsable de ejecutar el control al sistema o aplicación.

Paso 2: Periodicidad

El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, etc.) su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o se detecta de manera oportuna el riesgo.

Cada vez que se releva un control debemos preguntarnos si la periodicidad en que este se ejecuta ayuda a prevenir o detectar el riesgo de manera oportuna. Si la respuesta es SÍ, entonces la periodicidad del control está bien diseñada. Esto se debe a que la posibilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando y se deben hacer controles periódicos de la actividad en el transcurso del año.

Hay controles que no tienen una periodicidad específica como, por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores. La periodicidad debe quedar redactada de tal forma que indique: que cada vez que se desarrolla la actividad en donde existe una posibilidad de ocurrencia del riesgo se ejecuta el control.

Todos los controles deben tener una periodicidad específica. Si queda a criterio la periodicidad de la realización del control, tendríamos un problema en el diseño del control.

Paso 3: Propósito

El control debe tener un propósito que indique para qué se realiza, y que este conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo. Con el

objetivo de llevar a cabo los ajustes y correctivos en el diseño del control o en su ejecución.

Al momento de identificar los controles para mitigar el riesgo, debemos preguntarnos si es una actividad o un control, y para diferenciarlo es importante tener en cuenta que el control (verifica, valida, concilia, coteja, compara, etc.) ayuda a la mitigación del riesgo, por eso es importante que pensemos primero en tener controles preventivos antes que detectivos o correctivos.

Paso 4: Como se realiza

El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo.

Paso 5: Desviaciones

El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, es importante revisar si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen. En caso tal de ser así la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones.

Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas aclaraciones, el control tendría problemas de diseño.

Paso 6: Evidencia

El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente:

1. Fue realizado por el responsable que se definió.
2. Se realizó de acuerdo a la periodicidad definida.
3. Se cumplió con el propósito del control.
4. Se dejó la fuente de información que sirvió de base para su ejecución.
5. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control.

Hay controles en los que su evidencia queda en un flujo a través de una aplicación como un "aprobado" o "revisado" y otros en los que la evidencia es la configuración y programación de la aplicación, cuando es un control automático. Es importante aclarar que esta evidencia tiene que ser suficiente para poder complementar o apoyar el proceso de socialización y publicación de resultados.

Ejemplos de controles bien diseñados:

A. Cada vez que se va a realizar un contrato **(Periodicidad),** el profesional de contratación **(Responsable)** verifica a través de una lista de chequeo **(Cómo se Realiza)** que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación **(Propósito)** En caso de encontrar información faltante, solicita al proveedor por correo la información y poder continuar con el proceso de contratación **(Desviaciones).** Como registro se deja la lista de chequeo diligenciada **(Evidencia),** con la información de la carpeta del cliente y los correos a que hubo lugar en donde solicitó la información faltante (en los casos que aplique).

   El auxiliar de cartera **(Responsable)** mensualmente **(Periodicidad)** verifica que los valores recaudados en 'Banco' correspondan con los saldos adeudados por los clientes **(Propósito),** este toma dicha información directamente del portal bancario e identifica las cuentas por cobrar **(Cómo se Realiza),** es decir, pendientes de pago, y que fueron canceladas según los extractos bancarios revisados. En caso de observar cuentas de cobro que a la fecha no se ha recibido el pago **(Desviaciones),** liste las cuentas pendientes de pago, realice llamadas a los clientes y solicite la fecha para el pago de las mismas. **Evidencia:** el listado de cuentas por cobrar pendientes de pago con los compromisos acordados con los clientes y el extracto bancario.

B. Cada vez que se va a realizar un pago **(Periodicidad),** el sistema SAP **(Responsable)** valida que el proveedor al cual se le va a girar el pago no esté reportado en listas restrictivas **(Propósito),** comparando el número de identificación tributaria (NIT) o cédula con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo **(Cómo se Realiza).** En caso de encontrar coincidencias el sistema no permite realizar el pago **(Deviaciones).** Como evidencia queda la programación interna del aplicativo y el reporte de coincidencia con listas restrictivas.

10.2.3.3. Calificación de Controles Existentes

Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%

Características			Descripción	Peso
Atributos Informativos	Documentación	Documentado	Controles que están documentadosen el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propiodel proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva elriesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de laejecución del control.	-

Para mayor claridad se toma el siguiente ejemplo:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo durante el trascurso del todo el periodo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se verifica con las actividades de evaluación realizadas por auditoría interna o control interno.

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO - PESO DE LA EJECUCIÓN DEL CONTROL
Fuerte	El control se ejecuta de manera consistente por parte del responsable
Moderado	El control se ejecuta algunas veces por parte del responsable
Débil	El control no se ejecuta por parte del responsable.

Dado que un riesgo puede tener varias causas, a su vez varios controles la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo. La solidez del conjunto de controles se obtiene calculando

el promedio aritmético simple de los controles por cada riesgo. El formato E-PID-FR-081 Identificación de Riesgos cuenta con la formulación definida para realizar este cálculo.

10.2.3.4. Determinación del Riesgo Residual

La mayoría de los controles que se diseñan son para disminuir la probabilidad de que ocurra una causa o evento que pueda llevar a la materialización del riesgo y muy pocos son dirigidos al impacto. Sin embargo, si no existieran controles para disminuir la probabilidad del riesgo, el impacto de un riesgo por el número de eventos que se llegarían a materializar sería mayor, por tal razón al momento de evaluar si los controles ayudan a disminuir el impacto o la probabilidad, estos controles se calificarán teniendo en cuenta que de manera indirecta disminuyen también el impacto y es el resultado de aplicar la efectividad de los controles al riesgo inherente es el riesgo residual.

Como vemos en la tabla anterior el resultado obtenido a través de la valoración del riesgo es el riesgo residual, así, el desplazamiento dentro de la Matriz determinará finalmente la selección de las opciones de tratamiento y medidas de respuesta.

- Cuando el riesgo residual sea igual al riesgo inherente y éste se ubique en una zona alta o extrema, los controles propuestos deben implementarse en un término no mayor a tres meses.

- Cuando el riesgo residual sea igual al riesgo inherente y éste se ubique en una zona alta o extrema, los controles propuestos no pueden ser los mismos controles existentes estos deben ser cambiados, fortalecidos o mejorados en su diseño o se deberá volver a analizar y revisar dicho tratamiento

10.2.3.5. Tratamiento a los Riesgos de Gestión

Deberían escogerse los controles adecuados y con una segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este. Los riesgos de gestión serán tratados según su probabilidad e impacto así:

- Cuando el riesgo se ubique en la zona baja, este es Reducido mediante el fortalecimiento de los controles existentes; o eliminado mediante la supresión de las causas o actividades que generan el riesgo.
- Cuando el riesgo se ubique en la zona moderada o alta, se debe llevar a zona baja mediante el fortalecimiento de los controles tomando medidas

de prevención y protección; estos riesgos también pueden ser eliminados mediante la supresión de las causas o actividades que generan el riesgo.

- Preguntar cómo hacer la distinción de la zona moderada o alta o si se toma los mismos procedimientos para mitigar ambos riesgos
- Cuando el riesgo se ubique en la zona extrema, requieren de un tratamiento prioritario. Se deben implementar los controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección; estos riesgos también pueden ser eliminados mediante la supresión de las causas o actividades que generan el riesgo.

Zona de riesgo	Medidas de respuesta
Muy Alta	Evitar el riesgo (solamente es posible cuando se deja de realizar la actividad) Reducir el riesgo Transferir el riesgo
Alta	Evitar el riesgo (solamente es posible cuando se deja de realizar la actividad) Reducir el riesgo Transferir el riesgo
Moderada	Reducir el riesgo
Baja	Aceptar el riesgo Reducir el riesgo

Riesgos Bajos: Son aquellos que en la entidad no representan efectos que perjudican el normal funcionamiento de sus procesos, cuya presencia es esporádica y su tiempo de permanencia es corto o tiene niveles de afectación económica muy bajo y la afectación reputacional en proporciones mínimas. Este es Reducido mediante el fortalecimiento de los controles existentes; o aceptado haciendo un monitoreo periódico al riesgo y sus controles.

Riesgos Moderados: Son aquellos riesgos con probabilidad e impacto medio en el funcionamiento en el presupuesto de la entidad o en la reputación de la entidad internamente. Este es Reducido mediante el fortalecimiento de los controles tomando medidas de prevención y protección.

Riesgos Altos y Muy Altos: Deben tener un tratamiento especial en la formulación del plan de mitigación de riesgos, eliminando la actividad que genera el riesgo en la medida que sea posible, o implementando controles de prevención para reducir la probabilidad del riesgo, de protección para disminuir el Impacto o transferir el riesgo.

10.2.4. Tratamiento del Riesgo: Acciones para Abordar los Riesgos de Gestión

Las acciones de tratamiento se agrupan en:

- Disminuir la probabilidad: acciones encaminadas a gestionar las causas del Riesgo.
- Disminuir el impacto: acciones encaminadas a disminuir las consecuencias del riesgo

Las acciones para abordar riesgos contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Se debe tener en cuenta que los controles se despliegan a través de los procedimientos documentados y que las actividades de control deben por sí solas mitigar o tratar las causas del riesgo y ejecutarse como parte del día a día de las operaciones.

10.2.4.1. Clasificación de Actividades de Control

- Controles Preventivos: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.
- Controles Detectivos: Controles que se generan durante la ejecución del proceso. Detectan la situación no deseada o riesgo para que se corrija y se tomen las acciones correspondientes.
- Controles Correctivos: Controles accionados en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

10.2.4.2. Formulación de Acciones Software o Herramienta Utilizada

El dinamizador del proceso acompañará a los equipos de mejoramiento en el cargue de los riesgos y los planes en el software o herramienta dispuesta para tal fin, de acuerdo a las orientaciones de la Dirección de Desarrollo Organizacional.

10.2.4.2.1. Plan de Riesgos de Gestión

El responsable del plan de riesgos de gestión es el líder del proceso, quién deberá incluir la información de las causas y las acciones que se desarrollarán para el tratamiento y mitigación del riesgo.

Ejemplo de plan de acciones para dar riesgos de gestión:

Tratamiento de riesgos			
Riesgo	**Actividades**	**Evidencia**	**Indicadores del riesgo**
Sistema Integral de Gestión y	Desarrollar plan de comunicación y apropiación del SIGC	Listados de asistencia y fotos	**Eficacia:** Índice de cumplimiento
Control que no contribuya al mejoramiento institucional	Realizar campaña de apropiación del SIGC	Una Campaña realizada	actividades= (# de actividades cumplidas / # de actividades programadas) x 100
	Capacitar en el uso de la herramienta Isolución	Número de funcionarios capacitados	
	Realizar procedimiento que describa la metodología a utilizar para la revisión al desempeño del proceso	Un procedimiento implementado	**Efectividad**: ((# de hallazgos al SIGC presentados periodo actual - # de hallazgos al SIGC periodo anterior) / # de hallazgos al SIGC presentados periodo anterior) x100
	Realizar seguimiento al cumplimiento de las autoevaluaciones	Informes de seguimiento	

Las acciones que se definan serán acciones preventivas que permitan mejorar los controles actuales, implementar controles que sean más efectivos y realizar seguimiento al riesgo y sus controles. Estas acciones se cargarán a al software o herramienta utilizada, definiendo responsables, producto entregable y fechas de compromiso.

Los usuarios responsables deben incluir los avances y resultados que se han obtenido de cada actividad, es importante que se carguen los archivos que evidencien dichos avances y resultados.

10.2.5. Aceptación del Riesgo de Gestión

La Gobernación de Cundinamarca ha definido los siguientes aspectos para los niveles de aceptación de riesgo de gestión:

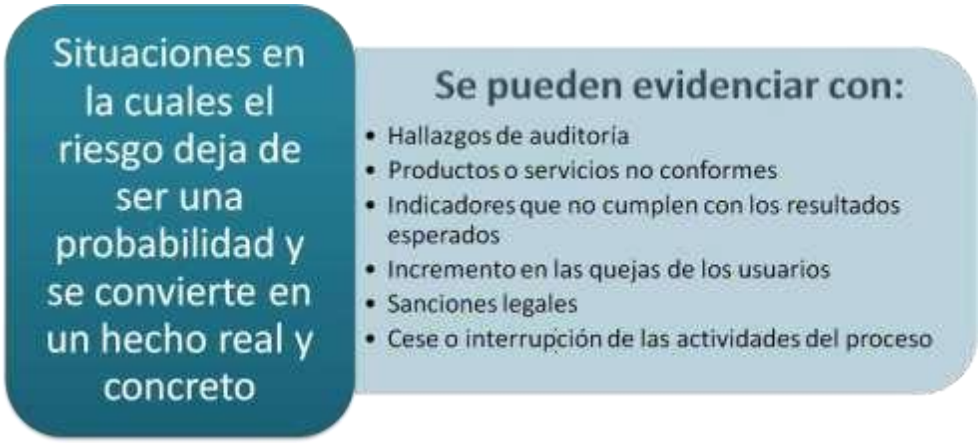
- La alta dirección de la Gobernación de Cundinamarca ha definido como umbral aceptable de riesgo de gestión todos aquellos que se encuentren por debajo de la zona de riesgo externo. Podrían aceptarse riesgos de gestión por encima de este nivel en circunstancias específicas.
- Siempre se debe considerar la relación entre el beneficio estimado y el riesgo de gestión estimado.
- Cualquier riesgo de gestión relacionado al incumplimiento de una ley o reglamentación no son aceptados en la Gobernación de Cundinamarca.
- Dependiendo la naturaleza del riesgo de gestión se podrían incluir actividades de tratamiento futuras siempre y cuando haya un compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación en la Gobernación de Cundinamarca consideran los siguientes elementos:

- Criterios de la Gobernación de Cundinamarca
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas
- Factores sociales y humanitarios

10.2.6. Materializaciones de Riesgos de Gestión

La siguiente figura muestra la definición de materialización de riesgo de gestión y escenarios en los cuales se pueden evidenciar dichas materializaciones:



Las materializaciones (ocurrencia) de riesgos pueden ser detectadas por:

- Servidores públicos los cuales comunicarán a un integrante del equipo de mejoramiento del proceso para registrar la no conformidad siguiendo el procedimiento de acciones correctivas y preventivas.
- Equipos de mejoramiento los cuales levantaran no conformidades siguiendo el procedimiento de acciones correctivas y preventivas.
- Líderes de proceso los cuales implementaran acciones correctivas siguiendo el procedimiento de acciones correctivas y preventivas.
- La Dirección de Desarrollo Organizacional la cual levantará no conformidades que no levanten los equipos de mejoramiento ante la evidencia de riesgos materializados.
- La Oficina de Control Interno a través de las auditorías internas y verificaciones.

Las materializaciones de riesgos se registrarán en el software o herramienta utilizada, siguiendo el Procedimiento Gestión de Acciones para la Mejora Continua.

10.2.7. Monitoreo y Revisión de Riesgos de Gestión

En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo de trabajo realizarán monitoreo trimestral a la gestión de riesgos y la efectividad de sus controles mediante el informe de revisión al desempeño de los procesos (Revisión al Desempeño del Proceso). De igual forma acorde a lo establecido en la Política para la Administración de Riesgos se monitorean los factores internos y externos a fin de establecer cambios que determinen nuevos riesgos.

Esta actividad busca en primer lugar, la alineación continua de la gestión de riesgos con los objetivos de la Gobernación de Cundinamarca y con los criterios de aceptación de riesgos y la pertinencia continua del proceso de gestión de riesgos para los objetivos o la actualización del proceso

El monitoreo debe contener análisis de las acciones y controles que se han implementado para los riesgos, evaluar los controles implementados para evitar materializaciones, determinar su efectividad y emprender cambios de ser necesario.

El monitoreo realizado debe permitir:

- Determinar si los controles son suficientes para evitar que el riesgo se materialice.
- Garantizar que los controles son efectivos.
- Obtener información adicional que permita mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
- Detectar cambios en el contexto interno y externo. Identificar riesgos emergentes.
- Determinar efectividad de las actividades de control

Anualmente en la revisión por la dirección se analizarán los resultados de la gestión realizada sobre los riesgos de gestión, donde se revisará la variación de la cantidad de riesgos que se ubican en cada zona (Muy Alto, Alto, Moderado, Bajo).

Es importante tener en cuenta que los riesgos no pueden ser cerrados en el transcurso de la vigencia, el cierre se puede dar a la vigencia siguiente.

10.3. SEGUIMIENTO Y EVALUACIÓN

Un funcionario de la Dirección de Desarrollo Organizacional realizará seguimiento a la ejecución de los planes de riesgos de gestión, verificando las actividades realizadas y archivos anexos cargados. Este funcionario realizará un informe que entregará al responsable designado por la Dirección como encargado de consolidar el seguimiento a los planes de riesgos. Esta Dirección también verificará la eficacia de las actividades y del plan de riesgos.

No se debe confundir la verificación, a las actividades definidas por los procesos para la gestión de los riesgos, realizada por la Dirección de Desarrollo Organizacional, con la evaluación de controles. La Dirección de Desarrollo Organizacional verifica la ejecución de las actividades de los planes de riesgos

cargados en el software o herramienta de consulta, definiendo como "Eficaz" una actividad cumplida o "No eficaz" una actividad no cumplida o insuficiente para abordar las causas del riesgo. La evaluación de los controles de los riesgos se realiza durante las auditorías. Así las cosas, una actividad eficaz no necesariamente indica que el control sea efectivo y viceversa.

Al momento en que la Dirección de Desarrollo Organizacional dé cierre "No Eficaz" a la actividad o a los planes de acción de riesgos, se debe retomar o reevaluar las actividades no cumplidas o insuficientes para tratar el riesgo. Esta labor se plasmará explícitamente en el formato Revisión al Desempeño del Proceso o en nuevos planes de riesgos de gestión.

La Dirección de Desarrollo Organizacional adelantará el seguimiento a las actividades y acciones de los planes de riesgos de gestión mensualmente y se consolidará de manera trimestral; se socializa a la Alta Dirección en los comités correspondientes.

La actualización de los mapas de riesgos de gestión para cada vigencia se debe realizar antes del 30 de abril y los planes de acción con corte al 31 de diciembre.

11. COMUNICACIÓN Y CONSULTA: MAPA DE RIESGOS INSTITUCIONAL

Dando cumplimiento al Modelo Integrado de Planeación y Gestión - MIPG, la Dirección de Desarrollo Organizacional consolidará el mapa de riesgos institucional en el cual se llevan todos los riesgos que afectan la entidad en su conjunto, los riesgos identificados en los procesos misionales, riesgos de gestión, riesgos de corrupción, riesgos de seguridad digital, riesgos de seguridad y salud en el trabajo y riesgos de gestión ambiental.

El mapa de riesgos institucional estará disponible para consulta en el aplicativo o herramienta tecnológica utilizada por la Entidad.