



“POR MEDIO DE LA CUAL SE MODIFICA LA POLITICA DE ADMINISTRACION DE RIESGOS EN LA CORPORACION AUTONOMA REGIONAL DEL GUAVIO – CORPOGUAVIO Y SE TOMAN OTRAS DETERMINANTES

El Director General de la Corporación Autónoma Regional del Guavio CORPOGUAVIO, en ejercicio de las facultades legales y estatutarias, en especial las conferidas por los artículos 28 y 29 de la Ley 99 de 1993 y el Acuerdo de Consejo Directivo No. 016 del 23 de octubre de 2015 y,

CONSIDERANDO

Que el artículo 269 de la Constitución Política de 1991 establece que las entidades públicas, están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de Control Interno, de conformidad con lo que dispone la Ley;

Que el literal a) del artículo 2° de la Ley 87 del 29 de noviembre de 1993 “Por la cual se establecen normas para el ejercicio de Control Interno en las entidades y organismos del Estado y se dictan otras disposiciones”, establece que se deben proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten;

Que la Ley 489 del 29 de diciembre de 1998 “Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones”, en su artículo 28, referente al fortalecimiento del Sistema de Control Interno de las Instituciones públicas, dispuso la aplicación de instrumentos de gerencia, con el fin de fortalecer el cumplimiento cabal y oportuno de las funciones del Estado;

La Ley 1474 de 2011 determinó el rol que deben desempeñar las oficinas de control interno, auditoría interna o quien haga sus veces, deberán posicionar su labor con el fin de contribuir de manera independiente en la consecución de los objetivos de sus entidades. Esta disposición permite a las unidades de control interno, auditoría interna o quien haga sus veces, alcanzar un mayor nivel de independencia respecto de los representantes legales de las entidades, así como generar un ambiente propicio para desarrollar sus funciones de manera objetiva e imparcial, sin olvidar que su función constituye una parte estratégica para la organización. Con el fin de contribuir en la consecución de los objetivos de las entidades, los jefes de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces, deben convertirse en actores estratégicos por medio de la generación de valor a la entidad y la alerta de manera oportuna sobre aquellos riesgos actuales o potenciales que pueden afectar el desempeño institucional.

Que de acuerdo con lo señalado en el artículo 9 de la Ley 87 de 1993 el jefe de control interno es el encargado de medir y evaluar la eficiencia y eficacia de la gestión de la respectiva entidad a la que pertenece. Que el artículo 9 de la Ley 1474 de 2011, modificado por el artículo 231 del Decreto ley 019 de 2012, determina que los jefes de control interno o quien haga sus veces, sin perjuicio de las demás obligaciones legales, deberá reportar a los organismos de control, los posibles actos de corrupción e irregularidades que haya encontrado en el ejercicio de sus funciones.



Con ocasión de la entrada en vigencia del Modelo Integrado de Planeación y Gestión (MIPG), que integra los Sistemas de Gestión de la Calidad y de Desarrollo Administrativo, crea un único Sistema de Gestión y, lo articula con el Sistema de Control Interno, el Modelo de las Tres Líneas de Defensa, con el fin de entregar a los ciudadanos, lo mejor de la gestión para producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción

Que el artículo 73 de la Ley 1474 del 12 de julio de 2011 determina que cada entidad del orden nacional deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano, la cual debe contemplar, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad y las medidas concretas para mitigar esos riesgos, en concordancia con lo establecido en la política de transparencia, participación y servicio al ciudadano, componente plan anticorrupción del nuevo modelo integrado de planeación y gestión, reglamentado mediante el Decreto 2482 del 3 de diciembre de 2012.

Que el Decreto 943 del 21 de mayo de 2014 "Por el cual se actualiza el Modelo Estándar de Control Interno para el Estado Colombiano MECI", en su artículo 2° señala que el establecimiento y desarrollo del Sistema de Control Interno en los organismos y entidades públicas a que hace referencia el artículo 5 de la Ley 87 de 1993, será responsabilidad de la máxima de las entidades y organismos, así como de los demás funcionarios de la respectiva Entidad;

Que dentro de la estructura del Modelo Estándar de Control Interno MECI 2014, existe un Módulo de Planeación y Gestión, y dentro de este un Componente de Administración del Riesgo, el cual a su vez se encuentra integrado por los siguientes Elementos de Control: Políticas de Administración de Riesgos, Identificación de Riesgos y Análisis y Valoración de Riesgos.

Que los controles sobre los riesgos pueden establecerse con base en la identificación, análisis, valoración y tratamiento de los riesgos.

Que la Corporación Autónoma Regional del Guavio – CORPOGUAVIO, mediante Resolución Numero 850 del 23 de diciembre de 2014, actualiza y adopta el Sistema Integrado de Gestión y Control SIGYCO y se dictan otras disposiciones.

Que la Corporación Autónoma Regional del Guavio – CORPOGUAVIO, mediante Resolución Número 850 del 23 de diciembre de 2014, adopta y reglamenta la Política de Administración de Riesgos en la Corporación Autónoma Regional del Guavio – CORPOGUAVIO con base en lo establecido en el Sistema Integrado de Gestión y Control - SIGYCO y se dictan otras disposiciones.

El Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones presentan la "Guía para la Administración del Riesgo de Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas", incluidos sus anexos, como una herramienta con enfoque preventivo, vanguardista y proactivo que permitirá el manejo del riesgo y corrupción, así como el control en todos los niveles de la entidad pública, brindando seguridad razonable frente al logro de sus objetivos.

Que la Guía Metodológica para la Administración del Riesgo antes referenciada, requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su



gestión en la Corporación, el conocimiento de la misma desde de un punto de vista estratégico, de la aplicación de los tres (3) pasos básicos que esta determina para su desarrollo y de la definición e implementación de estrategias de comunicación transversales a toda la Corporación para que su efectividad pueda ser evidenciada.

Para la formulación de la Política se contó con la participación de todos los procesos involucrado en el actuar de la Corporación, y con los lineamientos de carácter técnico establecidos por el Departamento Administrativo de la Gestión Pública –DAFP–, tales como la “Guía de Administración del Riesgo”, “Guía para la Gestión de Riesgo de Corrupción” y “Estrategias para la construcción del Plan Anticorrupción y Atención al Ciudadano”

Por lo que es necesario establecer, documentar, aplicar y adoptar las Metodologías y los Instrumentos Técnicos necesarios para la Administración de Riesgos de gestión, de corrupción y seguridad digital por procesos en la Corporación.

El numeral 2.2.1 “Política de Planeación institucional” de la dimensión “Direccionamiento Estratégico y Planeación” menciona que, para responder a la pregunta ¿Cuáles son las prioridades identificadas por la entidad y señaladas en los planes de desarrollo nacionales y territoriales?, se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

De igual forma, se menciona en esta dimensión que, para llevar a cabo el ejercicio de planeación, la entidad debe documentar dicho ejercicio en donde se describa la parte conceptual u orientación estratégica; y la parte operativa en la que se señale de forma precisa los objetivos, las metas y resultados a lograr, las trayectorias de implantación o cursos de acción a seguir, cronogramas, responsables, indicadores para monitorear y evaluar su cumplimiento y los riesgos que pueden afectar tal cumplimiento y los controles para su mitigación.

Que conforme lo anterior, se hace necesario ajustar la Política de Administración del Riesgo, adoptar las metodologías expedidas por el Gobierno Nacional, el monitoreo y seguimiento a los riesgos de gestión, de corrupción y de Seguridad Digital.

RESUELVE

TITULO I

DE LA POLITICA DE ADMINISTRACION DE RIESGOS DE GESTION, DE CORRUPCION Y SEGURIDAD DIGITAL.

ARTÍCULO PRIMERO: MODIFICACION DE LA POLÍTICA. Modifíquese la Política de Administración de Riesgos de Gestión y de Corrupción por Política de Administración de Riesgos de Gestión, Corrupción y Seguridad Digital, para la Corporación Autónoma Regional del Guavio – CORPOGUAVIO, la cual deberán seguir todos y cada uno de los servidores públicos y colaboradores de la Entidad.



ARTÍCULO SEGUNDO: OBJETIVO DE LA POLÍTICA. El objetivo que se busca con la Política de Administración de Riesgos de Gestión, de Corrupción y de Seguridad Digital es proteger a la Corporación de las situaciones indeseables que impidan el cabal cumplimiento de su misión u objetivos institucionales, así como combatir la corrupción, además de esto incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en cada entidad pública.

ARTÍCULO TERCERO: DE LA POLÍTICA: Es obligación de cada uno de los servidores públicos y Contratistas de la Corporación Autónoma Regional del Guavio – CORPOGUAVIO; observar la Administración de Riesgos de Gestión, de Corrupción y de Seguridad Digital previo el conocimiento de las siguientes directrices:

1. Los Riesgos de Gestión, de Corrupción y de Seguridad Digital deben preverse antes de la ejecución de las acciones y son inherentes al ejercicio de planeación.
2. Los Riesgos de Gestión, de Corrupción y de Seguridad Digital se manejarán y administrarán por proceso.
3. En el manejo de los Riesgos de Gestión, de Corrupción y de Seguridad Digital por proceso, deben prevalecer las acciones preventivas antes que las correctivas.
4. Para la implementación de una acción o mecanismo de control para prevenir o mitigar un Riesgos de Gestión, de Corrupción y de Seguridad Digital por proceso debe analizarse la relación costo - beneficio, de tal manera que no sea más costoso el mecanismo de control que el costo del impacto del siniestro.
5. La Administración de Riesgos de Gestión, de Corrupción y de Seguridad Digital por Proceso debe estar implícita en el Modelo Integrado de Gestión y Control MIPG.
6. El manejo adecuado de la Administración de Riesgos de Gestión, de Corrupción y de Seguridad Digital por Proceso de cada una de las dependencias de la Corporación Autónoma Regional del Guavio – CORPOGUAVIO será responsabilidad de cada uno de los jefes de las mismas, el manejo inadecuado de la administración de riesgos se considera un acto de negligencia y se sanciona conforme a la Ley 734 del 2002.
7. Los mecanismos de control interno, deben estar orientados a eliminar o mitigar los Riesgos de Gestión, de Corrupción y de Seguridad Digital por proceso y estos deben estar intrínsecos en los procedimientos conforme lo establece la Ley 87 de 1993, y estos mecanismos deben revisarse y evaluarse en cada ciclo de mejora del Modelo integrado de Gestión y Control MIPG.
8. En la fase diagnóstica de la formulación del Plan Estratégico Institucional, se deben identificar los Riesgos de Gestión, de Corrupción y de Seguridad Digital de cada proyecto que afecten el cumplimiento de los objetivos institucionales, y las acciones que se proyecten deben estar orientadas a eliminarlos, mitigarlos o prevenirlos.



ARTÍCULO CUARTO: RIESGOS DE SEGURIDAD DIGITAL

La información que hace parte de una Entidad Pública es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Entidad, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad o de un Estado.

Los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo o un grupo de activos dentro del proceso:

Integridad, confidencialidad o disponibilidad.

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

los riesgos de seguridad digital, se deben generar indicadores, para medir la gestión realizada, en esencia la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad debería definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

1. indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.
2. indicador de efectividad, para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

TITULO II DE LA METODOLOGIA PARA ADMINISTRAR LOS RIESGOS

ARTÍCULO QUINTO: TERMINOS Y DEFINICIONES

- **Causas:** Son los medios, circunstancias y agentes generadores del riesgo.
- **Compartir el Riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, procesos, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.



- **Consecuencias:** El resultado real o potencial sea este una pérdida, perjuicio, desventaja o ganancia, frente a la consecución de los objetivos del proceso o de la entidad.
- **Contexto Externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos que puede ser: ambiente cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, nacional, regional o local.
- **Contexto Interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos, el cual puede ser: gobierno, estructura organizacional, funciones, responsabilidades, políticas, normas, directrices adoptadas por la organización, objetivos, estrategias implementadas, recursos (capital, tiempo, personas, procesos, sistemas, tecnologías).
- **Contexto Estratégico:** Insumo básico para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones internas y externas de la institución.
- **Control:** Acciones establecidas para disminuir la probabilidad de ocurrencia del riesgo, el impacto de los riesgos y/o asegurar la continuidad del servicio en caso de llegarse a materializar el riesgo.
- **Controles Correctivos:** Aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.
- **Controles Preventivos:** Aquellos que actúan para eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.
- **Evaluación del Riesgo:** Proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
- **Evento:** Incidente o situación potencial que puede ocurrir en un lugar determinado durante un periodo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie de causas.
- **Evitar el Riesgo:** Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
- **Frecuencia:** Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo y proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.



- **Impacto:** Consecuencias que puede ocasionar a la entidad la materialización del riesgo.
- **Mapa de Riesgos:** Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias y sus acciones preventivas.
- **Monitorear:** Comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.
- **Plan de Manejo del Riesgo:** Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.
- **Política de Riesgos:** Intención global u orientación de una entidad frente a la gestión del riesgo.
- **Probabilidad:** Grado en el cual es probable que ocurra un evento, que se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir.
- **Riesgo de Corrupción:** La posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo Inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo Residual:** nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.
- **Riesgo:** Es el resultado de la combinación entre la probabilidad de ocurrencia de un evento y sus posibles consecuencias que tendrán un impacto mayor o menor sobre la capacidad de lograr los objetivos.
- **Valoración del Riesgo:** Elemento de Control, que determina el nivel o grado de exposición de la entidad pública al impacto del riesgo, permitiendo estimar las prioridades para su tratamiento según El Decreto 1599 de 2005.

ARTÍCULO SEXTO: METODOLOGÍA: Riesgos de Gestión, de Corrupción y de Seguridad Digital de la Corporación Autónoma Regional del Guavio – CORPOGUAVIO, identificados en los Mapas de Riesgos de cada Proceso del Modelo de Operación, se adoptan las metodologías expedidas por el Gobierno Nacional a través del Departamento Administrativo de la Función Pública DAFP (Riesgos de Gestión) y de la Secretaría de Transparencia del Departamento Administrativo de la Presidencia de la República DAPRE (Riesgos de Corrupción), Ministerio de Tecnologías de la Información y Comunicaciones Riesgos de Seguridad Digital, las cuales forman parte integral de la presente Resolución, que incluyen los siguientes pasos:

Paso 1: Política de Administración del Riesgo



ACTO ADMINISTRATIVO No

725 25 JUL. 2019

La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos

Paso 2: Identificación del Riesgo.

Le corresponde a la Segunda Línea de Defensa, el análisis de los objetivos de la entidad tanto del orden estratégico como de procesos.

-Identificación de activos de seguridad de la información

Le corresponde a la primera línea de defensa, realizar la identificación de activos en cada proceso.

- Identificación de riesgos -técnicas para la identificación de riesgos.

Paso 3: Valoración del Riesgo.

Comunicación y Consulta (Aspecto Transversal)

ARTÍCULO SEPTIMO: PASO UNO. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO:

Es la declaración de la Dirección y las intenciones generales de la Corporación con respecto a la gestión del riesgo. La Gestión o Administración del Riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos y es determinada por la Alta Dirección de la Corporación (Comité Directivo).

ARTÍCULO OCTAVO: PASO DOS. IDENTIFICACIÓN DEL RIESGO: En este paso se establecen las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

Establecimiento del Contexto: Se debe establecer el Contexto Externo e Interno de la Corporación y el Contexto del Proceso. Es posible hacer uso de Herramientas y Técnicas.

Identificación del Riesgo: La identificación del riesgo se realiza determinado las CAUSAS, con base en el contexto interno, externo y del proceso ya analizado para la Corporación, y que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la Corporación se podrán evidenciar en el análisis de contexto correspondiente, para ser tenidas en cuenta para el análisis y valoración del riesgo.

Aceptación del Riesgo: Si el nivel del riesgo cumple con los criterios de aceptación de riesgo es necesario poner controles y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.

Compartir el Riesgo: Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad de riesgo.

ARTÍCULO NOVENO: TRES PASOS . VALORACIÓN DEL RIESGO:

- **Análisis del Riesgo:** Se busca establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).



- **Valoración del Riesgo:** Se busca Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).
- **Evaluación de Riesgos:** Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

Elaboración del Mapa de Riesgos: El mapa de riesgos es una representación final de la probabilidad e impacto de uno o mas riesgos frente a un proceso, proyecto o programa. Como productos finales se obtienen:

- **Mapa de Riesgos Institucional:** Contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la Corporación, se alimenta con los riesgos residuales Altos o Externos de cada uno de los procesos, los cuales pueden afectar el cumplimiento de la misión institucional y objetivos de la Corporación. En este mapa se deberán incluir los riesgos identificados como posibles actos de corrupción, en cumplimiento del artículo 73 de la Ley 1474 de 2011.
- **Mapa de Riesgos por Proceso:** Recoge los riesgos identificados para cada uno de los procesos, los cuales pueden afectar el logro de sus objetivos.

Monitoreo y Revisión: Debe asegurar que las acciones establecidas en los mapas se están llevando a cabo y evaluar la eficiencia de su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que puedan estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe estar a cargo de:

Los responsables de los procesos: En cargados de realizar las acciones asociadas a los controles establecidos para cada uno de los riesgos identificados para su proceso.

La Oficina de Control Interno: Encargada de realizar el seguimiento a los riesgos que a nivel institucional han sido consolidados, es importante mencionar que se deben tener en cuenta las fechas establecidas por la Guía de la Secretaria de Transparencia denominada (Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano) para el seguimiento a los riesgos sobre posibles actos de corrupción. Así mismo en sus procesos de auditoría interna debe analizar el diseño e idoneidad de los controles determinando si son o no adecuados para prevenir o mitigar los riesgos en los procesos.

La Oficina de Control Interno dentro de su función asesora debe comunicar y presentar luego del seguimiento y evaluación sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

El monitoreo es esencial para garantizar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.



Una vez diseñados y validados los Planes para Administrar los Riesgos en los Mapas de Riesgos de Gestión de cada Proceso y los Mapas de Riesgos de Corrupción de cada Proceso, es necesario monitorearlos teniendo en cuenta que estos nunca dejan de representar una amenaza para la Corporación.

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe estar a cargo de los Líderes de los Procesos, la Subdirección de Planeación y la Oficina de Control Interno o quien haga sus veces, quienes deberán reportar cada cuatro (4) meses el resultado de dicha actividad, con corte a 30 de abril, 31 de agosto y 31 de diciembre de cada vigencia fiscal.

La finalidad principal del seguimiento y monitoreo a los mapas de riesgos de gestión y de corrupción y planes de manejo de los mismos que realiza cada cuatro (4) meses la Oficina de Control Interno, Asesor, Coordinador, Auditor Interno o quien haga sus veces, será la de seguir los correctivos y ajustes necesarios para asegurar un efectivo manejo de los riesgos tanto de gestión como de corrupción por proceso.

El Jefe de la Oficina de Control Interno, Asesor, Coordinador, Auditor Interno o quien haga sus veces, dentro de su función asesora comunicará y presentará luego del seguimiento y monitoreo, sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

LA OFICINA DE CONTROL INTERNO REALIZARÁ SEGUIMIENTO A LOS RIESGOS DE GESTIÓN, A LOS RIESGOS DE CORRUPCIÓN Y DE SEGURIDAD DIGITAL DE CADA PROCESO DEL MODELO DE OPERACIÓN TRES (3) VECES AL AÑO ASÍ:

Primer Seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.

Segundo Seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre.

Tercer Seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

ARTÍCULO DECIMO: COMUNICACIÓN Y CONSULTA (Aspecto Transversal): La comunicación y consulta con las partes involucradas tanto internas como externas debe tener lugar durante todas las etapas del proceso para la gestión del riesgo.

Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios.

Así mismo es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

**TITULO III
DE LOS ROLES EN LA ADMINISTRACIÓN DE RIESGOS**



ARTÍCULO DECIMO PRIMERO: Para adelantar este proceso se considerará importante señalar los roles de los diferentes actores, así:

Compromiso de la Alta y Media Dirección: Para el éxito en la Implementación de una adecuada Administración del Riesgo tanto de Gestión, Corrupción y de seguridad Digital de cada Proceso, es indispensable el compromiso de la Alta Gerencia como encargada, en primera instancia, de estimular la cultura de la identificación y prevención del riesgo y en segunda instancia de definir las políticas. Para lograrlo es importante la definición de canales directos de comunicación y el apoyo a todas las acciones emprendidas en este sentido, propiciando los espacios y asignando los recursos necesarios.

Roles y Responsabilidades del Representante de la Dirección con relación a la Administración del Riesgo:

1. Formular, orientar, dirigir y coordinar el proyecto de diseño e implementación del Componente de la Administración del Riesgo tanto de Gestión, de Corrupción y de Seguridad Digital de cada Proceso.
2. Asegurar que se desarrollen a cabalidad cada una de las etapas previstas para el diseño e implementación del Componente de Administración del Riesgo tanto de Gestión, de Corrupción y de Seguridad Digital de cada Proceso.
3. Informar a la Alta Dirección sobre la planificación y avances del proyecto de diseño e implementación del Componente de la Administración del Riesgo tanto de Gestión, de Corrupción y de Seguridad Digital de cada Proceso.
4. Dirigir y coordinar las actividades del Equipo SIGYCO relacionadas con la Administración de Riesgos tanto de Gestión, de Corrupción y de Seguridad Digital de cada Proceso.
5. Coordinar con los directivos o responsables de cada área o procesos las actividades que requiere realizar el Equipo SIGYCO en armonía y colaboración con los servidores de dichas áreas, relacionadas con la Administración de Gestión, de Corrupción y de Seguridad Digital de cada Proceso.
6. Hacer seguimiento a las actividades planeadas para el diseño e implementación del Componente de Administración del Gestión, de Corrupción y de Seguridad Digital de cada Proceso, aplicando correctivos donde se requiera.
7. Someter a consideración del Comité de Coordinación del Sistema de Control Interno las propuestas de diseño e implementación del Componente de la Administración del Riesgo tanto de Gestión, de Corrupción y de Seguridad Digital de cada Proceso, para su aprobación.

Roles y Responsabilidades de los Jefes de las Dependencias o Líderes de Proceso:

1. Asegurarse que se desarrollen cada una de los pasos de la política de administración del riesgo de Gestión de Corrupción y de Seguridad Digital de cada Proceso establecidos en la presente resolución.



2. Asegurar la completa articulación de los riesgos identificados tanto de Gestión como de Corrupción de cada Proceso, con el Sistema Integrado de Planeación Gestión MIPG y con los Planes Operativos por Dependencia.
3. Revisar en cada ciclo de mejora los riesgos tanto Gestión, de Corrupción y de Seguridad Digital de cada Proceso, realizar los ajustes pertinentes y adelantar las acciones de mejora que se deriven de dicha revisión

Roles y Responsabilidades del Equipo SIGYCO

El Equipo SIGYCO, cumplirá los siguientes roles y responsabilidades:

1. Adelantar el proceso de diseño e implementación del Componente de Administración del Riesgo Gestión, de Corrupción y de Seguridad Digital de cada Proceso, bajo las orientaciones del Representante de la Dirección.
2. Capacitar a los servidores de la Corporación en el Modelo y el Componente de Administración del Riesgo tanto de Gestión, de Corrupción y de Seguridad Digital de cada Proceso.
3. Asesorar a las áreas de la Corporación en el diseño e implementación del Componente de Administración del Gestión, de Corrupción y de Seguridad Digital de cada Proceso.
4. Revisar, analizar y consolidar la información para presentar propuestas de diseño e implementación del Componente de Administración del Riesgo de Gestión, de Corrupción y de Seguridad Digital de cada Proceso al Representante de la Dirección, para su aplicación.
5. Trabajar en coordinación con los servidores designados por área en aquellas actividades requeridas para el diseño e implementación del Componente de Administración del Riesgo de Gestión, de Corrupción y de Seguridad Digital de cada Proceso.

Roles y Responsabilidades del Jefe de la Oficina de Control Interno, Asesor, Coordinador, Auditor Interno o quien haga sus veces, los cuales son de dos clases, directas o indirectas.

Rol Directo: Asesorar el proceso de identificación de los riesgos institucionales tanto de Riesgo de Gestión, de Corrupción y de Seguridad Digital de cada Proceso y con base en ellos, realizar recomendaciones preventivas y/o correctivas con los responsables de los procesos. Igualmente, el Jefe de la Oficina de Control Interno, Asesor, Coordinador, Auditor Interno o quien haga sus veces, debe hacer seguimiento a la evolución de los riesgos tanto de Gestión como de Corrupción de cada Proceso y al cumplimiento de las acciones propuestas, con el fin de verificar el cumplimiento de las mismas y proponer mejoras.

Para cumplir el rol de Valoración del Riesgo, las Oficinas de Control Interno como agentes dinamizadores del Sistema de Control Interno, ejercen un doble rol, por un lado deben realizar el seguimiento y monitoreo de los mapas de riesgos, mediante la aplicación técnicas de auditoría que permitan establecer la idoneidad de los controles establecidos



para los riesgos identificados, determinando si son o no efectivos para evitar la materialización de los mismos; por otro lado en desarrollo de su rol de asesoría y acompañamiento deben crear espacios donde sea posible generar acciones de mejora a partir de la experiencia de los funcionarios en la gestión de los riesgos identificados a los procesos, los cuales, dependiendo del entorno y de la misma complejidad de la entidad, pueden cambiar o requerir acciones adicionales para mejorar la efectividad de los controles. En algunos casos dependiendo del grado de madurez del proceso de administración del riesgo de la entidad, dicha oficina debe prestar asesoría y acompañamiento técnico, específicamente desde el conocimiento de la metodología para la elaboración de los mapas de riesgos.

Frente al rol de Asesoría y Acompañamiento, éste tiene como objetivo principal promover el mejoramiento continuo de los procesos de la entidad, ayudando a la Alta Dirección, en la búsqueda del cumplimiento de los objetivos institucionales, por lo que este rol consiste principalmente en la orientación técnica y recomendaciones orientadas a:

- Facilitar grupos de mejoras de procesos;
- Facilitar grupos de trabajo para la identificación, análisis y valoración de riesgos;
- Evaluar los productos y servicios ofrecidos por la entidad;
- Evitar desviaciones en los planes, procesos, actividades y tareas;
- Promover la mejora de los procesos y la eficacia de las operaciones;
- Evaluar a través de la auditoría los riesgos identificados y la administración de los mismos;
- Fortalecer el Control Interno en general, principalmente en los procesos críticos;
- Incrementar la calidad y veracidad de la información;
- Identificar fuentes de recuperación y ahorro;
- Fomentar la cultura del control.

ARTÍCULO DÉCIMO SEGUNDO: La Metodología para la Administración de Riesgos tanto de Gestión como de Corrupción de cada Proceso elaborada, validada, socializada y aplicada a partir de la firma de la presente resolución, así como los mapas de riesgos de gestión y de corrupción que se ajusten a los planes de manejo de los mismos, quedan adoptados con el presente acto administrativo y forman parte integral del mismo. Cualquier ajuste o modificación tanto a la metodología como a los mapas de riesgos, se entiende que estará regulado por las disposiciones de la presente resolución.

ARTÍCULO DÉCIMO TERCERO: La política de administración del riesgo será de obligatorio cumplimiento en cada dependencia y será orientada por la Subdirección de Planeación y evaluada por la Oficina de Control Interno y deberá incluirse dentro de los planes operativos de las dependencias como un compromiso institucional y estratégico.

ARTÍCULO DÉCIMO CUARTO. VIGENCIAS: Esta Resolución deroga en su integralidad la Resolución 051 del 02 de febrero de 2017 "Por medio de la cual se adopta y reglamenta



Corporación Autónoma Regional del Guavio - **CORPOGUAVIO**



ACTO ADMINISTRATIVO No **725** ... **25 JUL. 2019**

la política de administración del riesgo en la Corporación Autónoma Regional del Guavio – “CORPOGUAVIO” con base en lo establecido en el Sistema Integrado de Gestión y Control SIGYCO y se dictan otras disposiciones”.

ARTÍCULO DÉCIMO QUINTO: Esta resolución rige a partir de la fecha de su expedición

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

OSWALDO JIMÉNEZ DÍAZ
Director General

Proyectó: Jefferson Fabian Novoa Usaquén/ Contratista 
Revisó: Diego Leandro Cárdenas Chala /Subdirector de Planeación 
Aprobó: Cesar Augusto Acevedo Silva / Secretario General