COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Política de Administración de Riesgos 2022

Coordinaciones:
Coordinación Ejecutiva
Planeación Estratégica

Líder: Yamile Mateus.

Julio de 2022

Comité Institucional de Coordinación de Control Interno

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE LA CRC

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, al establecer los lineamientos para la gestión del riesgo a través del establecimiento de la presente política, así como los parámetros para el seguimiento y efectividad de los controles.

Para dar continuidad a la política de administración de riesgos, se hace necesario definir los criterios orientadores respecto al tratamiento de estos, a fin de mitigar sus efectos y propender por el cumplimiento de los objetivos estratégicos; por lo que el fin de la presente política es definir los lineamientos de la Alta Dirección sobre la manera de abordar la administración de los riesgos institucionales, en todos los niveles de la Entidad, socializarla con todos los funcionarios y contratistas en un lenguaje claro, común y sencillo.

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 diciembre de 2020 (versión 5), la cual da lineamientos para los riesgos de gestión, corrupción y seguridad de la información.

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 establecidos.

Elementos conceptuales que deben ser aplicados en la Entidad.

La CRC cuenta con un Código de Integridad, instrumento mediante el cual se definen las reglas de comportamiento que deben gobernar la conducta de los funcionarios de la entidad, a través del cual se busca que los integrantes de la entidad interioricen este código como parte inherente al desarrollo

cotidiano de sus labores, con el fin de prestar un mejor servicio, actuar con transparencia, hacer buen uso de los recursos y contribuir con 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 busca garantizar la operación normal de la Entidad, minimizar la probabilidad e impacto de los riesgos, fortalecer la cultura de control y aumentar la capacidad de alcanzar los objetivos estratégicos definidos por la CRC.

2. DEFINICIONES APLICABLES A LA GESTIÓN DE RIESGOS EN LA CRC

Con el fin de facilitar el entendimiento del contenido y aplicación de la presente Política, a continuación, se listan las principales definiciones relacionadas con la gestión de riesgos, las cuales se toman de manera literal de la Guía para la Administración del Riesgo y Diseño de Controles en las Entidades Públicas, Versión 5, expedida por el Departamento Administrativo de la Función Pública en diciembre de 2020:

- ***Aceptación del riesgo****: decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.*
- ***Activo de información:*** *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.*
- ***Apetito al 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.*
- ***Capacidad de Riesgo:*** *es el máximo valor del nivel del 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 las cuales se puede presentar el 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 permite reducir o mitigar un riesgo.*
- ***Control Automático****: son los ejecutados por un sistema.*
- ***Control Correctivo:*** *control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.*
- ***Control Detectivo:*** *control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.*
- ***Control Manual:*** *controles que son ejecutados por personas.*
- ***Control Preventivo****: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.*
- ***Disponibilidad:*** *propiedad de ser accesible y utilizable a demanda por una entidad.*
- ***Factores de riesgo:*** *son las fuentes generadoras de riesgos.*
- ***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.*
- ***Impacto:*** *se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.*
- ***Integridad:*** *propiedad de exactitud y completitud.*
- ***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. 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.*
- ***Riesgo:*** *efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales 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.*
- ***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:*** *el resultado de aplicar la efectividad de los controles al riesgo inherente.*
- ***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. ROLES, RESPONSABILIDADES Y AUTORIDAD EN LA GESTIÓN DE RIESGOS EN LA CRC.

A partir del esquema de líneas de defensa establecido dentro del Modelo Integrado de Planeación y Gestión, para la CRC las responsabilidades respecto al control, la gestión, seguimiento y evaluación son las siguientes[1]:

Línea de Defensa	Integrantes	Responsabilidades y Actividades
Línea Estratégica	Alta dirección y Comité Institucional de Coordinación de Control Interno. Alta Dirección. (Director Ejecutivo, Comisionados y Coordinador Ejecutivo) Comité Institucional de Coordinación de Control Interno. (Director Ejecutivo, Comisionados de Comunicaciones y de Contenidos Audiovisuales, Coordinador Ejecutivo y Coordinadores de los Grupos Internos de Trabajo)	• Establecer la gestión del riesgo en la Entidad a través de la Política de Administración del Riesgo. • Analizar los riesgos y amenazas institucionales que pueden afectar el cumplimiento de los planes estratégicos. • Dar lineamientos, asesorar y tomar decisiones en temas de Control Interno. • Articular el adecuado funcionamiento del Sistema de Control Interno en la entidad. • Revisar el cumplimiento de los objetivos institucionales y la incidencia de los riesgos materializados en el cumplimiento de dichos objetivos. • Revisar las acciones correctivas y planes de acción ante la materialización de los riesgos, con el fin de tomar medidas efectivas y oportunas que permitan evitar la recurrencia del evento o incidente. • Establecer acciones de intervención para asegurar los resultados, solicitar el ajuste de los procesos que intervienen en el logro de los resultados, así como reorganizar los equipos de trabajo y los recursos para asegurar los resultados, esto a partir del análisis de los indicadores de gestión de la Entidad. • Establecer la periodicidad de reuniones del Comité Institucional de Coordinación de Control Interno, de acuerdo con lo establecido en la Resolución 147 de 2022.
Primera Línea	Todos los funcionarios de la entidad que ejecutan actividades como líderes de procesos, proyectos y/o	• Identificar, controlar, mitigar y evaluar los riesgos continuamente a través del autocontrol. Para ello se debe apoyar en los puntos de control de los procedimientos de los procesos a su cargo. • Ejecutar los controles de los riesgos del proceso a su cargo y hacer seguimiento continuo a los mismos.

[1] Manual operativo MIPG Versión 3. Diciembre de 2019.

Línea de Defensa	Integrantes	Responsabilidades y Actividades
	actividades continuas.	• Medir, analizar y mejorar los indicadores asociados a los riesgos del proceso a su cargo. • Contar con las evidencias sobre los controles aplicados a los riesgos a su cargo. • Ejecutar las acciones correctivas para el tratamiento por la materialización de riesgos y contar con las evidencias. Reportar de manera inmediata a la 2ª. Línea de Defensa para que se ejecuten los planes de contingencia y se identifiquen las causas y las acciones de mejoramiento que eviten la recurrencia de materialización. • Reportar a la 2ª Línea de Defensa por lo menos una vez al mes, en las reuniones de seguimiento de los procesos, la gestión de cada uno de los riesgos del proceso.
Segunda Línea	Comité Institucional de Gestión y Desempeño. (Director Ejecutivo, Comisionados de Comunicaciones y de Contenidos Audiovisuales, Coordinador Ejecutivo y Coordinadores de los Grupos Internos de Trabajo) -Coordinadores de Grupos Internos de Trabajo. -Líderes de los sistemas (Ambiental, Seguridad y Salud en el Trabajo, Seguridad Digital, ISO 9001). -Comité de Comisionados. -Sesión de Comisión.	• Asegurar que las actividades desarrolladas en la 1ª línea de defensa sean las apropiadas y estén funcionando de manera correcta y adecuada, a través de la supervisión en la identificación, análisis, evaluación y formulación de las acciones para el tratamiento de gestión de riesgos. • Revisar que los controles y los planes de acción para la mitigación de los riesgos estén diseñados de manera adecuada y se estén ejecutando continuamente; así mismo, hacer recomendaciones de mejora, seguimiento y fortalecimiento de estos. • Identificar los temas clave para la toma de decisiones y las acciones de prevención que eviten la materialización de los riesgos. • Realizar seguimiento periódico a la primera línea de defensa sobre la gestión de riesgos del proceso. • Reportar trimestralmente desde la segunda línea a la Línea Estratégica a través del Asesor del Sistema Integral de Gestión, sobre los resultados del aseguramiento, generación de alertas y presentación de recomendaciones sobre la gestión de riesgos en los procesos a su cargo. Dejar evidencia del aseguramiento en las Reuniones de Análisis Estratégico (RAEs) de los procesos a su cargo. • Comunicar oportunamente a la tercera línea de defensa y a la línea estratégica, el resultado de la gestión de los riesgos a través del Asesor del Sistema Integral de Gestión.

Línea de Defensa	Integrantes	Responsabilidades y Actividades
Tercera Línea	Oficina 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 Sistema de Control Interno, 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. • Reportar y alertar a la línea estratégica sobre la gestión de riesgos, de acuerdo con los reportes de la primera y segunda línea de defensa. • 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. • Asesorar a la Línea Estratégica, así como a la primera y segunda línea de defensa sobre el marco normativo que aplica a la CRC, con el fin articular de manera efectiva los riesgos.

4. 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.

NORMA	DESCRIPCIÓN
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, especialmente los que se relacionan a continuación: En el Artículo 3º se establece el rol que deben desempeñar las oficinas de control interno, entre ellas: ➢ (…) que se enmarca en cinco tópicos (…) ➢ valoración de riesgos. El parágrafo del Artículo 4º señala como objetivos del sistema de control interno ➢ (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (…) ➢ Así mismo establece en este mismo artículo que la administración de riesgos, hace 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, especialmente en el numeral 1.3 donde se hace referencia a los componentes de administración del riesgo.
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 943 de 2014	Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
Decreto 1081 de 2015	Este Decreto señala o establece la metodología para elaborar la estrategia de lucha contra la corrupción, entre otros, la gestión de riesgos como

NORMA	DESCRIPCIÓN
	primer componente del Plan Anticorrupción y de Atención al Ciudadano.
CONPES 3854 – 2016	La "Política Nacional de Seguridad Digital", consideró que era necesario cambiar el enfoque tradicional e incluir la gestión de riesgo como uno de los elementos más importantes para abordar la temática, estableciendo como objetivo general: "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país."
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 "por 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. Diciembre 2020.	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, Versión 5.

5. OBJETIVOS

5.1. 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.

5.2. Objetivos Específicos

- Formalizar al interior de la CRC una metodología para administrar los riesgos de toda naturaleza a los que se enfrenta la entidad: gestión, corrupción, seguridad digital, salud y seguridad en el trabajo, ambientales, entre otros.
- Establecer pautas para la identificación de los factores que representan amenazas u oportunidades para el cumplimiento de los objetivos.
- Definir los roles y responsabilidades para le gestión de riesgos bajo el esquema de 3 líneas de Defensa en la CRC.
- 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, seguridad digital, ambientales, salud y seguridad en el trabajo.
- Caracterizar el instrumento para la administración del riesgo (Mapa de riesgos) de acuerdo con los requisitos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas – V5 de la Función Pública.
- Cumplir con los principios del Modelo Integrado de Planeación y Gestión – MIPG, Modelo Estándar de Control Interno y el Sistema Integral de Gestión de la CRC.
- Establecer un mecanismo y periodicidad para la difusión y apropiación de la política de riesgos por parte de todo el equipo de la CRC.

6. ALCANCE DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS EN LA CRC.

La presente política es aplicable a todos los procesos y proyectos de la Entidad y a todas las actividades realizadas por los funcionarios y contratistas durante el ejercicio de sus funciones u obligaciones. La CRC mantiene los canales de información y comunicación apropiados, como el correo electrónico, página Web, redes sociales incluida la red interna Yammer, etc, para garantizar un adecuado conocimiento y gestión de los riesgos. Asimismo, para los proyectos regulatorios, la gestión de riesgos se realiza de acuerdo con lo establecido en el procedimiento P-2001 Diseño y Desarrollo de Proyectos de la Entidad.

Es de aclarar que, para los riesgos de seguridad de la información, se siguen los criterios definidos en el Modelo de Seguridad y Privacidad de la información MSPI[2] y de la guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 5 del Departamento Administrativo de la Función Pública - DAFP.

7. ALINEACIÓN CON EL PLAN ESTRATÉGICO 2021-2025

La CRC definió el siguiente Plan Estratégico para la vigencia 2021-2025:

Propósito Superior
Una Colombia con servicios de comunicaciones que mejoren la calidad de vida de toda la ciudadanía.

Misión
Regular los mercados de comunicaciones bajo criterios de mejora normativa para proteger los derechos de la ciudadanía, promover la competencia, la inversión, la calidad de los servicios y el pluralismo informativo.

Visión
Consolidar un ambiente regulatorio innovador, simple, dinámico, transparente, plural y con usuarios empoderados, que contribuya al desarrollo del país.

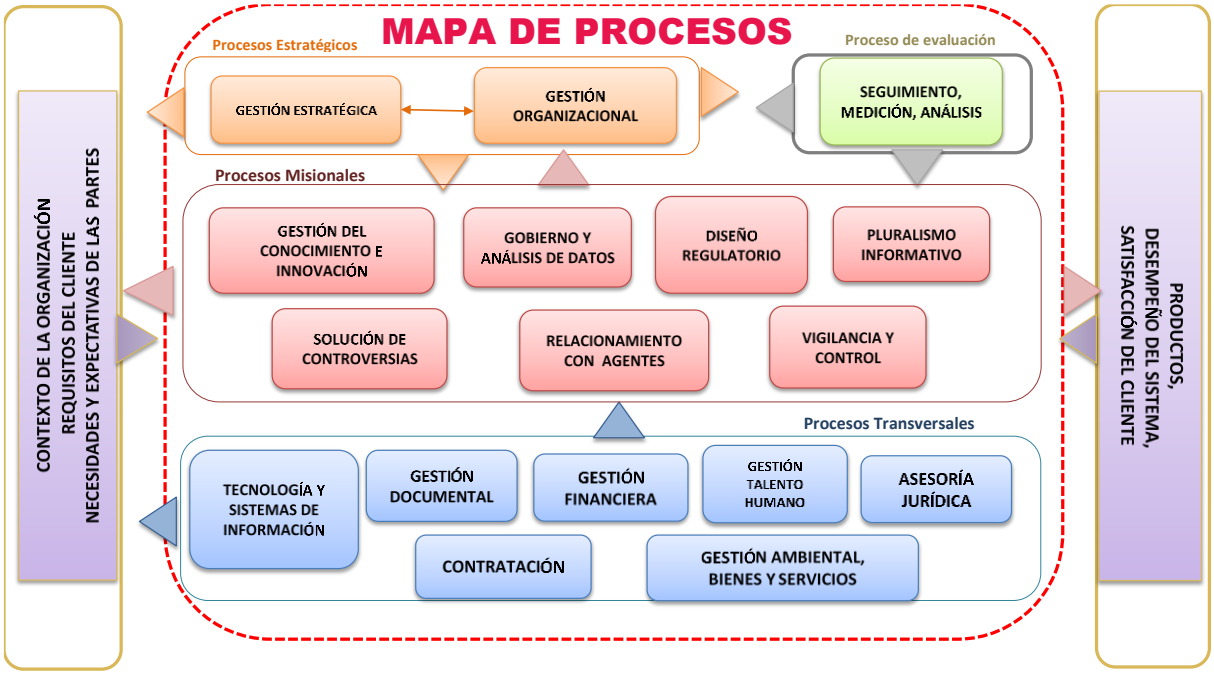
[2] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Mapa Estratégico

Fuente: Elaboración propia CRC.

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, el cual está integrado por las normas ISO 9001, NTC ISO 14001 y el Sistema de Gestión de Seguridad y Salud en el Trabajo Decreto 1082 de 2015 y Resolución 312 de 2019 del Ministerio del Trabajo, con el siguiente Mapa de Procesos:

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, y de esta manera se asegura la alineación de los riesgos con el direccionamiento estratégico de la Entidad. El seguimiento a la efectividad de los controles de los riesgos y sus planes de acción se ejecuta a través del desarrollo del esquema de tres líneas de defensa, información que queda documentada en los informes trimestrales de desempeño de cada proceso, así como en los informes gerenciales de revisión trimestral y, la línea estratégica define la gestión del riesgo con la aprobación de la presente Política, en el Comité Institucional de Coordinación de Control Interno.

8. CONTEXTO

Para la identificación de los riesgos que pueden afectar los diferentes procesos de la entidad, se contemplan los siguientes factores para cada categoría. Es importante mencionar que se mantienen los criterios establecidos en la guía para la administración del riesgo y el diseño de Controles en Entidades Públicas 2018 (versión 4), teniendo en cuenta que estos criterios continúan vigentes y son pauta para establecer el contexto en la identificación de los riesgos:

8.1. 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, salud pública.
- **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.
- **Auditorías externas**: evaluaciones llevadas a cabo por los organismos de control, como la Contraloría General de la República. Resultado de auditoría externa al Sistema Integral de Gestión (Este criterio se incluye como recomendación del Departamento Administrativo de la Función Pública –DAFP resultados FURAG 2021).

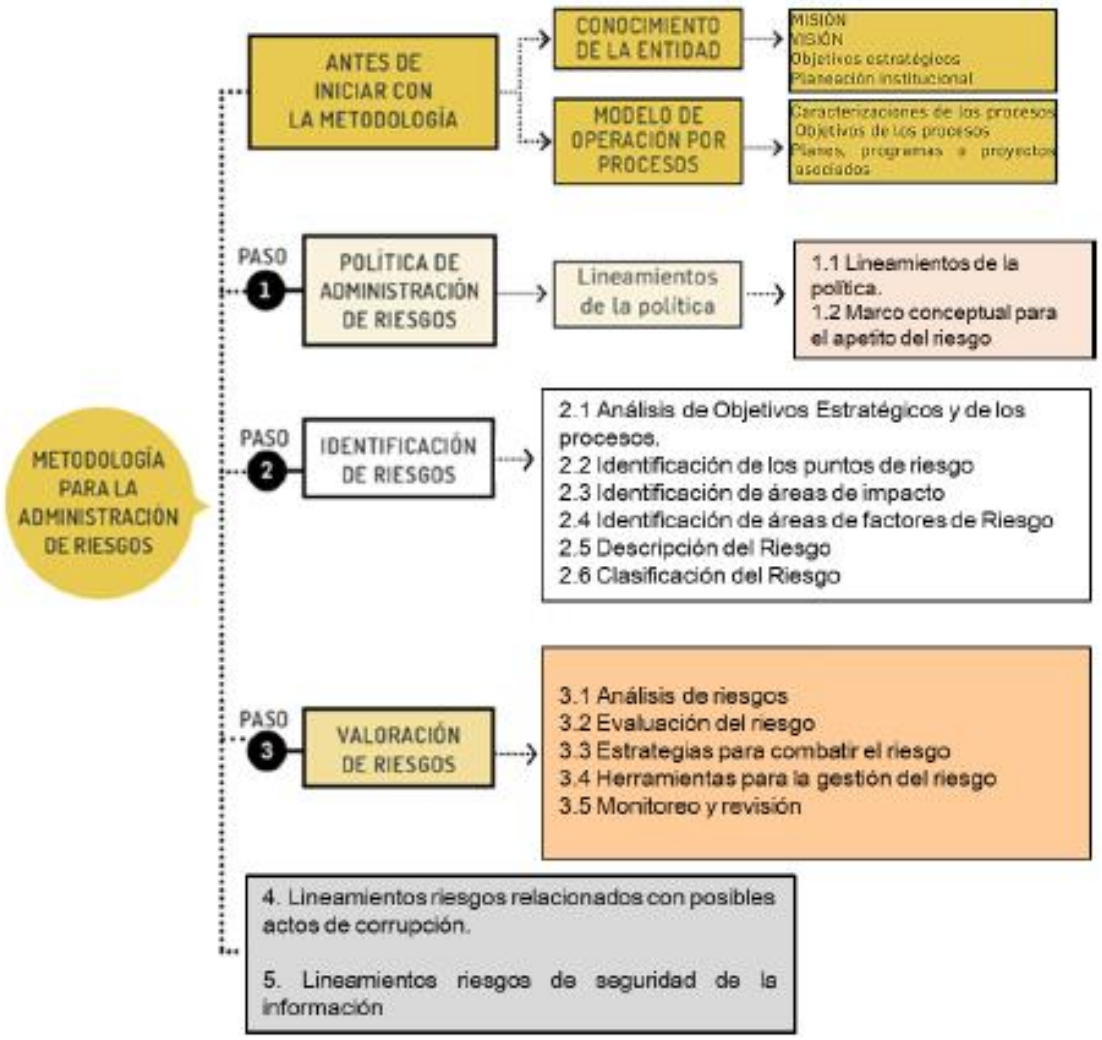
8.2. Contexto Interno

- **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.
- **Auditorías Internas:** evaluaciones llevadas a cabo por la Oficina de Control Interno y resultados de las auditorías internas al Sistema Integral de Gestión.

9. METODOLOGÍA DE GESTIÓN DE RIESGOS EN LA CRC

La metodología de administración de riesgos en la CRC se ha diseñado según las especificaciones contenidas en la Guía para la Administración del Riesgo – V5. DAFP[3]. Lo anterior, siguiendo el siguiente esquema:

[3] Departamento Administrativo de la Función Pública – DAFP. Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5, diciembre de 2020.



Fuente: Guía de Administración del Riesgo, DAFP. Versión 5. 2020.

9.1. Identificación de los riesgos.

Para la identificación general de los riesgos de gestión y de corrupción, cada grupo interno de trabajo responsable de los diferentes procesos en la CRC realiza reuniones con diferentes funcionarios para la identificación de aspectos tales como objetivo de cada proceso, contexto externo e interno, causas o fuentes, efectos, y factores que se deben tener en cuenta para realizar el análisis y la valoración de los riesgos.

El paso inicial es la realización del análisis de los objetivos estratégicos del proceso y ajustar el objetivo del proceso cuando sea necesario. Los objetivos deben incluir el qué, cómo, para qué, cuándo y cuánto y, debe contener los atributos mínimos de la metodología SMART (Específico, Medible, Alcanzable, Relevante y en Tiempo).

También se deben tener en cuenta los puntos de riesgo, es decir las actividades donde pueden ocurrir eventos operativos de incertidumbre que deben estar controlados para asegurar el cumplimiento de los objetivos de cada uno de los procesos y los objetivos estratégicos.

Se deben identificar las fuentes generadoras del riesgo, es decir, las causas del riesgo, para ello se deben utilizar preguntas de referencia: ¿cómo puede suceder?, ¿por qué puede suceder? y, posteriormente identificar ¿qué consecuencias tendría su materialización?

Asimismo, se debe incluir la descripción del riesgo que contenga todos los detalles necesarios para que se pueda entender, para ello se deben tener en cuenta las siguientes frases: lo que puede ocurrir (qué), cuál es la causa inmediata (cómo) y finalmente la causa raíz (¿Por qué?).

Ejemplo:

Afectación del presupuesto. **(qué)**

Por disminución de la contribución de los operadores. **(cómo)**

Disminución de los ingresos de los operadores por recesión económica durante la vigencia. **(por qué)**

En la redacción del riesgo se deben tener en cuenta los siguientes aspectos:

- **a.** Evitar redactar con palabras negativas y palabras que denoten un factor de riesgos como: ausencias de, falta de, deficiente, etc.
- **b.** No describir las causas en el riesgo; el riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.
- **c.** Tener en cuenta que no existen riesgos transversales, existen causas transversales, pero el riesgo siempre debe contar con un proceso responsable.

De otra parte, en la redacción de los riesgos de corrupción se debe tener la siguiente estructura: acción u omisión + uso del poder + desviar la gestión de lo público + beneficio privado. Ejemplo: Posibilidad de recibir o pedir algún beneficio a nombre propio o de un tercero para realizar un trámite.

Para los riesgos de seguridad digital se debe iniciar con la identificación de los activos de información, y la redacción se debe dar por la combinación de:

Pérdida de confidencialidad, integridad y/o disponibilidad + Activo(s) de información afectado(s) + Vulnerabilidad(es) + Amenaza(s).

Ejemplo:
Pérdida de disponibilidad del portal WEB de la CRC debido a ataques informáticos por configuraciones por defecto en el servidor.

9.2. Clasificación de los Riesgos

De acuerdo con lo establecido en la mencionada Guía de Administración del Riesgo del DAFP, versión 5, los riesgos se clasifican en las siguientes categorías:

a. ***Ejecución y administración de procesos:*** *pérdidas derivadas de errores en la ejecución y administración de procesos.*
b. ***Fraude externo:*** *actos de fraude por personas ajenas a la organización (aquí no participa o actúa personal de la Entidad).*
c. ***Fraude interno:*** *actuaciones irregulares, abuso de confianza, apropiación indebida. Involucrado al menos un funcionario de la Entidad.*
d. ***Fallas tecnológicas:*** *errores de hardware, software, interrupción de servicios.*
e. ***Relaciones laborales:*** *se refiere a las pérdidas generadas por actividades y acciones que sean contrarias a las leyes y acuerdo de empleo, salud, seguridad.*
f. ***Usuarios, productos y prácticas:*** *fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación.*
g. ***Daños a activos fijos:*** *pérdida por daños o extravíos de activos por desastres naturales u otros eventos externos provocados por atentados, vandalismo, orden público.*

9.3. Análisis de Riesgos

Antes de iniciar el análisis de los riesgos se deben tener claros los siguientes conceptos:

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, para de esta forma asegurar la correcta administración de los riesgos. Esta información se puede evidenciar en el mapa de riesgos de la Entidad.

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.

Ahora bien, con el análisis de riesgos se busca establecer la probabilidad de ocurrencia de un riesgo y el impacto o consecuencias de este, para así establecer o identificar la zona de riesgo inicial, lo que es llamado **Riesgo inherente**. Posteriormente, se realiza la evaluación con el fin de comparar el análisis del riesgo inicial con los controles establecidos, para así determinar la zona de riesgo final, es decir el **Riesgo residual.**

Determinar 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 se determina teniendo en cuenta los siguientes criterios:

	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 de Administración de Riesgos. DAFP. Versión 5. 2020

Para los riesgos de seguridad de la información, se tendrán en cuenta los siguientes criterios para medir la probabilidad:

Nivel	Descriptor	Histórico	Prospectiva
1	Rara vez	En los últimos cinco (5) años no se ha materializado el riesgo	Se espera que el evento de riesgo se materialice en los próximos cinco (5) años.
2	Improbable	En los últimos cinco (5) años se ha materializado el riesgo al menos una vez	Se espera que el evento de riesgo se materialice más de una vez en los próximos cinco (5) años.
3	Posible	En los últimos dos (2) años se ha materializado el riesgo al menos una vez	Se espera que el evento de riesgo se materialice al menos una vez en los próximos dos (2) años.
4	Probable	En el último año se ha materializado el riesgo al menos una vez	Se espera que el evento de riesgo se materialice una vez en el próximo año
5	Casi seguro	En el último año se ha materializado el riesgo más de una vez	Se espera que el evento de riesgo se materialice más de una vez en el próximo año

Fuente: Elaboración Propia CRC

Determinar el Impacto:

Por impacto se entienden las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. Se puede clasificar en impacto económico y reputacional. Es importante tener en cuenta, que cuando se presentan las dos variables se debe tomar el valor más alto. La tabla de valoración del impacto de los riesgos, establecida por el DAFP es la siguiente:

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 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 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía de Administración de Riesgos. DAFP. Versión 5. 2020

Para los riesgos de seguridad de la información, se tendrán en cuenta las siguientes variables para valorar el impacto:

Nivel	Descriptor	Consecuencias Cuantitativas	Consecuencias Cualitativas
1	**Insignificante**	• No hay pérdidas económicas. • Afectación Imagen a nivel de grupo o equipo. • Llamados de atención a nivel grupo o equipo. • No hay daño medioambiental. • Indisponibilidad de los servicios menor a una hora • Afectación a datos personales públicos.	• No hay interrupción de las operaciones de la entidad. • No se generan observaciones por entes de regulación o control. • Pérdida de información clasificada como baja. • No se Incumplen las metas y objetivos institucionales. • No se afecta la imagen institucional de forma significativa.

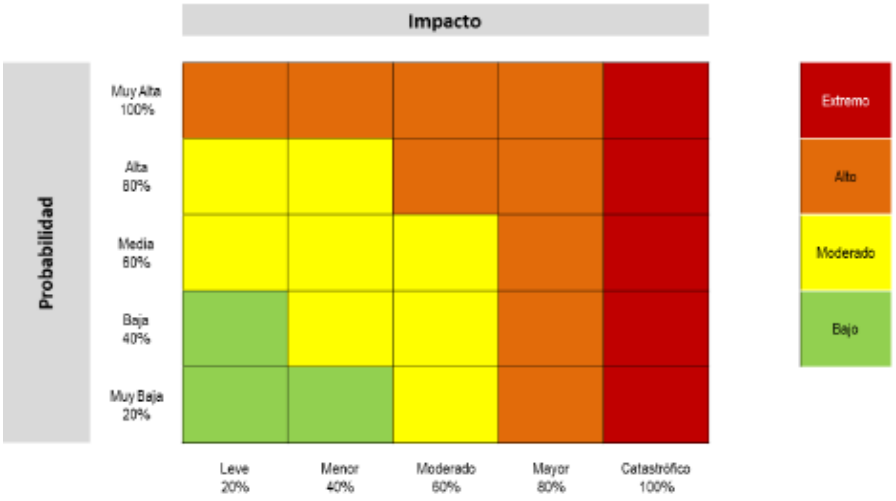
Nivel	Descriptor	Consecuencias Cuantitativas	Consecuencias Cualitativas
2	**Menor**	• Pérdidas económicas hasta de 10 SMMLV. • Afectación Imagen nivel de área • Sanciones o llamados de atención a nivel área. • Daño ambiental menor a un día recuperación • Indisponibilidad de los servicios menor a un día • Afectación a datos personales semiprivados	• Interrupción de las operaciones de la entidad hasta por 24 horas. • Se generan observaciones administrativas por entes de regulación o control. • Pérdida de información clasificada como media. • Atrasos de actividades del plan de acción Institucional. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
3	**Moderado**	• Pérdidas económicas entre 10.1 y 100 SMMLV. • Afectación Imagen del proceso • Sanciones o llamados de atención a nivel de proceso. • Daño ambiental menor a una semana de recuperación • Indisponibilidad de los servicios menor a una semana. • Afectación a datos personales privados o sensibles	• Interrupción de las operaciones de la entidad entre 24 y 48 horas. • Se generan observaciones administrativas con incidencia disciplinaria por entes de regulación o control. • Pérdida de información clasificada como alta. • Incumplimiento o atrasos en un proyecto estratégico de la CRC. • Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
4	**Mayor**	• Pérdidas económicas entre 100.1 y 200 SMMLV. • Afectación Imagen a Nivel Nacional • Sanciones o llamados de atención a toda la entidad. • Daño ambiental menor a un mes de recuperación • Indisponibilidad de los servicios menor a un mes. • Afectación a datos personales vulnerables o sensibles	• Interrupción de las operaciones de la entidad por más de dos (2) días. • Se generan observaciones administrativas con incidencia fiscal o penal por entes de regulación o control. • Pérdida parcial y recuperable de la información clasificada como crítica de la entidad. • Incumplimiento o atraso en los objetivos estratégicos de la CRC.

Nivel	Descriptor	Consecuencias Cuantitativas	Consecuencias Cualitativas
			• Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos. También por envío de información errónea y exposición de un vocero no autorizado.
5	**Catastrófico**	• Pérdidas económicas mayores a 300 SMMLV. • Afectación Imagen a Nivel internacional • Sanciones de Contraloría, Procuraduría y/o Fiscalía. • Daño ambiental mayor a un mes de recuperación • Indisponibilidad de los servicios mayor a un mes. • Afectación a datos personales vulnerables.	• Interrupción de las operaciones de la entidad por más de cinco (5) días. • Se genera intervención por parte de un ente de regulación o control. • Pérdida total de la información clasificada como crítica de la entidad. • Incumplimiento en la misión de la CRC. • Imagen institucional afectada en el orden nacional o regional por actos, hechos de corrupción comprobados o equivocación en el cargue de resultados.

Fuente: Elaboración Propia CRC

9.4. Evaluación del Riesgo:

Se debe tener en cuenta que, para realizar esta evaluación, en primera instancia se debe hacer el análisis preliminar, es decir al riesgo inherente, donde se aplican los valores de las tablas de probabilidad e impacto al riesgo antes de establecer controles, y para ello se debe tomar como base la siguiente tabla o matriz de calor:



Fuente: Guía de Administración de Riesgos. DAFP. Versión 5. 2020

Criterios para calificar el impacto para riesgos de corrupción

Para calificar el impacto de los riesgos de corrupción, se mantienen los criterios de la guía del DAFP en la versión 4 de 2018 y se debe dar respuesta a las siguientes preguntas:

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

Pregunta. Si el riesgo de corrupción se materializa, podría...	Sí	No
18 ¿Afectar la imagen nacional?		
19 ¿Generar daño ambiental?		

Fuente: Guía de Administración de Riesgos. DAFP. Versión 4. 2018

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

Fuente: Guía de Administración de Riesgos. DAFP. Versión 4. 2018

9.5. Identificación de Controles:

Una vez identificado el riesgo inherente se realiza la valoración de cada uno de los controles identificados para cada riesgo. Existen tipologías de controles así:

- **Control preventivo:** este control busca asegurar el resultado final. Establece condiciones que permiten evitar la materialización del riesgo. Estos controles atacan la probabilidad.
- **Control detectivo:** se presenta cuando se está ejecutando la actividad. Esto genera reprocesos.
- **Control correctivo:** este control se identifica cuando se ha materializado el riesgo, este tipo de controles tienen costos. Atacan el impacto.

Adicionalmente, los controles según la forma como se realizan se clasifican en:

- **Control manual:** son controles ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

Para evaluar los controles se deben tener en cuenta los criterios descritos en la siguiente tabla:

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: Guía de Administración de Riesgos. DAFP. Versión 5. 2020

Posterior a identificar y calcular los controles, se realiza el cálculo para definir el valor del riesgo residual y de esta manera poder ubicar dicho riesgo en la matriz de calor. **(Ver ejemplos de cálculo Guía de Administración del Riesgos. Versión 5. 2020 página 48)**

Es importante tener presente que si los controles no son correctivos el impacto residual es el mismo calculado inicialmente.

9.6. Niveles de tratamiento y aceptación de los Riesgos (APETITO DE RIESGO)

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. El seguimiento se realiza de manera trimestral a través de los informes de gestión de los procesos. Adicionalmente, las actividades de revisión, validación y aprobación se ejecutarán de acuerdo con los roles de la primera y segunda línea de defensa, así como la evaluación por parte de la Oficina de Control Interno. **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 y la elaboración de un plan de acción, como lo establece la Guía de Administración del Riesgo, el cual debe contener acción, responsable, fecha de implementación, fecha de seguimiento, seguimiento y estado. El seguimiento se realiza de manera trimestral a través de los informes de gestión de los procesos. Adicionalmente, las actividades de revisión, validación y aprobación se ejecutarán de acuerdo con los roles de la primera y segunda línea de defensa, así como la evaluación por parte de la Oficina de Control Interno y el correspondiente reporte a la línea estratégica.

Evitar el riesgo: se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que lo provoca. El seguimiento se realiza de manera trimestral a través de los informes de gestión de los procesos. Adicionalmente, las actividades de revisión, validación y aprobación se ejecutarán de acuerdo con los roles de la primera y segunda línea de defensa, así como la evaluación por parte de la Oficina de Control Interno.

Para mayor claridad la CRC aceptará los riesgos, en los siguientes casos:

Clase de riesgo	Zona de riesgo (identificada por la CRC)	Nivel de aceptación o máxima desviación
Riesgos por ejecución de Procesos. (estratégicos, Financieros, de cumplimiento, operativos)	Baja	La CRC asumirá el riesgo y se administrará por medio de las actividades propias del proceso.

Riesgos Fallas tecnológicas incluye también (Riesgos de seguridad digital)	Extrema o moderada	La CRC no admitirá aceptación del riesgo, siempre deben conducir a un tratamiento.
Riesgos de relaciones laborales	Extrema o moderada	La CRC no admitirá aceptación del riesgo, siempre deben conducir a un tratamiento.
Usuario, productos y prácticas	Moderada	La CRC no admitirá aceptación del riesgo, siempre deben conducir a un tratamiento.
Riesgo de corrupción fraude interno y externo	Extremo	La CRC no admitirá aceptación del riesgo, siempre deben conducir a un tratamiento.
Daños a Activos Fijos/Eventos Externos	Baja	La CRC asumirá el riesgo y se administrará por medio de las actividades preventivas ya establecidas en cada proceso, especialmente en Gestión Ambiental, Bienes y Servicios.
Riesgo de imagen o reputacional	Baja o moderado	La CRC asumirá el riesgo y se administrará por medio de las actividades preventivas ya establecidas en todos los procesos de la Entidad.

Fuente: Elaboración propia CRC.

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

9.7. Nivel de severidad del riesgo

BAJO	Aceptar riesgo
MODERADO	Reducir riesgo
ALTO	Reducir riesgo
EXTREMO	Reducir riesgo

Fuente: Elaboración propia CRC.

Los riesgos de corrupción en la CRC siempre van a estar ubicados en los niveles de severidad alto y extremo, y no se reducen ni se evitan.

9.8. Periodicidad para el seguimiento

El seguimiento a la gestión de riesgos se lleva a cabo de la siguiente manera:

a) Anualmente se revisa el mapa de riesgos completo de la Entidad, siguiendo el esquema de tres líneas de defensa y en los plazos establecidos dentro del Plan Anticorrupción y de Atención al ciudadano de cada vigencia, para lo cual se toma 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 es realizada de manera conjunta por los equipos de trabajo y los coordinadores de los diferentes Grupos Internos de Trabajo. El Asesor del Sistema Integral de Gestión como parte de la segunda línea de defensa debe hacer revisión general a la matriz para verificar que la misma no presente campos vacíos o fechas que no sean concordantes con los controles y el plan de acción identificados.

   Una vez ajustada la matriz por la primera y segunda línea de defensa, la misma es presentada por el grupo interno de trabajo de Planeación Estratégica, al Comité Institucional de Coordinación de Control Interno, en su rol de línea estratégica, para que desde dicha instancia se imparta el direccionamiento correspondiente y se dé la respectiva aprobación.

   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. El proceso de actualización de la matriz de riesgos es dinámico y por ende se puede actualizar cuando se identifiquen cambios, ajustes, eliminaciones, nuevos riesgos, etc.

   Responsables: todo el esquema de líneas de defensa, descrito en el numeral 3 del presente documento.

b) El seguimiento se realizará trimestralmente así: reporte del estado de los controles de los riesgos a través del formato establecido en el manual de Tres Líneas de Defensa, documento que va anexo a 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 y reporte del estado de los controles 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 del proceso, lo cual se garantiza con el seguimiento y reporte efectuado por la primera línea de defensa, de acuerdo con lo establecido en el manual de líneas de defensa, lo anterior para que exista una participación activa en las RAES.

   Responsable: cada uno de los Coordinadores de los Grupos Internos de Trabajo en su rol de segunda línea de defensa.

c) Ante la materialización de los riesgos de gestión, la primera y segunda línea de defensa responsables de la actividad deben hacer revisión inmediata de los controles, previa

identificación de las causas generadoras, aplicar los planes de contingencia y reportar a la tercera línea de defensa y a línea estratégica a través del Comité Institucional de Coordinación de Control Interno.

NOTA: Para las materializaciones de los riesgos de Seguridad Digital o de la Información, se tratarán como incidentes de seguridad de la información y se deberán informar al Coordinador del proceso de Tecnologías y Sistemas de Información y al Oficial de Seguridad de la Información. Igualmente, les aplican los reportes establecidos en el Manual de Tres Líneas de Defensa.

Responsable: cada uno de los Coordinadores de los Grupos Internos de Trabajo en su rol de segunda línea de defensa.

d) Igualmente, al identificar la materialización de los riesgos de corrupción se debe hacer revisión inmediata de los controles, previa identificación de las causas generadoras, tomar las medidas correctivas, realizar identificación de nuevos controles y reportar a la tercera línea de defensa y a la línea estratégica a través del Comité Institucional de Coordinación de Control Interno. En paralelo, se debe **informar o poner en conocimiento de las autoridades correspondientes tales como la Fiscalía, Contraloría, Procuraduría, Control Interno Disciplinario**, o la autoridad que la CRC considere pertinente, teniendo en cuenta la práctica corrupta identificada.

Responsable: cada uno de los Coordinadores de los Grupos Internos de Trabajo en su rol de segunda línea de defensa.

e) Desde el grupo Interno de trabajo de Planeación Estratégica, como segunda línea de defensa, se debe presentar trimestralmente los resultados del análisis y gestión de riesgos a la tercera línea de defensa y a la línea estratégica a través del Comité Institucional de Coordinación de Control Interno y, dejar documentado dicho análisis y seguimiento en 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 modificar o eliminar alguno que con el tiempo no aplique a la entidad.

Responsable: Grupo interno de trabajo de Planeación Estratégica.

f) Fortalecer el cumplimiento de la presente política a través de capacitaciones establecidas dentro del Plan Anual de Capacitaciones de la Entidad.

Responsables: el grupo interno de trabajo de Planeación Estratégica realiza la solicitud y entrega los insumos correspondientes y, el grupo interno de trabajo de Gestión Administrativa y Financiera ejecuta la capacitación.

g) En cumplimiento del componente de Información y Comunicación del MECI, la presente política debe ser publicada en la página Web y la Intranet de la CRC. Así mismo, se debe informar a todos los integrantes de la Entidad sobre su actualización, a través de los canales de comunicación interna establecidos.

Responsables: coordinadores de los grupos de trabajo de Planeación Estratégica y Relacionamiento con Agentes.

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, teniendo claro que el plan de contingencia es diferente al plan de acción establecido cuando la opción de tratamiento es reducir el riesgo.