RESOLUCIÓN No. 0754

"Por medio de la cual se actualiza la Política de Administración de Riesgos en la Corporación Autónoma Regional de Nariño – CORPONARIÑO, con base en lo establecido en el Sistema Integrado de Gestión Pública y se dictan otras disposiciones."

EL DIRECTOR GENERAL DE LA CORPORACIÓN AUTÓNOMA REGIONAL DE NARIÑO — CORPONARIÑO

En uso de sus facultades legales, en especial las que le confiere el artículo 2.2.22.3.8 delDecreto 1083 de 2015

CONSIDERANDO

Que la Constitución Política de Colombia, por medio de su artículo 209, señala que las autoridades administrativas deben coordinar sus actuaciones para un adecuado cumplimiento de las funciones del Estado y en todos sus órdenes tendrá un control interno, el cual se ejercerá en los términos que señale la ley.

Que la ley 87 del año 1993, estableció normas para el ejercicio del control interno en las entidades y organismos del Estado y dentro de este propósito las Oficinas de Control Interno deben asesorar a la dirección en la continuidad del proceso administrativo, la reevaluación de los planes establecidos y la introducción de los correctivos necesarios para el cumplimiento de las metas y objetivos previstos.

Que mediante el artículo 28, de la misma Ley 87 de 1993, se dispuso la aplicación de instrumentos de gerencia, con el fin de fortalecer el cumplimiento cabal y oportuno de las funciones del Estado.

Que en la misma ley, se establece como mecanismos de verificación y evaluación del control interno, además de las normas de auditoría generalmente aceptadas, la selección de indicadores de desempeño, los informes de gestión y de cualquier otro mecanismo moderno de control que implique el uso de mayor tecnología, eficiencia y seguridad.

Que de acuerdo con el artículo 73 de la Ley 1474 de 2011, cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano; dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias antitrámites y los mecanismos para mejorar la atención al ciudadano.

Que el Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción señalará una metodología para diseñar y hacerle seguimiento a la señalada estrategia y en aquellas entidades donde se tenga implementado un sistema integral de administración de riesgos, se podrá validar la metodología de este sistema con la definida por este Programa.

Que mediante el Decreto 124 de 2016, se sustituyó el título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 relativo al Plan Anticorrupción y de Atención al Ciudadano y se establecieron las Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano V2 elaboradas por la Secretaría de Transparencia de la Presidencia de la República, así como la metodología para diseñar y hacer seguimiento a los Mapas de Riesgos de Corrupción de que trata del artículo 73 de la Ley 1474, la cual fue establecida en el documento "Guía para la Gestión de Riesgos de Corrupción".
Que mediante el Decreto 648 del 19 de abril de 2017 “Por el cual se modifica y adiciona el Decreto 1083 de 2015 Decreto Único Reglamentario del Sector Función Pública”, se estableció dentro de los roles de la Oficina de Control Interno el de "Evaluación de la Gestión del Riesgo".

Que en el mismo decreto, en su artículo 2.2.21.1.6, se dispone que son funciones del Comité Institucional de Coordinación de Control Interno: ”b. Aprobar el Plan Anual de Auditoría de la entidad presentado por el jefe de control interno o quien haga sus veces, hacer sugerencias y seguimiento a las recomendaciones producto de la ejecución del plan de acuerdo con lo dispuesto en el estatuto de auditoría, basado en la priorización de los temas críticos según la gestión de riesgos de la administración,“ Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta”.

Que mediante el Decreto 1499 de 2017, se modificó el Decreto 1083 de 2015, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Que mediante el Decreto 1499 de 2017, antes mencionado, se define el Sistema de Gestión, se establecen las políticas de gestión y desempeño institucional y se actualiza el Modelo Integrado de Planeación y Gestión, su objetivo, ámbito de aplicación, instancias y demás elementos para su implementación y evaluación; y además, se articula el Sistema de Control Interno, con el Modelo Integrado de Planeación y Gestión, a través de la Dimensión de control interno, la cual actualiza el Modelo Estándar de Control Interno MECI.

Que mediante el mismo Decreto 1499 de 2017, se incorpora la Gestión del Riesgo como uno de los cinco componentes del Modelo Estándar de Control Interno mediante un esquema de asignación de responsabilidades (Modelo de las Tres Líneas de Defensa) el cual se da una mirada simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes en todos los niveles de la organización.

Que este esquema se complementa con los lineamientos para la gestión del riesgo señalados en la Guía de Administración del Riesgo publicada por este Departamento Administrativo en 2018, cuyo contenido se encuentra sustentado los desarrollos incluidos en la norma ISO 31010, por tratarse del referente internacional a partir del cual se han venido realizando las actualizaciones a la guía en mención desde el año 2011.

Que no obstante, se hace necesario incorporar al texto de la Política Integral de Administración de la CAR, unos elementos básicos contenidos en la Guía para la Administración del Riesgo y el Diseño de Controles en la Entidades Públicas elaborada

por el Departamento Administrativo de la Función Pública en 2018.

Que, en virtud de lo anteriormente expuesto,

RESUELVE:

ARTÍCULO 1. ACTUALIZACIÓN DE LA POLÍTICA. Actualícese la Política de Administración de Riesgos para la Corporación Autónoma Regional de Nariño CORPONARIÑO, la cual deberán seguir todos los colaboradores de la Entidad; de conformidad con el contenido de la Guía para laAdministración del Riesgo y el Diseño de Controles en Entidades Públicas elaborada por el Departamento Administrativo de la Función Pública en 2018, la cual hará parte integral del presente acto administrativo.

ARTÍCULO 2. OBJETIVO DE LA POLÍTICA. El objetivo de la política es **e**stablecer las directrices y orientaciones metodológicas que permitan una adecuada identificación, análisis, valoración, evaluación, monitoreo, revisión y seguimiento de los Riesgos de la Corporación Autónoma Regional de Nariño –CORPONARIÑO, que le permita a la alta dirección de la Entidad tener una seguridad razonable en el logro de sus objetivos de proceso y/o institucionales, tomando medidas correctivas inmediatas en caso de alguna materialización.

ARTÍCULO 3. ALCANCE DE LA POLÍTICA. La presente política de Administración de Riesgos es extensible y aplicable a todos los procesos de la Corporación Autónoma Regional de Nariño CORPONARIÑO, a todas y cada una de las sedes de la entidad en sus diferentes ubicaciones geográficas y a todas las acciones ejecutadas por los servidores y contratistas de la Entidad, durante el ejercicio de sus funciones y obligaciones contractuales en todos los niveles de la organización, Esta política es la declaración de la Alta Dirección de la Corporación, con la participación del Comité Institucional de Coordinación de Control Interno respecto a la Gestión o Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital de CORPONARIÑONariño.

ARTICULO 4. ELEMENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS. En la

administración de los Riesgos de la Corporación, se consideran los siguientes elementos que permiten su eficiente Administración:

1. Política de Administración de Riesgos (Lineamientos de la Política)
2. Identificación de Riesgos:

   2.1 Establecimiento Contexto (Interno, Externo, del proceso, Identificación de activos)

   2.2 Identificación de Riesgos (Tipología de Riesgos)
3. Valoración de Riesgos

   3.1 Análisis de Riesgos (Análisis de Impacto)

   3.2 Evaluación de Riesgos (Riesgo Inherente, valoración de los controles, RiesgoResidual)

   3.3 Monitoreo y Revisión (Responsabilidades-Líneas de Defensa)

   3.4 Seguimiento (Reportes Periódicos)
4. Comunicación y Consulta

ARTICULO 5. METODOLOGÍA. La metodología se ajusta a la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas: Riesgos de Gestión, Corrupción y Seguridad Digital del Departamento Administrativo de la Función Pública DAFP, vigente.

Parágrafo. La Identificación y Valoración de Riesgos de los elementos del ARTÍCULO CUARTO de la presente Resolución, se encuentran descritos en **el Procedimiento Administración de Riesgos** GSG-PR-05 del Sistema Integrado de Gestión Pública y brinda los lineamientos de gestión detallada de la administración y gestión del Riesgo.

ARTICULO 6. NIVELES DE ACEPTACIÓN AL RIESGO. Los niveles de aceptación al riesgo de corrupción son.

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
Riesgos de Gestión porProcesos y **Riesgos de SeguridadDigital**	Baja	Se **ACEPTARÁ** el riesgo, no se adoptará ninguna medida que afecte la probabilidad o el impacto del Riesgo. **NINGÚN RIESGO DE CORRUPCIÓN PODRÁ** **SER ACEPTADO. (**Esta Zona de Riesgo sólo aplica para Gestión y Seguridad Digital**).**
	Moderada	Se adoptan medidas para **REDUCIR** la probabilidad o el impacto del riesgo o ambos, generalmente conlleva a la implementación de controles.

	Alta y Extrema	*Se adoptan medidas para **REDUCIR** o, *Tomar decisión de **EVITAR** el riesgo mediante la cancelación-abandono de las actividades que dan lugar al riesgo, es decir no iniciar o no continuar con la actividad que lo provoca (No hay riesgos después de tomar medidas de tratamiento) *Si es muy dificil para la entidad reducir el riesgo a un nivel aceptable: **COMPARTIR** el riesgo, reduciendo la probabilidad o el impacto y se transfiere parte del riesgo Ejemplo: Seguros o Tercerización (mecanismos de transferencia del riesgo deben estar formalizados a través de un acuerdo contractual) No se transfiere la responsabilidad, si el riesgo
Riesgos de Corrupción	Moderado	**REDUCIR, EVITAR, COMPARTIR (**No se transfiere la responsabilidad)
	Alta Extrema	**REDUCIR, EVITAR, COMPARTIR (**No se transfiere la responsabilidad)

ARTÍCULO 7. VALORACIÓN DE RIESGOS. La valoración de los Riesgos, consiste en establecer la Probabilidad de ocurrencia del riesgo (P) y el Nivel de Impacto (I), con el fin de estimar la zonade Riesgo Inicial (Riesgo Inherente).

Valoración del Riesgo = P (probabilidad) X I (Impacto)

ARTÍCULO 8. NIVELES PARA CALIFICAR LA PROBABILIDAD. La probabilidad es la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia (analiza el número de eventos en un periodo determinado) y factibilidad (analiza la presencia de factores internos y externos que pueden propiciar el riesgo, la posibilidad que se materialice).

La probabilidad es común en sus niveles a los Riesgos de Gestión, Corrupción y Seguridad Digital, así:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA

5	Casi seguro	Se espera que el evento ocurra enla mayoría de las circunstancias	Más de 1 vez alaño.
4	Probable	Es viable que el evento ocurra enla mayoría de las circunstancias	Al menos 1 vez enel 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 enlos últimos 5 años.
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.

ARTÍCULO 9. NIVELES PARA CALIFICAR EL IMPACTO. El impacto, son las consecuencias que ocasiona a la organización la materialización del riesgo, incluyendo sus potenciales consecuencias. **Parágrafo 1.** Para los Riesgos de Gestión y Seguridad Digital el impacto se mide en cinco (5) niveles a saber: Insignificante, Menor, Moderado, Mayor y Catastrófico.

RIESGOS DE GESTIÓN

NIVEL	IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO
CATASTRÓFICO 5	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución

	- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYO R4	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcialo incompleta. - Sanción por parte del ente de control uotro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación

MODERADO 3	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de Carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR 2	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.

	entidad.	
INSIGNIFICANTE 1	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicaso administrativas. - No se afecta la imagen institucional deforma significativa.

Parágrafo 2. Para los Riesgos de Corrupción los niveles de impacto son tan solo tres (3): Moderado, Mayor y Catastrófico, porque los Riesgos de Corrupción **SIEMPRE SON SIGNIFICATIVOS** en el impacto para la entidad, por eso NUNCA se pueden ASUMIR NI TOLERAR, y su impacto se califica a través de una Encuesta de Criterios.

Cada proceso debe diligenciar un (1) cuestionario de criterios para calificar impacto por cada riesgo de corrupción identificado, conservar original del documento diligenciado y remitir mediante memorando la respectiva copia soporte de cada calificación de impacto a la Oficina Asesora de Planeación en la administración de los Riesgos Institucionales, para que repose como evidencia de la calificación del Riesgo Inherente del Mapa de Riesgos de Corrupción.

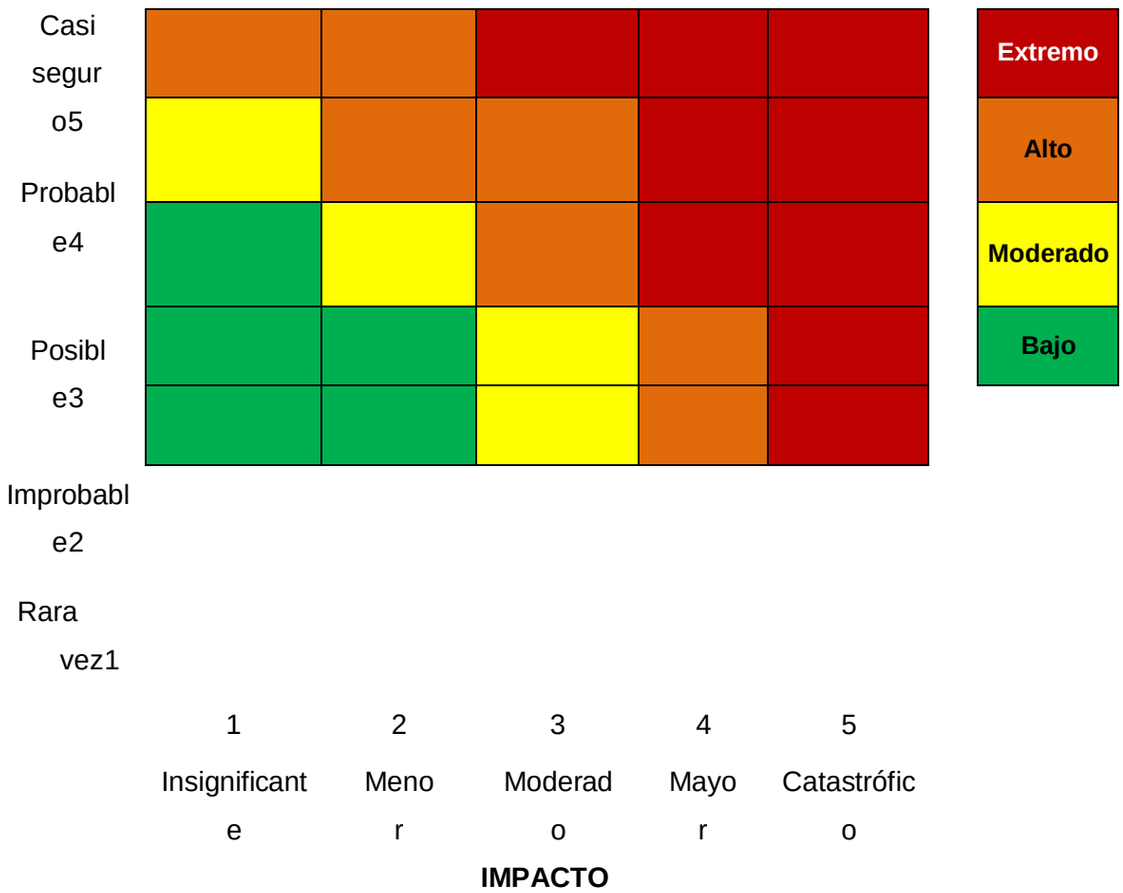
Para calificar el **impacto** a los **riesgos de corrupción** se debe partir del caso hipotético de la materialización del riesgo y tener en cuenta el siguiente cuestionario de criterios:

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SEMATERIALIZA PODRÍA…	RESPUEST ASI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el d metas y objetivos d la cumplimiento e e dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el de l misió del al qu cumplimiento a n sector e pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de **UNA a CINCO** pregunta (s) genera unimpacto **MODERADO** Responder afirmativamente de **SEIS a ONCE** pregunta (s) genera un impacto **MAYOR**			

Responder afirmativamente de **DOCE a DIECINUEVE** pregunta (s) generaun impacto **CATASTRÓFICO**			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad		

ARTÍCULO 10. NIVEL DE RIESGO. Para definir el nivel del riesgo, se inicia ubicando la valoración de la probabilidad (Rara vez, Improbable, Posible, Probable o Casi seguro). Posteriormente se determina el impacto en las columnas correspondientes. (Insignificante,Menor, Moderado, Mayor o Catastrófico).

Finalmente, se define el punto de intersección de las dos; que corresponderá al nivel de riesgo, de acuerdo al siguiente mapa de calor.



Fuente: Secretaría de Transparencia de la Presidencia de la República.

ARTICULO 11. RESPONSABLES, MONITOREO Y REVISIÓN. El Modelo Integrado de Planeacióny Gestión (MIPG) en la dimensión 7 “Control interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control. El modelo de las

líneas de defensa, es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad. Esté, proporciona aseguramiento de la gestión y previene la materializaciónde los riesgos en todos sus ámbitos.

A continuación, se detallan los roles y responsabilidades de todos los actores de la gestión del riesgo y el control en la Corporación Autónoma de Nariño –CORPONARIÑO, apropia el modelo de líneas de defensa, sus roles y responsabilidades, para proporcionar aseguramiento de la gestión institucional, previniendo la materialización de los Riesgos mediante el monitoreo y la revisión de los mismos, así:

LÍNEAS DE DEFENSA	RESPONSABLES	ACTIVIDADES
Línea Estratégica Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento.	*Alta Dirección *Comité Institucional de Coordinación de Control Interno	La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente: - Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. - Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. - Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. - Revisar los informes presentados de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como

		aquellas que están ocasionando que no se logre el cumplimiento de los

		objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. - Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
Primera Línea	*Líderes de procesos, programas y proyectos	Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente: - Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso. - Revisión como parte de sus procedimientos de supervisión,

Desarrolla implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	*Gerentes Públicos	la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación delos riesgos. - Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. - Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. - Revisar y reportar a planeación, los

		eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. - Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. - Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
Segunda Línea Soporta y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al	*Jefes de planeación Supervisores e interventores de contratos o proyectos - Coordinadores de otros sistemas de gestión TICS Riesgos de Seguridad Digital	- 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 solicitar y apoyar en la actualización de las matrices deriesgos. - La Oficina de las Tecnologías TIC´S acompañará el monitoreo y asesoramiento de la gestión y planes de tratamiento de los Riesgos de Seguridad Digital. - Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las

cumplimiento de las etapas de la gestión de riesgos.		recomendaciones a que haya lugar. - 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 determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos. - Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad. - Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. - Revisar los planes de acción 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 vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.
Tercera Línea Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el	Oficina de control interno	La oficina de control interno o auditoría interna monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente: - Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se

cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.		- identifiquen y actualicen las matrices de riesgos por parte de los responsables. Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. - Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. - Revisar el adecuado diseño y ejecución de los controles para lamitigación 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 los mismos. - Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. - Llevar a cabo la evaluación independiente a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno - Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas. - Para mitigar los riesgos de losprocesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

ARTICULO 12. MATERIALIZACIÓN DE UN RIESGO. Al materializarse un Riesgo de Corrupciónse debe impulsar las siguientes acciones:
1: Primera y Segunda Línea de Defensa:

- Informar a las autoridades y organismos de control correspondientes de la ocurrenciadel hecho de corrupción
- Revisar el Mapa de Riesgos en particular análisis de causas, valoración del riesgo, controles.
- Verifir si se tomaron las acciones y actualizar el mapa de corrupción con el ajuste del nivel de riesgo, nuevos controles y determinar acciones correctivas en el Plan Único de Mejoramiento Institucional PUMI, incrementar el monitoreo del riesgo.

Al materializarse un riesgo de Gestión el accionar debe ser:

- La primera línea de defensa debe informar a la segunda y tercera línea de defensa la materialización del riesgo
- Revisar y ajustar el Mapa de Riesgos en particular análisis de causas, valoración del riesgo, controles.
- Tomar acciones correctivas, de control y de mejora y actualizar el mapa de riesgos con el ajuste del nivel de riesgo, nuevos controles y determinar acciones correctivas en el Plan Único de Mejoramiento Institucional PUMI, monitoreando su cumplimiento y no repetición en su materialización.

Al materializarse un riesgo de Seguridad Digital se adiciona el hecho de informar a la Oficina de Tecnologías de la Información para que adelante las acciones en materia de seguridad digital a que haya lugar, y acompañe el establecimiento de controles aún más restrictivos que permitan asegurar que la triada de la información en el activo se mejore y mantenga e identificar las nuevas amenazas y vulnerabilidades para los activos de información.

2: Tercera Línea de Defensa: Para los Riesgos de Gestión, Seguridad Digital y Corrupción.

- Informar a las autoridades y organismos de control correspondientes de la ocurrenciadel hecho de corrupción

- Determinar la efectividad de los controles
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir omitigar los riesgos.
- Determinar si se adelantaron acciones de monitoreo
- Revisar las acciones de Monitoreo y el cumplimiento y efectividad del Plan de Mejoramiento realizando la retroalimentación a las líneas de defensas anteriores de las observaciones y hallazgos.

ARTICULO 13. VARIABLES DEL DISEÑO DE CONTROLES. Al momento de definir un control para que mitigue de manera adecuada el riesgo, se deben considerar obligatoriamente, desde la redacción del mismo, las siguientes seis (6) variables:

VARIABLE	DESCRIPCIÒN
1. RESPONSABLE (QUIÈN)	- Persona asignada para ejecutar el control. - El control debe iniciar con un cargo responsable o un sistema o aplicación (nunca nombres de personas) - Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso (debe tener un remplazo o apoyo, para que así si este responsable quisiera hacer algo indebido, por sí solo, no lo podrá hacer).
2. PERIODICIDAD (CADA CUÀNTO)	- Definir una periodicidad específica para la ejecución del control - De igual forma hay controles automáticos que son programados para que se ejecuten en un tiempo específico, estos controles también tienen una periodicidad (Cada vez que se va a realizar...)
3. PROPÓSITO DEL CONTROL (QUÈ BUSCA)	- El control debe tener un propósito (verificar, validar, cotejar, comparar, revisar, etc.) para mitigar la causa de la materialización del riesgo. - El propósito debe indicar para qué se realiza y que ese propósito conlleve a prevenir las causas que generan el riesgo

4. CÒMO SEREALIZA (CÒMO)	- Debemos preguntarnos si la fuente de información es confiable, el control debe indicar cómo se realiza de manera que se pueda evaluar la fuente (a través de.. se toma dicha información directamente de… comparando.) ejemplo listas de chequeo, portal web, base de datos entre otros
5. QUÈ PASA CONLAS	- El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control (en caso de…). - Si como resultado de un control preventivo se observan derencias o
OBSERVACIONESO DESVIACIONES (QUÈ PASARÌA SI..)	- aspectos que no se cumplen la actividad NO debería continuarsehasta que se subsane la situación.
6. EVIDENCIA (DÓNDE QUEDA)	- Dejar evidencia de la ejecución del control, documento para poder - evaluar que el control realmente fue ejecutado de acuerdo a las cincovariables anteriores.

ARTICULO 14. ACTIVIDADES DE CONTROL. Son las acciones establecidas a través de políticas (establecen las líneas generales del control interno) y procedimientos (llevan las políticas a la práctica) que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que indicen en el cumplimiento de los objetivos. La actividad de control debe por sí misma mitigar o tratar la causa del riesgo y ejecutarse como parte del día a día de lasoperaciones.

Parágrafo 1: Controles Preventivos. 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. Ejemplo: Revisión al cumplimiento de requisitos contractuales en el proceso de selección del contratista o proveedor.

Parágrafo 2: Controles Detectivos. Controles que están diseñados para identificar un evento o resultado no previsto después que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes. Ejemplo: Realizar una conciliación bancaria para verificar que los saldos en libros correspondan a los saldos de bancos.

ARTICULO 15. SEGUIMIENTO Y EVALUACIÓN. Conforme a lo establecido por el Departamento Administrativo de la Función Pública DAFP y de la Secretaria de Transparencia, y atendiendo a la normatividad vigente aplicable; la periodicidad establecida por la Corporación Autónoma Regional de Nariño – CORPONARIÑO será:

1. El monitoreo de la segunda línea de defensa (Oficina Asesora de Planeación riesgos de gestióny Oficina de TIC´s para riesgos seguridad de la información) y la evaluación de la tercera línea de defensa al mapa de riesgos de gestión y seguridad digital, será con una **periodicidad de corte Semestral**, generando las acciones de comunicación y consulta pertinentes.

2. Para los Riesgos de Corrupción, **el monitoreo por parte de la segunda línea de defensa se realizará bimestralmente**, **y evaluación por parte de la tercera línea de defensa se realizará cuatrimestralmente,** así:

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirsedentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro delos diez (10) primeros días del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.
La evaluación independiente adelantada por la Oficina de Control Interno o quien haga sus veces, deberá publicar los resultados de tales evaluaciones en la página web de la Entidad en la sección: Transparencia y Acceso a la Información Pública, dentro del plazo establecido.

3: La estructuración y administración de la matriz Mapa de Riesgos Institucionales al igual que el procedimiento para operativizar la administración de los Riesgos de la Entidad, estará a cargo de la Oficina Asesora de Planeación bajo el proceso Gestión.

ARTICULO 16. COMUNICACIÓN Y CONSULTA. Es un elemento transversal a todo el proceso de Administración del Riesgo, estrategias de comunicación, trabajo en equipo, conocimiento y análisis de cada uno de los procesos, la información, comunicación y reporte se establece en el siguiente esquema por líneas de defensa, así:

LÍNEA DE DEFENSA	INFORMACIÓN, COMUNICACIÓN Y REPORTE
LÍNEA ESTRATÉGICA	- Corresponde al Comité Institucional de Coordinación de Control Interno-CICCI, establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.
PRIMERA LÍNEA DE DEFENSA	- Corresponde a los líderes de procesos, jefes de área y/o grupo (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.
SEGUNDA LÍNEA DEFENSA	- Corresponde a la Oficina Asesora de Planeación encargada de la gestión del riesgo (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación. La Oficina de las Tecnologías TIC´S acompañará el monitoreo y asesoramiento de la gestión y planes de tratamiento de los Riesgos de Seguridad Digital.
TERCERA LÍNEA DEFENSA	- Le corresponde a la Oficina de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

ARTICULO 17. VIGENCIA. La presente Resolución rige a partir de la fecha de su expedición.

ARTÍCULO 18. **PUBLICACIÓN**. Publicar el presente acto administrativo en la página WEB y elBoletín de la Corporación.

ARTÍCULO 19. Contra la presente resolución no procede recurso alguno, de conformidad con lodispuesto en el artículo 75 de la Ley 1437 de 2011.

Dada en Pasto a los 31 Días del mes de diciembre de 2021

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

HUGO MIDEROS LÓPEZ

Director General-CORPONARIÑO

Proyectó:

Daniel Hernández-Contratista MIPG - Planeación y D.E

Revisó:

PABLO CESAR ROJAS C.

Jefe Oficina de Planeación y D.E

FABIO CÁRDENAS

Jefe Oficina de Control Interno.

IVÁN MAURICIO SANTACRUZ
Jefe Oficina Jurídica