Corporación Autónoma
Regional del Tolima
¡Siembra Tu Futuro!

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS EN LA CORPORACIÓN AUTÓNOMA REGIONAL DEL TOLIMA - CORTOLIMA

AGOSTO

2022

TABLA DE CONTENIDO

1. DECLARACION DE COMPROMISO 2
2. INTRODUCCIÓN 3
3. DEFINICIONES:..... 3
4. ALINEACIÓN CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN 8
5. OBJETIVO GENERAL. 9
5.1 OBJETIVOS ESPECIFICOS. 10
6. ALCANCE 10
7. RESPONSABILIDADES..... 11
8. POLITICA DE ADMINISTRACION DE RIESGOS 17
10. NIVELES DE ACEPTACION DE RIESGO 20
11. NIVELES DE VALORACION DE IMPACTO Y PROBABILIDAD 22
Determinación de la probabilidad. 22
Determinación del impacto..... 23
12. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS..... 25
13. SEGUIMIENTO A LOS MAPAS DE RIESGOS Y CONTROLES..... 26
14. ESTRATEGIA SEGUIMIENTO AL PLAN DE ACCION DEL MAPA DE RIESGOS.... 27
15. COMUNICACIÓN Y SOCIALIZACIÓN..... 28

1. DECLARACION DE COMPROMISO

La Corporación Autónoma Regional del Tolima –Cortolima- se compromete a administrar los riesgos operativos, de corrupción y de seguridad digital, relacionados

con las actividades que desarrollan los procesos para el logro de los Objetivos, Planes y proyectos, orientando sus esfuerzos en la identificación, valoración y control de los riesgos con el fin de mantenerlos en niveles aceptable procurando evitar su materialización, usando para ello el esquema de líneas de defensa.

2. INTRODUCCIÓN

La estructuración del presente documento está basada en la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5, elaborada por el Departamento Administrativo de la Función Pública –DAFP-, tomando como modelo la Política de Administración de Riesgos en Función Pública.

Este documento corresponde a una actualización de la política de administración de riesgos, teniendo en cuenta los ajustes generados en la estructura orgánica de la Corporación a partir del acuerdo 014 de 2021, mediante el cual se realizó el rediseño institucional de la entidad; así mismo en lo que respecta a la matriz de riesgos se realiza la actualización de los mismos y se incluyeron aspectos fundamentales para la organización para el cumplimiento de la misión y objetivos institucionales, como lo son los riesgos de Seguridad de la Información, riesgos en Seguridad y salud y trabajo, riesgos por conflicto de interés y los riesgos de daño antijurídico.

La política de la Corporación Autónoma Regional del Tolima - CORTOLIMA, se establece como un instrumento que direcciona la gestión del riesgo facilitando la toma de decisiones sobre el tema, fomenta la cultura organizacional de prevención ante el riesgo, establece los roles y responsabilidades de los servidores públicos en el marco de las líneas de defensa conforme a lo establecido en la Resolución 1811 del 29 de abril del 2022 expedida por Cortolima así como las que la modifiquen y/o adicionen.

3. DEFINICIONES:

Para facilitar la comprensión de la presente política se consideran los siguientes términos:

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

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

ÁREAS DE IMPACTO: consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

CAPACIDAD DE RIESGO: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

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

CAUSA INMEDIATA: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

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

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

CONTROL: Medida que permite reducir o mitigar un riesgo.

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

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

ESTRATEGIA PARA COMBATIR EL RIESGO. (Tratamiento): Decisión que se toma frente a un determinado nivel de riesgo. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente y puede ser:

REDUCIR: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

TRANSFERIR: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

MITIGAR: Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

ACEPTAR: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

EVITAR: Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

EVENTO: Riesgo materializado. Los eventos de riesgo son aquellos incidentes que generan o podrían generar pérdidas a la entidad.

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.

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

INTEGRIDAD: Propiedad de la información que se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

MAPA DE RIESGOS: Documento con la información resultante de la gestión del riesgo, administrado por la Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico.

MODELO DE TRES LÍNEAS DE DEFENSA: Realza el entendimiento del manejo de riesgos y controles mediante la asignación o clarificación de roles y responsabilidades a través de toda la Corporación.

NIVEL DE RIESGO: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad X Impacto.

PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO: Instrumento de tipo preventivo para el control de la corrupción, su metodología incluye cinco

componentes autónomos e independientes, que contienen parámetros y soporte normativo propio y un sexto componente que contempla iniciativas adicionales.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

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

PUNTOS DE RIESGO: Son actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

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

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

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

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

RIESGO RESIDUAL: Es el riesgo resultante de la aplicación de controles. Algunos requieren de un plan de acción para llevar su nivel de severidad al nivel del apetito del riesgo determinado por la, Corporación.

RIESGO OPERATIVO: El riesgo operativo hace referencia a la posibilidad de que la Corporación incurra en pérdidas originadas por errores humanos, fallas tecnológicas o procesos, infraestructura, o por factores externos.

SEVERIDAD: Nivel de un riesgo, dado por una probabilidad y un impacto. En cada nivel se define el tratamiento y los niveles de responsabilidad.

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

4. ALINEACIÓN CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN – MIPG

El Modelo Integrado de Planeación y Gestión – MIPG se define como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio[1].

El Modelo Integrado de Planeación y Gestión – MIPG, para su operación se encuentra estructurado por 7 dimensiones (talento humano, direccionamiento

[1] Manual Operativo MIPG, 2021, página 8

estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y control interno). Cada una de las dimensiones incluye una o varias políticas de gestión y desempeño institucional que al ser implementadas de manera articulada el MIPG funciona adecuadamente.

La dimensión de Direccionamiento Estratégico y Planeación, articula la gestión de administración del riesgo con el Modelo Integrado de Planeación y Gestión – MIPG, desde la política de Planeación Institucional, estableciendo los criterios para la formulación de la presente política. Otra dimensión que permite su articulación, es la de Control Interno, la cual determina aspectos relacionados con el esquema de las líneas de defensa, que permiten definir roles y responsabilidades enmarcados en la gestión del riesgo y el control fundamentado en los componentes del MECI, los cuales apoyan la estructuración del control dentro de la Corporación. Estos componentes son: ambiente de control, evaluación del riesgo y actividades de control.

5. OBJETIVO GENERAL.

Establecer las directrices y lineamientos metodológicos que permitan una adecuada identificación, análisis, valoración, evaluación, monitoreo, revisión, control y seguimiento de los Riesgos de la Corporación Autónoma Regional del Tolima - CORTOLIMA, con el fin de minimizar y controlar los efectos adversos que generan la materialización de los riesgos y fortalecer la toma de decisiones oportunas para el cumplimiento de las metas y objetivos institucionales en el marco del Modelo Integrado de Planeación y Gestión – MIPG y el Departamento Administrativo de la Función Pública.

5.1 OBJETIVOS ESPECIFICOS.

- Concientizar en todos los niveles de la Corporación sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos a la gestión institucional, de corrupción y los que afectan los activos de información.
- Establecer una metodología integral para la administración de riesgos, adecuada de acuerdo con el marco normativo vigente.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y planificación institucional.
- Identificar el nivel de aceptación del riesgo de gestión, corrupción y seguridad de la información que asume la entidad frente al apetito, tolerancia y capacidad del riesgo.

6. ALCANCE

La Política de Administración de Riesgos es aplicable a todos los procesos de la Corporación Autónoma Regional del Tolima – CORTOLIMA, planes, proyectos, trámites, servicios, procesos de la entidad durante su gestión, y a todos los servidores públicos y contratistas mediante el ejercicio de sus funciones y obligaciones contractuales en todos los niveles y oficinas territoriales.

Incluye directrices para gestionar de manera adecuada los riesgos de gestión, corrupción, fraude, seguridad de la información, conflictos de interés, daño antijurídico y seguridad y salud en el trabajo. También hace referencia a otras clasificaciones de riesgos basados en requisitos legales y normativos.

Involucra las etapas de análisis, identificación, tratamiento, evaluación, monitoreo y seguimiento de los riesgos que puedan afectar la carta estratégica institucional.

No aplica para riesgos antrópicos, naturales y políticos.

Para los riesgos relacionados con los bienes de Cortolima o los que se encuentran en su custodia, con la finalidad de proteger el patrimonio público, en caso de pérdida, daño o deterioro de los bienes del Estado y con el fin de obtener su resarcimiento, se deben constituir pólizas de seguros que amparen dichos bienes, conforme a lo establecido en la Ley 42 del 1993.

7. RESPONSABILIDADES

La responsabilidad en asuntos propios de la identificación, valoración y control de los riesgos está definida mediante el esquema de líneas de defensa que se encuentran contenidos en la Resolución 1811 de 29 de abril de 2022 emitida por Cortolima, en especial lo establecido en el Articulo 5 “ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO, Identificar los roles y responsabilidades de los actores en la implementación, operación, seguimiento y fortalecimiento propuesto en el Modelo Integrado de Planeación y Gestión -MIPG, tal como se presenta en la tabla 1.

Tabla 1: *Esquema de responsabilidad de las líneas de defensa frente al riesgo.*

LINEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO.
LINEA ESTRATEGICA	Alta Dirección	- Analizar los cambios en el entorno (Contexto Interno y externo) que pueda tener un impacto significativo en la operación de la entidad y generen cambios en la estructura de riesgos y controles.
	Comité Directivo Comité de Gestión y Desempeño Institucional	- Asegurar la implementación y desarrollo de las Políticas de Gestión y directrices en materia de seguridad digital y de la información. - Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. - Recomendaciones de mejoras a la Política de operación para la administración del riesgo. - Garantizar el cumplimiento de los planes de la entidad. - Revisar el cumplimiento de los objetivos institucionales y de procesos, así como los indicadores e identificar en caso de

		incumplimiento los posibles riesgos que se están materializando.
	Comité Institucional de Coordinación de Control Interno	- Revisar y aprobar la Política de Administración del Riesgo previamente estructurada por parte de la Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico como segunda línea de defensa en la entidad; - Generar directrices para realizar seguimiento a la Política de Administración de Riesgos, para su posible actualización y evaluar su eficacia frente a la gestión del riesgo institucional. - Revisar la Política de administración del riesgo por lo menos una vez al año para su actualización y validar su eficacia a la gestión del riesgo institucional. - Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. - Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. - 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.
PRIMERA LINEA DE DEFENSA	Líderes de Procesos y subprocesos Equipos de trabajo.	- Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo. - Delegar por parte del Coordinador del proceso, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos al interior de los grupos de trabajo o dependencias. - Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. - Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y su documentación. - Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles

		seleccionados para el tratamiento de los riesgos identificados. - Reportar al SGI los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. - Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. - Informar a la Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo y aplicar las acciones correctivas o de mejora necesarias. - Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces. - En caso de la materialización de un riesgo no identificado, este debe ser gestionado en el mapa de riesgos institucional, informático o de corrupción. **El coordinador del proceso debe:** - Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación. - Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su proceso y/o subproceso y las acciones a seguir. - Comunicar al equipo de trabajo los resultados de la gestión del riesgo. - Revisar y actualizar el mapa de riesgos con el acompañamiento de la Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico. **Los servidores en general deben:** - Participar en el diseño de los controles que tienen a cargo. - Ejecutar el control de la forma como está diseñado. - Proponer mejoras a los controles existentes.

		<u>El responsable del proyecto debe:</u> - Realizar la identificación de los riesgos del proyecto. - Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. - Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. - Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.
SEGUNDA LINEA DE DEFENSA	Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico	- Asesorar a la Línea Estratégica en el análisis del contexto interno y externo, la definición de la Política de Riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. - Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del Comité Institucional de Coordinación de Control Interno. - Capacitar al grupo de trabajo de cada proceso y subproceso como líder de la política de riesgos. - Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. - Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. - Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad. - Hacer monitoreo al Plan de Acción establecido por el proceso para la mitigación de los riesgos de los procesos reportados a la Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico.

		- Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos para presentación a la Oficina de Control Interno a la Gestión. - Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos o proyectos. - Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. - Coordinar con los líderes de proceso el responsable de reporte de seguimiento a los riesgos, controles y planes de acción. - Informar a la primera línea de defensa la importancia de socializar los riesgos consolidados en el mapa de riesgos de Cortolima, al interior de su proceso y/o subproceso. - Socializar y publicar el mapa de riesgos institucional. - Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. - Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y logar el cumplimiento a los objetivos. - Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser incluido en el mapa de riesgo institucional. - Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. - Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean gestionados por la primera línea de defensa.

TERCERA LINEA DE DEFENSA	Oficina Asesora de Control Interno a la Gestión	- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables, así mismo las modificaciones a la Política de Administración de Riesgos, cuando se amerite de acuerdo al contexto. - Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos, para el debido cumplimiento de los objetivos institucionales. - Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. - Asesorar a la primera línea de defensa de forma coordinada con la Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico, en la identificación de los riesgos y diseño de controles. - Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI. - Revisar el perfil del riesgo inherente y residual de cada proceso y pronunciarse sobre cualquier riesgo que se encuentre por fuera de la matriz de riesgos de la Corporación o que su calificación de impacto o probabilidad no sea coherente con los resultados de las auditorías realizadas. - Realizar seguimiento a la implementación de mejoras sobre los lineamientos de continuidad del negocio. - Realizar seguimiento a la implementación de la estrategia de continuidad del negocio y a las pruebas efectuadas. - Recomendar mejoras a la política de operación para la administración del riesgo.

Fuente: Resolución 1811 de 2022 Cortolima.

Así mismo, la matriz de responsabilidad y autoridad de la Corporación define los cargos que pueden identificar, valorar, evaluar y definir controles y reportar los riesgos institucionales, por lo cual dicha matriz hace parte de este documento.

8. POLITICA DE ADMINISTRACION DE RIESGOS

La política de administración de riesgos de la Corporación Autónoma Regional del Tolima – CORTOLIMA, es de carácter estratégico y se estructura con relación al Modelo Integrado de Planeación y Gestión – MIPG, la guía de administración del riesgo y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores y contratistas de la entidad.

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

Los riesgos operativos de cada proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.

Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

Los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

Los riesgos de seguridad y salud en el trabajo, en el marco del sistema de gestión de seguridad y salud en el trabajo se identifican y gestionan de acuerdo a lo definido en la GTC 45, que establecen la identificación de peligros, valoración de riesgos y establecimiento de controles, la cual se encuentra definido y valorado en la Matriz de Riesgos y Peligros IPEVR.

Los riesgos de daño antijurídico, que permiten prevenir las deficiencias administrativas y misionales que generen litigiosidad y que implique el uso de recursos públicos para mitigar estas causas generadoras de demandas contra la entidad.

Los riesgos de conflicto de interés en donde los servidores públicos y contratistas conozcan sobre las situaciones en las que sus intereses personales pueden influir en el cumplimiento de sus funciones y responsabilidades, en beneficio particular o de un tercero, afectando el interés público, con el fin de que puedan ser advertidos y gestionados en forma preventiva, evitando que se favorezcan intereses ajenos al bien común.

Los riesgos de fraude interno y externo se acogen metodológicamente a la presente política para la tipología de riesgos de gestión.

Así mismo, Cortolima determina que la matriz de riesgos, es la herramienta que permite identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción, de seguridad y salud en el trabajo, de seguridad digital, de conflictos de interés y de daño antijurídico, para lo cual la oficina asesora de planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento y cargue de información.

El periodo de revisión e identificación de los riesgos institucionales se debe realizar cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción anual, asegurando la articulación de éstos con los compromisos de cada proceso.

9. CLASIFICACIÓN DEL RIESGO

Los riesgos en la Corporación Autónoma Regional del Tolima - CORTOLIMA, se clasifican según las tipologías descritas en la tabla 2.

***Tabla 2**. Clasificación de los riesgos*

TIPO	CLASIFICACIÓN	DESCRIPCIÓN
	Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
	Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

Riesgos de gestión	Relaciones laborales	Pérdidas que surgen de acciones contrarias a lasleyes o acuerdos de empleo, contratación, salud o seguridad, del pago de demandas por dañospersonales o de discriminación.
	Usuarios, trámites y servicios	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios en la prestación de trámites y servicios.
	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.
	Legales	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la entidad debido a su incumplimiento o desacato a la normativa vigente.
	Estratégicos	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la Corporación y por tanto impactan toda la entidad.
	Sistemas de Gestión	Posibilidad de ocurrencia de eventos que afecten la implementación, operación, mantenimiento y sostenibilidad de los Sistemas de Gestión que conforman el Sistema Integrado de Gestión Pública SIGESPU.
Riesgos de seguridad de la información	Pérdida de confidencialidad	Pérdida de la propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
	Pérdida de integridad	Pérdida de la propiedad de exactitud y completitud de la información.
	Pérdida de disponibilidad	Pérdida de la propiedad de la información de ser accesible y utilizable a demanda por la entidad.
Riesgos de fraude	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 Corporación, en las cuales está involucrado por lo menos un participante interno de la entidad y en donde prevalece la intencionalidad y/o el ánimo de lucropara sí mismo o para terceros.

Riesgos relacionados con posibles actos de corrupción	Riesgos de corrupción	Posibilidad de que por acción u omisión, se use elpoder para desviar la gestión de lo público hacia un beneficio privado.
	Conflicto de intereses	Posibilidad de que una situación producida por un interés particular pueda influir o sesgar el juicio/decisión de un servidor público contratista en el ejercicio de sus funciones u obligaciones contractuales.
	Riesgos de corrupción asociados a trámites y servicios	Posibilidad de que por acción u omisión, se use elpoder para desviar la gestión de lo público en la prestación de trámites y servicios hacia un beneficio privado.

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

10. NIVELES DE ACEPTACION DE RIESGO

Conforme a los riesgos residuales aprobados por los líderes de procesos, se define la periodicidad de seguimiento anual, para los riesgos de gestión, seguridad de la información, conflictos de interés, defensa jurídica, seguridad y salud en el trabajo y en periodos cuatrimestrales para los riesgos de corrupción.

Cortolima determina que para los riesgos residuales de gestión y seguridad de la información que se encuentren en zona de riesgo baja, que se encuentren con una valoración inferior al 30%, la Corporación está dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento, no obstante, se determina el nivel de apetito del riesgo en 16%.

Respecto a los riesgos de seguridad de información en Cortolima, la responsabilidad para la identificación de estos recae en la Oficina Asesora de Direccionamiento estratégico TIC. Se identifican los siguientes tres (3) riesgos

inherentes de seguridad de la información:

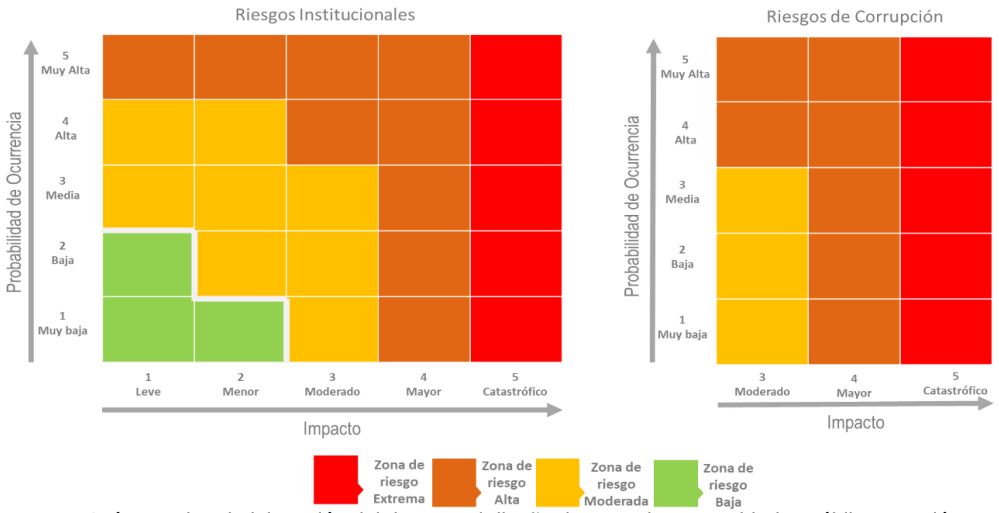
- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Nota: Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis. (https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b)

La siguiente grafica (Gráfica 1) muestra los rangos de valoración del impacto y la probabilidad con el fin de determinar el nivel de severidad del riesgo y establecer el curso de acción para su tratamiento.

Gráfica 1. Mapa de Calor y Matriz de Valoración y Calificación de Nivel de Severidad del Riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5

11. NIVELES DE VALORACION DE IMPACTO Y PROBABILIDAD

Determinación de la probabilidad.

Para efectos del análisis para calificar la probabilidad de ocurrencia, esta, se asocia a la exposición al riesgo del proceso o actividad que se esté examinando. De este modo: la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

La frecuencia en la que pasa la actividad por el punto de riesgo, determina la exposición al riesgo. La siguiente tabla establece la valoración de la probabilidad en porcentaje, y su clave de calor. Estos factores deberán tenerse en cuenta en la valoración del riesgo en lo referente a la probabilidad.

***Tabla 3**. Valoración de la probabilidad*

Frecuencia de la Actividad	Probabilidad

Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V 5, DAFP

Determinación del impacto.

El impacto se mide de acuerdo a la afectación de la Corporación por la materialización de un riesgo, bajo los parámetros, afectación económica y afectación reputacional. Cuando se presenten ambos impactos para un riesgo con diferentes niveles, se debe tomar el nivel más alto.

Para efectos de la medición del nivel de impacto del riesgo se deberá tener en cuenta la siguiente tabla.

***Tabla 4**, Criterios para definir el nivel de impacto*

	Afectación Económica	Reputacional
Leve: 20%	Afectación menor a 50 SMLMV	El riesgo afecta la imagen de algún área de la organización.

Menor: 40%	Entre 50 y 200 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de Consejo Directivo y/o de proveedores.
Moderado: 60%	Entre 200 y 1000 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor: 80%	Entre 1000 y 5000 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico: 100%	Mayor a 5000 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V 5, DAFP

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

Tabla 5. *Calificación del Impacto para los riesgos de Corrupción*

No.	Pregunta: Si el riesgo de corrupción se materializa podría	Respuesta Si	 No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		

6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Nivel	Descriptor	Descripción	Respuestas afirmativas
1	Moderado	Genera medianas consecuencias sobre la entidad.	1 a 5
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11
3	Catastrófico	Genera consecuencias desastrosas para la entidad.	12 a 19

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v5.

12. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se materializan los riesgos identificados en la matriz de riesgos se deben aplicar las acciones descritas en la tabla 6 Acciones de respuesta riesgos materializados.

***Tabla 6**, Acciones de respuesta riesgos materializados.*

Responsable	Acción

Coordinador de proceso (Primera línea de defensa)	Informar a la Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico sobre el hecho encontrado y dependiendo del alcance y/o al hecho de corrupción materializado. Identificar las acciones correctivas necesarias y documentarlas, generar el Plan de Mejoramiento con el respectivo análisis de causas y determinación de acciones preventivas y de mejora. Coordinar con la Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico, la actualización pertinente dentro del Mapa de riesgos.
Oficina Asesora de Planeación Institucional y Direccionamiento Estratégico (Segunda Línea de Defensa)	Incluir en el mapa de riesgos la actualización pertinente del riesgo materializado, revisando la adecuada identificación, valoración y diseño de controles realizadas por parte de la Primera Línea. Realizar monitoreo de las actividades de control establecías para el tratamiento del riesgo dentro de la periodicidad establecida. (*Cuatrimestral*). Realizar monitoreo al cumplimiento de las acciones correctivas necesarias y documentarlas, Requerir el Plan de Mejoramiento con el respectivo análisis de causas y determinación de acciones preventivas y de mejora elaborados por los Coordinadores de Procesos.
Oficina Asesora de Control Interno a la Gestión (Tercera Línea de Defensa)	Informar a los Coordinadores de procesos, quienes analizarán las situaciones y definirá las acciones a que haya lugar, realizando las denuncias respectivas ante los órganos de control correspondientes. Verificar que el riesgo materializado se encuentra correctamente incluido y controlado en el mapa de riesgos. Realizar seguimiento a las actividades de control establecías para el tratamiento del riesgo dentro de la periodicidad establecida. Realizar seguimiento al cumplimiento de las acciones correctivas necesarias y documentarlas, hacer seguimiento al Plan de Mejoramiento con el respectivo análisis de causas y determinación de acciones preventivas y de mejora.
Comité de Coordinación de Control Interno. (Línea Estratégica)	Analizará las causas de los eventos (riesgos materializados) y definirá cursos de acción.

13. SEGUIMIENTO A LOS MAPAS DE RIESGOS Y CONTROLES

La periodicidad de los mapas de riesgos y controles de Cortolima se realiza de acuerdo a lo indicado en la tabla 7, Seguimiento a mapa de riesgos y controles.

Tabla 7, Seguimiento a mapa de riesgos y controles***.***

Tipo de Riesgo	Estrategia de Tratamiento - Controles
Riesgos de Gestión y Riesgos de seguridad de la Información	Se realiza seguimiento a los controles con periodicidad **ANUAL** y se registra en el Mapa de Riesgos
Riesgos de Corrupción	Se realiza seguimiento a los controles con periodicidad **CUATRIMESTRAL** y se registra en el Mapa de Riesgos

Fuente: Política de Administración de Riesgos en Función Pública

14. ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCION DEL MAPA DE RIESGOS

Para los riesgos que requieran de plan de acción, de acuerdo a su valoración residual, se hace seguimiento de acuerdo a lo considerado en la tabla 8, Estrategias de Seguimiento al plan de acción.

Tabla 8, Estrategia de seguimiento al plan de acción

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de Tratamiento – Plan de Acción
Riesgos de	Baja (menos del 30%)	No se debe realizar plan de acción porque está dentro del nivel de aceptación del riesgo establecido por Cortolima.

Gestión, y Seguridad digital	Moderada Alta Extrema	El Coordinador del proceso define acciones orientadas a mitigar el riesgo residual, determinando la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles. Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.

Fuente: Política de Administración de Riesgos en Función Pública

15. COMUNICACIÓN Y SOCIALIZACIÓN

La Presente Política de Administración de Riesgos deberá ser publicada en la página web de la Corporación Autónoma Regional del Tolima – CORTOLIMA, www.cortolima.gov.co

Los mecanismos de comunicación y socialización para dar a conocer la Política de Riesgos en todos los niveles de la entidad, serán acordes al Plan de Comunicaciones con el que cuenta la Corporación.

16. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN
30/08/2022	00	Actualización de la Política de Administración de Riesgos. Se ajustan y actualizan actividades de acuerdo a la implementación del sistema de información. Se modifica codificación. Viene de procedimiento PR_EV_001 V-03