COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Política de Administración de Riesgos 2021

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

Agosto de 2021

Comité de Coordinación de Control Interno

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

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 en un lenguaje claro, común y sencillo y por último, difundir tales 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 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.

Elementos conceptuales que deben ser aplicados en la Entidad.

La CRC cuenta con un código de Buen Gobierno, Ética e Integridad, instrumento mediante el cual se definen las reglas de comportamiento que deben gobernar la conducta de los funcionarios de la entidad. 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 el 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:*** *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 de las líneas de defensa establecidas 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	Responsables	Actividades

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

Línea Estratégica	Alta dirección y Comité Institucional de Coordinación de Control Interno.	• Analizar los riesgos y amenazas institucionales que pueden afectar el cumplimiento de los planes estratégicos y para ello debe establecer la gestión del riesgo en la Entidad a través de la Política de Administración del Riesgo. • Dar lineamientos, asesorar y tomar decisiones en temas de Control Interno son funciones del Comité Institucional de Coordinación de Control Interno. Este Comité es la instancia que articula 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.
Primera Línea	Todos los funcionarios de la entidad que ejecutan actividades como líderes de proyectos y actividades continuas.	• Operar para el mantenimiento efectivo de los controles internos, la ejecución de la gestión y seguimiento de los riesgos en el día a día • Identificar, controlar, evaluar y mitigar los riesgos continuamente a través del autocontrol. Para ello debe contar procedimientos con puntos de control documentados y actualizados.
Segunda Línea	Comité Institucional de Gestión y Desempeño/Coordinadores de Grupos Internos de Trabajo/líderes de los sistemas (Ambiental, SST, Seguridad Digital, ISO 9001)	• El Rol principal de esta línea de defensa es asegurar que las actividades desarrolladas en la primera línea de defensa sean las apropiadas y estén funcionando de manera correcta y adecuada. Para ello debe revisar que los controles 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 los mismos. • Supervisa la correcta implementación de la gestión de los riesgos en los procesos. • Identifica los temas clave para la toma de decisiones y las acciones de prevención que eviten la materialización de los riesgos.
Tercera Línea	Oficina de Control Interno	• Asesora en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa • Identifica y evalúa 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. • Comunica al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. • Revisa la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad • Alerta sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

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.
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. 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.
- Cumplir con los principios del Modelo Integrado de Planeación y Gestión, 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 durante el ejercicio de sus funciones. La CRC mantiene los canales de información y comunicación apropiados para garantizar un adecuado conocimiento y gestión de los riesgos. Así mismo para los proyectos regulatorios, la gestión de riesgos se realiza de acuerdo con lo establecido en el procedimiento de diseño y desarrollo P-2001.

Es de aclarar que, para los riesgos de seguridad de la información, se deben seguir los criterios definidos en el Modelo de Seguridad y Privacidad de la información MSPI[2].

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

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

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

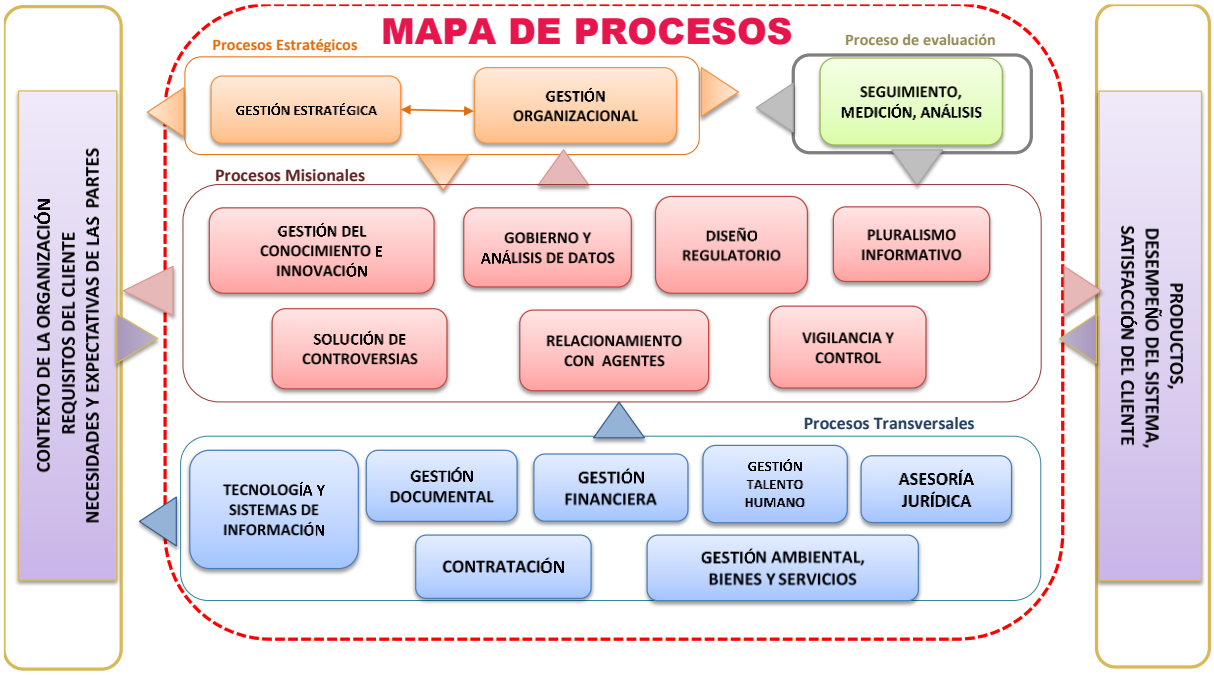
Consolidar un ambiente regulatorio innovador, simple, dinámico, transparente, plural y con usuarios empoderados, que contribuya al desarrollo del país.

Mapa Estratégico

Fuente: Elaboración propia.

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.

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 DAFP resultados FURAG 2020).

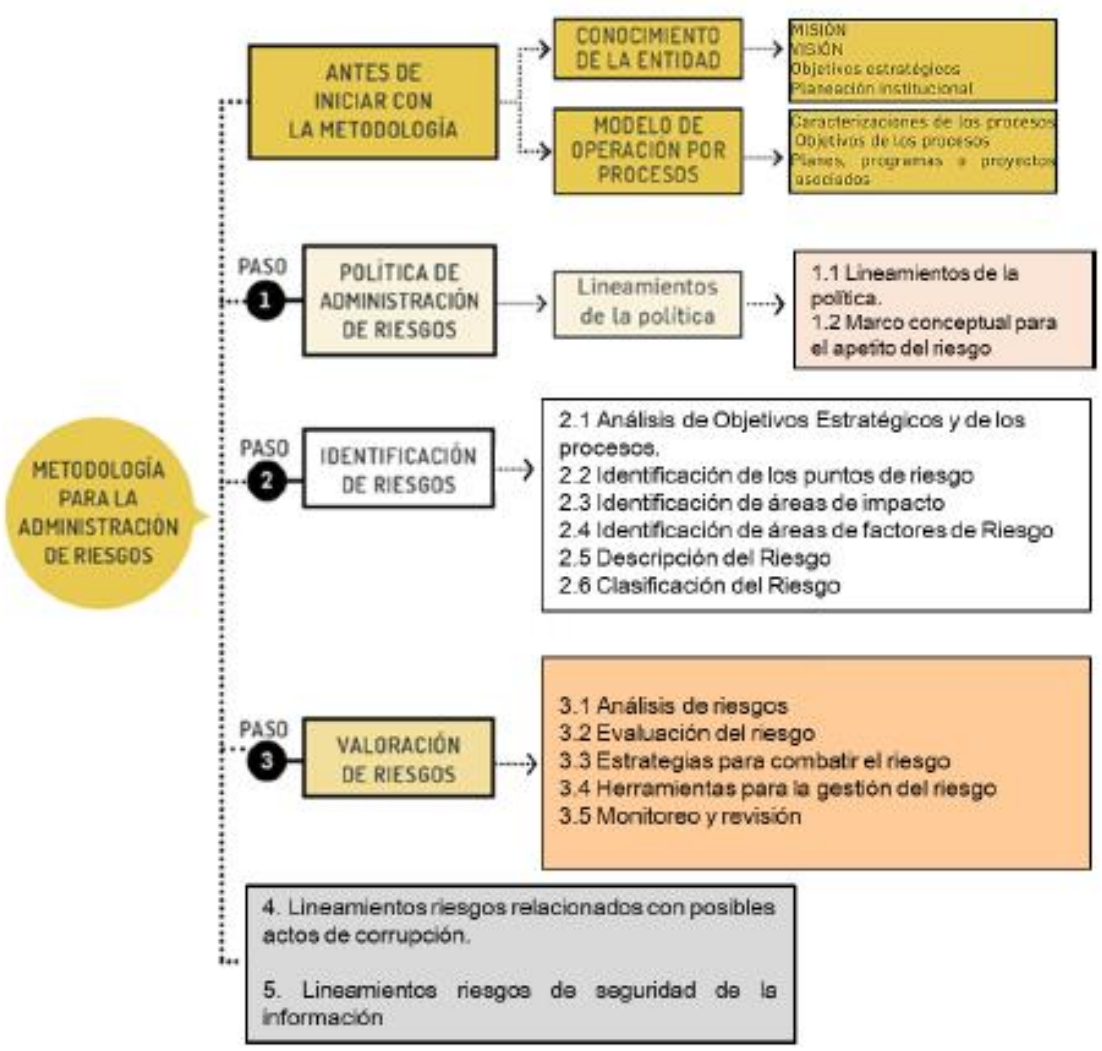
8.2. Contexto Interno

- **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 auditorias internas al Sistema Integral de Gestión. (Este criterio se incluye como recomendación del DAFP resultados FURAG 2020)

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.

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[3]. En todo caso siguiendo el siguiente esquema:



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

[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.

9.1. Identificación de los riesgos.

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

Para los riesgos de seguridad digital se debe iniciar con la identificación de los activos de información.

El paso inicial es la realización del análisis de los objetivos estratégicos y del proceso y ajustar el Objetivo del proceso cuando sea necesario. Los objetivos deben incluir el qué, cómo, para qué, cuándo y cuánto. El objetivo debe contener los atributos mínimos de 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 del proceso o los objetivos estratégicos.

Se deben identificar las fuentes generadoras del riesgo es decir las causas del riesgo, para ello utilizar preguntas ¿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 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 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.

9.2. Calificación 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 años 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

Determinar el Impacto:

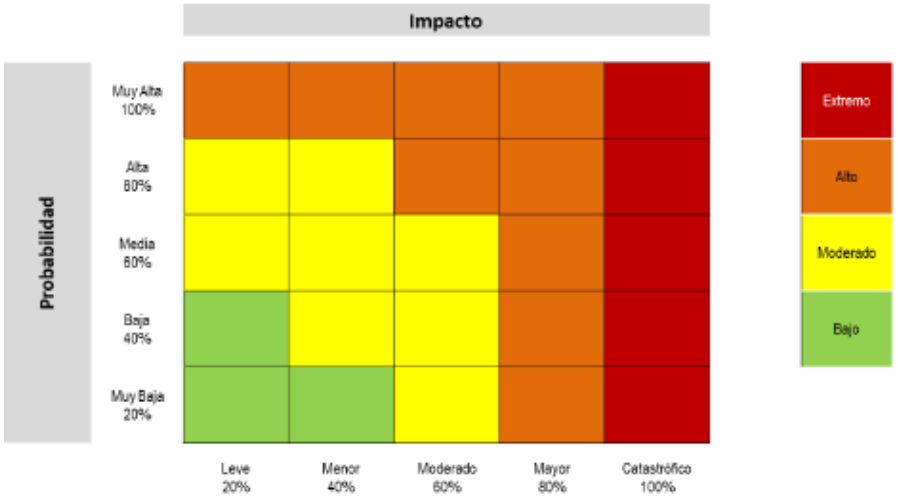
Por impacto se entienden las consecuencias que puede ocasionar a la entidad la materialización del riesgo. Se puede clasificar en impacto económico y reputacional. Es importante tener en cuenta que cuando se presentan las dos variables se debe tomar el valor más alto. La tabla de valoración del Impacto 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

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 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

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 realiza 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	25%

Características			Descripción	Peso
			intervención de personas para su realización.	
		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 sacar el valor del riesgo residual y de esta manera poder ubicar el riesgo residual 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. Se hace seguimiento trimestral a través de los informes de gestión de los procesos. Adicionalmente se ejecutarán las actividades de revisión, validación y aprobación 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. Se hace seguimiento trimestral a través de los informes de gestión de los procesos. Adicionalmente se ejecutarán las actividades de revisión, validación y aprobación 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.

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. Adicionalmente se ejecutarán las actividades de revisión, validación y aprobación 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 propias del proceso.

Riesgo de imagen o reputacional	Baja o moderado	La CRC asumirá el riesgo y se administrará por medio de las actividades propias del proceso. También se puede reducir con acciones preventivas.

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 de gestión 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.

9.7. Nivel de severidad del riesgo

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

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 evitan.

9.8. 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 RAES 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. 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.
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: Todos los Coordinadores de los Grupos Internos de Trabajo.

c) Ante la materialización de los riesgos de gestión se debe hacer revisión inmediata de los controles, previa identificación de las causas generadoras, aplicar los planes de contingencia y reportar a la Alta Dirección y al Comité de Coordinación de Control Interno.
Responsable: Todos los Coordinadores de los Grupos Internos de Trabajo.

d) Igualmente, al identificar la materialización de los riesgos de corrupción se deben 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 Alta Dirección y al Comité de Coordinación de Control Interno y en paralelo **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: Todos los Coordinadores de los Grupos Internos de Trabajo.

e) 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

f) 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

g) La presente política debe ser publicada en la página Web de la CRC y en la Intranet. 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: Coordinación Ejecutiva 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.