COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Política de Administración de Riesgos 2020

Coordinación Ejecutiva
Coordinador: Zoila Vargas Mesa.
Líder: Yamile Mateus.

Mayo de 2020

www.crcom.gov.co
@CRCCol /CRCCol /CRCCol CRCCOL

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

1. Introducción

Para la COMISIÓN DE REGULACIÓN DE COMUNICACIONES – CRC, la administración de riesgos es una herramienta gerencial fundamental para asegurar el cumplimiento de su misión institucional y el desarrollo de sus actividades mediante el cumplimiento de los objetivos trazados dentro del Plan Estratégico, alineado con el Sistema Integral de Gestión.

Teniendo en cuenta que los riesgos son posibilidades de ocurrencia de toda situación que pueda desviar el normal desarrollo de las actividades de los procesos y que dichas desviaciones pueden impedir el logro de los objetivos estratégicos para el cumplimiento de la misión institucional, la CRC se ha fortalecido, a partir del Modelo Integrado de Planeación y Gestión – MIPG en su dimensión de Direccionamiento Estratégico y Planeación, y en particular, la política de Planeación Institucional a través del análisis y estructuración de los elementos de control definidos en el Sistema Integral de Gestión.

Para dar continuidad a las políticas de administración de riesgos, se hace necesario definir criterios orientadores respecto al tratamiento de estos, a fin de mitigar sus efectos en la Entidad, siendo éste, el objetivo de la presente política, con la cual se pretende en primera instancia, transmitir la visión de la Alta Dirección sobre la manera de abordar la administración de los riesgos institucionales, socializar con todos los funcionarios un lenguaje común sobre el tema y por último, difundir los lineamientos que permitan la sostenibilidad de la administración del riesgo.

El presente documento comprende la definición de la política y lineamientos institucionales a emprender, lo que sin duda permitirá dirigir el accionar de la CRC hacia el uso eficiente de los recursos y la continuidad en la prestación de los servicios con calidad.

La Política de Administración de Riesgos de la CRC está alineada con los criterios que establece la Guía para la administración del riesgo y el diseño de controles en entidades públicas, expedida por el Departamento Administrativo de la Función Pública en octubre de 2018, la cual da lineamientos para los riesgos de gestión, corrupción y seguridad digital.

Con la presente Política la CRC deja documentada la gestión de los riesgos, junto con la descripción conceptual, orientación estratégica y el desarrollo operativo, con el fin de lograr el cumplimiento de los objetivos.

<u>Elementos conceptuales que deben ser aplicados en la Entidad.</u>

La CRC cuenta con códigos de Buen Gobierno, Ética e Integridad, instrumentos mediante los cuales se definen las reglas de comportamiento que deben gobernar la conducta de los funcionarios de la entidad, y que se convierten en guía del ejercicio de la función administrativa que compete. Se busca que los funcionarios de la entidad interioricen estos códigos como parte inherente al desarrollo cotidiano de sus labores con el fin de prestar el mejor servicio, actuar con transparencia, hacer el mejor uso de los recursos y contribuir a la consolidación de la imagen y el posicionamiento institucional.

Propósito de la Dirección con esta política

Mediante una adecuada administración de los riesgos, la Alta Dirección pretende alcanzar los mejores niveles de conocimiento respecto a la gestión de estos en la entidad, elevar la productividad y garantizar la eficiencia y la eficacia de los procesos organizacionales.

2. Definiciones

- **Aceptación del riesgo**: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
- **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.
- **Administración de riesgos**: Conjunto de elementos de control que, al interrelacionarse, permiten a la entidad evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar con sus diferentes elementos le permite a la entidad pública, autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.
- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis de riesgo:** Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.
- **Apetito al riesgo:** Magnitud y tipo de riesgo que la entidad está dispuesta a buscar o retener.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Compartir el riesgo:** Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.
- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Son 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 modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **Control detectivo:** Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.
- **Control preventivo**: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Factores de riesgo:** Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgos o tienden a aumentar la exposición, pueden ser internos o externos de la entidad.
- **Gestión del riesgo**: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Identificación del riesgo:** elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** propiedad de exactitud y completitud.
- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.
- **Nivel de aceptación del riesgo**: son los criterios de aceptación de riesgos establecidos que se emplean durante la etapa de evaluación de riesgos.
- **Plan Anticorrupción y de Atención al Ciudadano:** plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Riesgo:** es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.
- **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.
- **Riesgos de cumplimiento:** posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales**.**
- **Riesgo de gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
- **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgos estratégicos:** posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

- **Riesgos gerenciales:** posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
- **Riesgos financieros:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgos tecnológicos:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- **Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
- **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Tratamiento del riesgo:** consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.
- **Valoración del riesgo:** Busca identificar y analizar los riesgos que enfrenta la entidad, tanto de fuentes internas como externas relevantes para la consecución de los objetivos, para administrarlos.
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

3. Marco Normativo

El riesgo y la administración de este se fundamentan en el siguiente marco normativo:

NORMA	DESCRIPCIÓN
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). *Artículo 2 Objetivos del control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.*
Ley 489 de 1998	Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno.

Decreto 2145 de 1999	Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art. 8º. de la ley 1474 de 2011)
Decreto 2593 del 2000	Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999.
Decreto 1537 de 2001	Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado. El parágrafo del Artículo 4º señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (…) y en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su Artículo 4º la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…).
Decreto 1599 de 2005	Por el cual se adopta el Modelo Estándar de Control Interno para el Estado colombiano y se presenta el anexo técnico del MECI 1000:2005. 1.3 Componentes de administración del riesgo.
Decreto 943 de 2014	Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
Decreto 4485 de 2009	Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g) "establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder". Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.
Ley 1474 de 2011	Estatuto Anticorrupción. Artículo 73. "Plan Anticorrupción y de Atención al Ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.
Decreto 4637 de 2011	Crea la Secretaría de Transparencia en el Departamento Administrativo de la Presidencia de la República, quien establece lineamientos para la prevención de la corrupción.
Decreto 1649 de 2014	Funciones de la Secretaría de Transparencia: 13) Señalar la metodología para diseñar y hacer seguimiento a las estrategias de lucha contra la corrupción y de atención al ciudadano que deberán elaborar anualmente las entidades del orden nacional y territorial.
Decreto 1081 de 2015	Señala como metodología para elaborar la estrategia de lucha contra la corrupción la contenida en el documento "Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano."

Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único. Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Con el cual se crea el Modelo Integrado de Planeación y Gestión – MIPG.
Guía para la Administración de Riesgo y el Diseño de controles en Entidades Públicas.	Por la cual se establece la metodología para la administración del riesgo de gestión, corrupción de seguridad digital, expedida por el Departamento Administrativo de la Función Pública.

4. Objetivos

4.1. Objetivo General

Establecer el marco general y la metodología para la administración de los riesgos en la Comisión de Regulación de Comunicaciones – CRC – mediante la ejecución de un proceso ordenado y continuo que contribuya al mejoramiento constante de las actividades y al cumplimiento de los objetivos de la Entidad.

4.2. Objetivos Específicos

- Formalizar al interior de la CRC una metodología para administrar los riesgos de toda naturaleza a los que se enfrenta la entidad, de gestión, de corrupción, de seguridad digital, entre otros.
- Establecer pautas para la identificación de los factores que representan amenazas u oportunidades para el cumplimiento de los objetivos.
- Fijar las escalas de valoración para la probabilidad de ocurrencia y el impacto de cada factor de riesgo identificado, a partir de las metodologías establecidas por la Función Pública.
- Estipular las reglas para la identificación de las actividades de control que minimicen la ocurrencia e impacto de los factores de riesgo.
- Establecer lineamientos específicos para la administración de los riesgos de gestión, corrupción y seguridad digital.
- Caracterizar el instrumento para la administración del riesgo (Mapa de riesgos).
- Cumplir con los principios del Modelo Integrado de Planeación y Gestión, Modelo Estándar de Control Interno y el Sistema integral de Gestión de la Entidad
- Establecer un mecanismo y periodicidad para la difusión y apropiación de la política de riesgos por parte de todo el equipo de la CRC.

5. Alineación con el Plan Estratégico

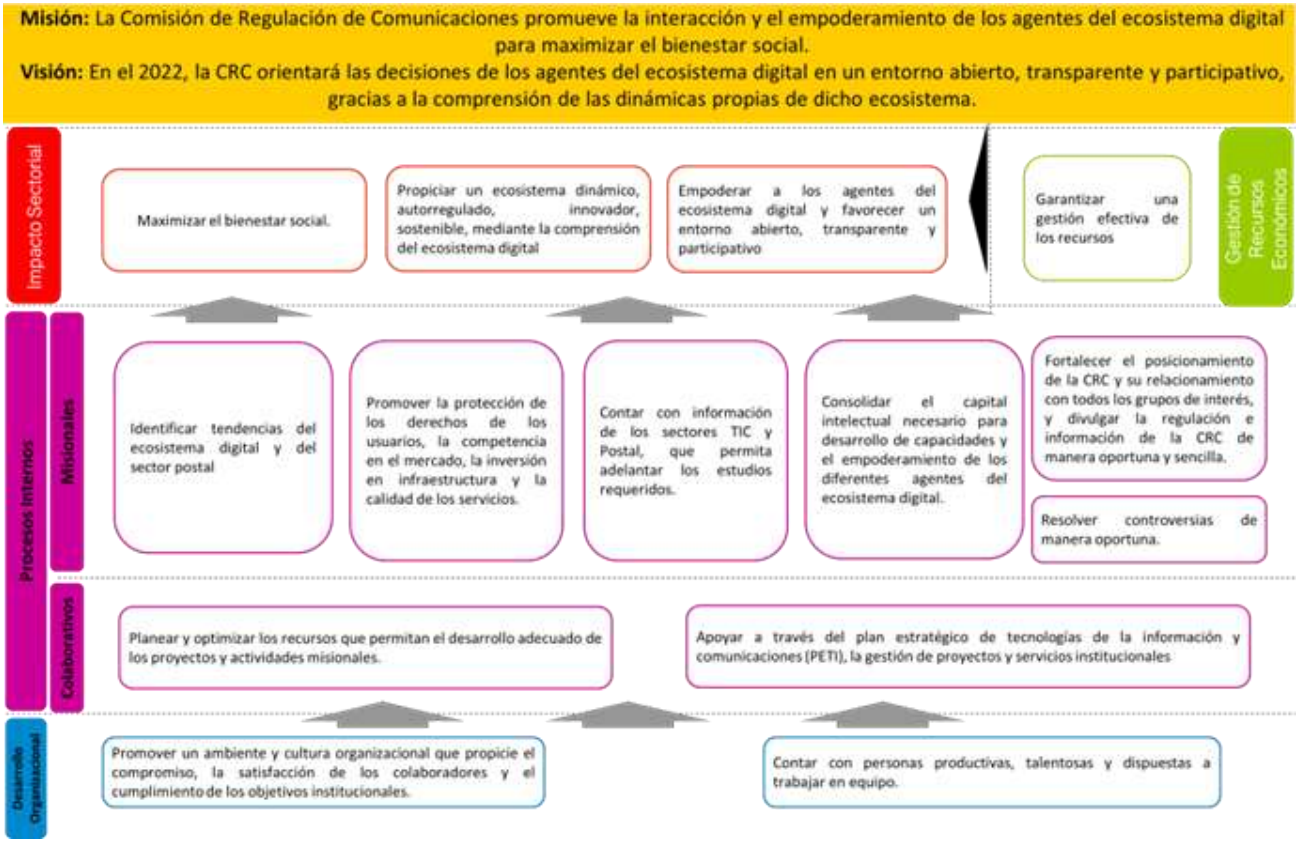
La CRC definió el siguiente Plan Estratégico para la vigencia 2018-2022:

Propósito Superior
Colombia, modelo de ecosistema Digital, dinámico, autorregulado, innovador y sostenible que maximiza el bienestar social.

Visión
En el 2022, la CRC orientará las decisiones de los agentes del ecosistema digital en un entorno abierto, transparente y participativo, gracias a la comprensión de las dinámicas propias de dicho ecosistema.

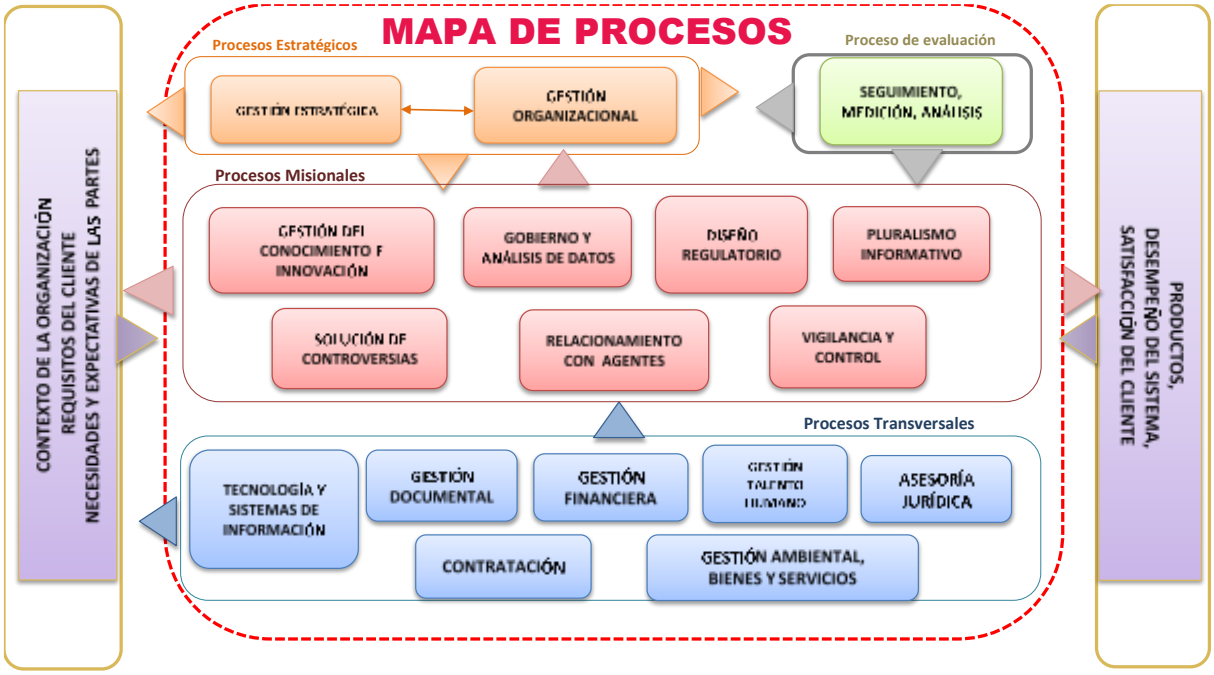
Misión
La Comisión de Regulación de Comunicaciones promueve la interacción y el empoderamiento de los agentes del ecosistema digital para maximizar el bienestar social.

Mapa Estratégico



Para la CRC, la administración de los riesgos es una herramienta de control fundamental para el cumplimiento de los objetivos estratégicos y de los procesos internos. Es por esto que, la presente política se encuentra armonizada con la misión y visión organizacional, así como con el Sistema Integral de Gestión.

Mapa de procesos de la CRC:



Se identifican riesgos de gestión para cada uno de los procesos establecidos para el Sistema Integral de Gestión de la CRC, de esta manera se asegura la alineación de los riesgos con el direccionamiento estratégico de la Entidad.

A través de los informes trimestrales de desempeño, la Dirección Ejecutiva valida el seguimiento de los diferentes riesgos, las actividades para su mitigación, la identificación de los factores internos o externos a la entidad que pueden generar riesgos que afecten el cumplimiento de los objetivos; así mismo, a través del Plan Anticorrupción y de Atención al Ciudadano y el Plan de Acción, se realizan seguimientos orientados al fortalecimiento de la presente política.

6. Alcance de la Política.

La política de riesgos es aplicable a todos los procesos y proyectos de la Entidad y a todas las actividades realizadas por los funcionarios durante el ejercicio de sus funciones. La CRC mantiene los canales de información apropiados para garantizar un adecuado conocimiento y gestión de los riesgos.

Es de aclarar que, para los riesgos de seguridad digital, se deben seguir los criterios definidos en el Modelo de Seguridad y Privacidad de la información. Estos riesgos tienen que estar alineados con el anexo 4 "Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas-Guía riesgos 2018". Dicho documento se puede consultar en el siguiente link: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-

/document_library/bGsp2IjUBdeu/view_file/34316352?_com_liferay_document_library_web_portlet_DLPortlet_INSTANCE_bGsp2IjUBdeu_redirect=https%3A%2F%2Fwww.funcionpublica.gov.co%2Fweb%2Feva%2Fbiblioteca-virtual%2F-%2Fdocument_library%2FbGsp2IjUBdeu%2Fview%2F34316316

7. Contexto

Para la identificación de los riesgos que pueden afectar los diferentes procesos de la entidad, se contemplan los siguientes factores para cada categoría:

7.1. Contexto externo

- Económicos: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
- Políticos: Cambios de gobierno, legislación, políticas públicas, regulación.
- Sociales: Demografía, responsabilidad social, orden público.
- Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
- Medioambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible, cambio climático.
- Legal: Decretos, Leyes, Ordenanzas y Acuerdos.

7.2. Contexto Interno

- Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
- Personal: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
- Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
- Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
- Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
- Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

7.3. Contexto del proceso

- Diseño del Proceso: Claridad en la descripción del alcance y objetivo del proceso.
- Interacciones con otros procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
- Procedimientos Asociados: Pertinencia en los procedimientos que desarrollan los procesos.

- Responsables Del Proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- Comunicación entre los procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.
- Activos de Seguridad Digital: Información, aplicaciones que se deben proteger para garantizar el funcionamiento interno de cada proceso y para el ciudadano.

A partir de lo establecido por el Departamento Administrativo de la Función Pública, en su Guía para la Administración del Riesgo, en las caracterizaciones de cada uno de los procesos de la entidad se encuentra la información relacionada con el contexto, igualmente, de manera trimestral, se realizan Reuniones de Análisis Estratégico en cada uno de los procesos, en los cuales, entre otros, se realiza un seguimiento al estado de los riesgos y se reporta, en caso de ser requerido, los ajustes o modificaciones a que haya lugar.

8. Identificación de Riesgos:

Para la identificación de los riesgos, cada grupo de trabajo realiza reuniones con diferentes funcionarios para la identificación de los aspectos de contexto externo e interno, causas, efectos, factores que se deben tener en cuenta para realizar el análisis y la valoración de los riesgos.

Al iniciar el proceso de identificación de riesgos se debe enfocar en el objetivo de cada uno de los procesos de la Entidad.

9. Análisis y calificación de los Riesgos

9.1. Análisis de la Probabilidad

La probabilidad es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos de la entidad, pudiendo entorpecer el desarrollo de sus funciones. La forma de medir su probabilidad y ocurrencia para los distintos tipos de riesgos (gestión, corrupción y seguridad digital), es la siguiente:

Probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años.
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años.

4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

9.2. Análisis de Impacto

Por impacto se entienden las consecuencias que puede ocasionar a la entidad la materialización del riesgo. De acuerdo con el tipo de riesgo, el impacto se calcula de manera diferente, así:

Criterios para calificar el impacto para riesgos de gestión

NIVEL	IMPACTO	CONSECUENCIAS CUANTITATIVAS	CONSECUENCIAS CUALITATIVAS
1	Insignificante	• 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 económicas o administrativas. • No se afecta la imagen institucional de forma significativa
2	Menor	• 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%	• 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.
3	Moderado	• 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	• Interrupción de las operaciones de la Entidad por un 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.

		ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad	• 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
4	Mayor	• 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 Comisión	• Interrupción de las operaciones de la Entidad por más de dos (2) días. • Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. • Sanción por parte del ente de control u otro 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 del servicio a los usuarios o • ciudadanos.
5	Catastrófico	• 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% • 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	• 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 presupuestal. • Imagen institucional afectada en el orden • nacional o regional por actos o hechos de corrupción comprobados.

Criterios para calificar el impacto para riesgos de seguridad digital

NIVEL	IMPACTO	CONSECUENCIAS CUANTITATIVAS	CONSECUENCIAS CUALITATIVAS
1	Insignificante	• Afectación ≥1% de la población. • Afectación ≥0,5% del presupuesto anual de la entidad.	• Sin afectación de la integridad. • Sin afectación de la disponibilidad. • Sin afectación de la confidencialidad.
2	Menor	• Afectación ≥5% de la población. • Afectación ≥1% del presupuesto anual de la entidad.	• Afectación leve de la integridad. • Afectación leve de la disponibilidad. • Afectación leve de la confidencialidad.

3	Moderado	• Afectación ≥10% de la población. • Afectación ≥5% del presupuesto anual de la entidad.	• Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
4	Mayor	• Afectación ≥20% de la población. • Afectación ≥20% del presupuesto anual de la entidad.	• Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
5	Catastrófico	• Afectación ≥50% de la población. • Afectación ≥50% del presupuesto anual de la entidad.	• Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Criterios para calificar el impacto para riesgos de corrupción

Para calificar el impacto de los riesgos de corrupción, se debe dar respuesta a las siguientes preguntas:

Pregunta. Si el riesgo de corrupción se materializa, podría…	**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?		
¿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?		

La calificación de impacto de riesgos de corrupción se realiza de la siguiente manera:

Nivel	Calificación	Consecuencia
MODERADO	Responder afirmativamente de UNA a CINCO preguntas generan un impacto moderado.	Genera medianas consecuencias sobre la entidad
MAYOR	Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.	Genera altas consecuencias sobre la entidad.
CATASTRÓFICO	Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.	Genera consecuencias desastrosas para la entidad

Evaluación de los riesgos de Gestión.

Se ejecuta al realizar la valoración de cada uno de los controles identificados para cada riesgo. Es de aclarar que cada causa debe tener un control. La valoración debe incluir los criterios de:

a. **Diseño del Control**[1]: aquí se establece cómo se definió el control para que mitigue el riesgo de manera adecuada. Se evalúa con seis variables:
   - Definición del responsable de ejecutar el control.
   - Periodicidad de ejecución del control.
   - Propósito del control.
   - Cómo se realiza la actividad.
   - Identificación de desviaciones y qué se hace con dichas desviaciones.
   - Evidencia de la Ejecución del control.

[1] Se realiza la valoración con las variables definidas en la Tabla 7 de la Guía de Administración del Riesgo y el diseño de Controles para Entidades Públicas. Versión 4. Página 61.

b. **Solidez del Control:** la solidez individual de los controles se da frente a los siguientes criterios: Fuerte, Moderado y Débil, de acuerdo con los criterios de la guía establecidos en la tabla de la página 63. Luego se saca la solidez de los controles en conjunto para cada riesgo, sacando un promedio simple, teniendo en cuenta que Fuerte (100), Moderado (50) y Débil (0).

10. Niveles de tratamiento de los riesgos y mapa de calor

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: significa que no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. En la CRC cuando se acepta un riesgo se ejecutan las actividades propias del proceso, así como los controles establecidos. No obstante, si el riesgo corresponde a un proceso estratégico, misional, tecnológico o su impacto afecta la prestación del servicio, se debe incluir en el mapa de riesgos institucional. Se hace seguimiento trimestral a través de los informes de gestión de los procesos. En la CRC ningún riesgo de corrupción puede tener como tratamiento, el aceptar el riesgo.

Reducir el riesgo: se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos. Por lo general conlleva a la implementación de controles. Se hace seguimiento trimestral a través de los informes de gestión de los procesos. En la CRC ningún riesgo de corrupción puede tener como tratamiento, el reducir el riesgo.

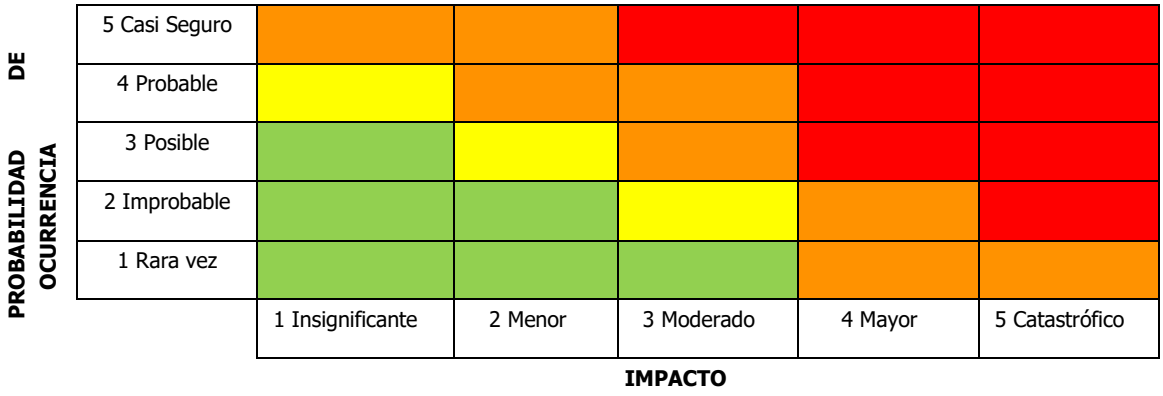
Evitar el riesgo: se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que lo provoca. Se hace seguimiento trimestral a través de los informes de gestión de los procesos.

Compartir el riesgo: se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Para el caso de los riesgos de corrupción, se puede compartir, pero no se puede transferir su responsabilidad. Se hace seguimiento trimestral a través de los informes de gestión de los procesos.

Adicionalmente, se deberán documentar al interior de los procesos planes de contingencia (después de que ocurra el evento) con el fin de tratar el riesgo materializado, con criterios de oportunidad, evitando el menor daño en la prestación de los servicios; estos planes estarán documentados y son anexos al mapa de riesgos de la entidad.

La valoración de los riesgos se realiza multiplicando la calificación de la Probabilidad por la calificación del Impacto dando como resultado los niveles de severidad del riesgo: (Ver tabla 8 de la Guía de Administración del Riesgo – DAFP).

Mapa de Calor



Nivel de severidad del riesgo:

BAJO	Aceptar riesgo
MEDIO	Aceptar o reducir riesgo
ALTO	Reducir, evitar, compartir riesgo
EXTREMO	Evitar, reducir, compartir riesgo

Los riesgos de corrupción siempre van a estar ubicados en los niveles de severidad, Alto y Extremo.

11. Clasificación del Riesgo

Existen dos tipos de riesgo para su tratamiento, los cuales se detallan a continuación:

Riesgo Inherente (antes de controles): es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

El tratamiento se realiza mediante la definición de una serie de acciones o controles, los cuales tienen un responsable y una fecha para el seguimiento, buscando de esta forma asegurar la correcta administración de los riesgos. Esta información se puede evidenciar en el mapa de riesgos de la entidad.

Para esto, la Política de Riesgos en la CRC establece los principios para dar correcto tratamiento de los riesgos, mediante el establecimiento de planes de acción estratégicos y asegurando la continuidad del proceso.

Riesgo Residual (después de controles): El riesgo residual es el riesgo resultante después de aplicar los controles necesarios para su mitigación y prevenir su ocurrencia. El tratamiento de estos riesgos se clasifica de acuerdo con el nivel de severidad.

De acuerdo con la probabilidad e impacto de los riesgos y a los controles aplicados se evalúa el riesgo residual y dependiendo de este resultado se analiza si los riesgos (i) se asumen (ii) se reducen (iii) se comparten o transfieren, o (iv) se evitan.

Teniendo en cuenta lo anterior, la CRC ha establecido seguimientos con cierta periodicidad en cada uno de sus procesos de control, donde se evidencia también el responsable. Toda esta información está registrada en la Herramienta de Gestión Estratégica /módulo de riesgos, donde se encuentra toda la información relacionada con la administración de los riesgos.

12. Tipos de control

Estratégicos: establece objetivos generales, controla el desempeño y los resultados de la entidad en su totalidad. se basa en el ejercicio de planeación estratégica que está en cabeza del Comité de Comisionados.

Operacionales: es el control sobre la ejecución de las tareas y las operaciones desempeñadas por el personal no administrativo de la entidad. Su acción es inmediata. Se evidencia en el control diario de ejecución de actividades.

Lo controles se determinan de acuerdo con su naturaleza y por la forma de implementación:

Determinar su naturaleza:

a. Controles preventivos: Son las acciones que evitan o previenen que el riesgo suceda o se materialice.
b. Controles correctivos: Se ejecutan después de materializado el riesgo y lo que buscan es enfrentar la situación y recuperar la operación o servicio afectado.

De acuerdo con la Implementación:

a. Automáticos: son los controles que para su ejecución utilizan herramientas o sistemas de información. Ejemplo, alarmas, sistemas de grabación.
b. Manuales: Se refiere a las acciones relacionadas con políticas de operación, como firmas, confirmaciones por correo electrónico, listas de chequeo, entre otros.

13. Periodicidad para el seguimiento

Se deberá incluir la administración de riesgos dentro de los sistemas de gestión organizacional para facilitar la apropiación de este tema, y se seguirá realizando el seguimiento mediante las Reuniones de Análisis Estratégico (RAE) realizadas por los diferentes Grupos Internos de Trabajo de manera continua para todos los procesos cada trimestre. El cumplimiento de esta política, así como la aplicación de la metodología de administración de riesgos de la Entidad se realizará de la siguiente manera:

a) Anualmente se revisa el mapa de riesgos completo de la Entidad, en los plazos establecidos dentro del Plan Anticorrupción y de Atención al ciudadano de cada vigencia, para lo cual se tomará como insumo, las auditorías realizadas por Control Interno y Organismos de Control, así como lo reportado en las diferentes RAE e informes de desempeño presentados por los diferentes procesos. Esta revisión será realizada con el acompañamiento de los coordinadores de los diferentes Grupos Internos de Trabajo y de esta manera se ajustará el mapa de riesgos de acuerdo con los cambios normativos sectoriales y nacionales. El control de cambios estará bajo la responsabilidad del Asesor del Sistema Integral de Gestión, quien debe diligenciar el cuadro maestro de registro de control de cambios de los documentos del Sistema Integral de Gestión.
Responsable: Coordinación Ejecutiva con apoyo de los Grupos Internos de Trabajo.

b) El seguimiento se realizará trimestralmente; dentro de los informes de desempeño de cada Grupo Interno de Trabajo, con los resultados del periodo y previo a esa fecha se deben realizar las reuniones de análisis estratégico RAE de los diferentes Grupos Internos de Trabajo, las cuales en su agenda incluirán el análisis de los riesgos, para hacer seguimiento a los mismos y revisar los controles por parte del equipo asistente a la reunión. Para alcanzar dicho objetivo, el equipo que haga parte de la RAE debe conocer los riesgos y el estado actual de los mismos para participar activamente en cada reunión.
Responsable: Grupos Internos de Trabajo.

c) Presentar trimestralmente los resultados del análisis de riesgos a la Alta Dirección, a través de los informes de entrada y salida del Sistema Integral de Gestión, con el fin de evidenciar si se materializó algún riesgo, si es necesario crear alguno nuevo o si se requiere eliminar alguno que con el tiempo no aplique a la entidad.
Responsable: Coordinación Ejecutiva

d) Fortalecer el cumplimiento de la presente política a través de capacitaciones establecidas dentro del Plan Anual de Capacitaciones de la entidad.
Responsables: Gestión Administrativa y Financiera y Capital Intelectual.

14. Niveles de responsabilidad sobre el seguimiento y evaluación

A partir de las líneas de defensa establecidas dentro del Modelo Integrado de Planeación y Gestión, las responsabilidades respecto la gestión, seguimiento y evaluación de los riesgos son las siguientes:

Línea de defensa	Responsables	Actividades

Línea Estratégica	Alta dirección y Comité Institucional de Coordinación de Control Interno.	• Establecer la Política de Administración del Riesgo • Específicamente el Comité Institucional de Coordinación de Control Interno, evaluar y dar línea sobre la administración de los riesgos en la entidad • Realimentar a la Alta Dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. • Hacer seguimiento a su gestión, gestionar los riesgos y aplicar los controles
Primera Línea	Coordinadores de Grupos Internos de Trabajo	• Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales • Definir y diseñar los controles a los riesgos. • A partir de la política de administración del riesgo, establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección. Con base en esto, establecer los mapas de riesgos. • Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. Implementan procesos para identificar, disuadir y detectar fraudes; y revisan la exposición de la entidad al fraude con el auditor interno de la entidad.
Segunda Línea	Todos los funcionarios de la entidad	• Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada • Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude • Monitorear cambios en el riesgo legal, regulatorio y de cumplimiento • Consolidar los seguimientos a los mapas de riesgo • Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar • Los supervisores de contratos deben realizar seguimiento • a los riesgos de estos e informar las alertas respectivas

Tercera Línea	Coordinación de Control Interno	• Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa • Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna • Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías • Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad • Alertar sobre la probabilidad de riesgo de fraude o • corrupción en las áreas auditadas

Finalmente, para facilitar el cumplimiento de la misión y objetivos institucionales de la CRC a través de la prevención y administración de los riesgos y como complemento a la presente política, la entidad cuenta con el procedimiento PS_80015 "Procedimiento Administración de Riesgos", en el cual se describe el paso a paso para la adecuada definición, seguimiento y control a los diferentes riesgos establecidos en cada uno de los procesos de la entidad, así como la metodología para determinar el plan de contingencia a seguir en caso que alguno de los riesgos se materialice.