COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Política de Administración de Riesgos 2025

Proceso de Seguimiento y Evaluación

Coordinación de Planeación y Gestión
Coordinador: Sandra Villabona Duque

Junio de 2025

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ÍNDICE DE TABLAS

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE LA CRC

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 Institucional, alineado con el Sistema Integrado 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), así como los ajustes de la versión 6, que incluye los conceptos relacionados con el riesgo fiscal, guías que dan lineamientos para identificación y control de los riesgos de gestión, corrupción, seguridad y privacidad de la información y fiscales.

Con la presente Política la CRC deja documentados los lineamientos de 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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Lineamientos generales que deben ser aplicados en la Entidad

La Comisión de Regulación de Comunicaciones – CRC cuenta con un Código de Integridad, el cual establece las reglas de comportamiento que deben guiar la conducta de los funcionarios de la Entidad, a través del cual se busca que sus integrantes 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.

1. 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 expedidas por el Departamento Administrativo de la Función Pública en su última versión:

- **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.
- **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.
- **Análisis de riesgo**: proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo inherente.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- **Capacidad del 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**: cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.
- **Confidencialidad**: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Contexto de la Identidad**: definición de las características o aspectos esenciales del entorno interno y externo en el cual opera la entidad.
- **Control**: medida que permite reducir o mitigar un riesgo.
- **Control Automático**: son 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.
- **Daños a activos fijos**: pérdida por daños o extravíos de activos por desastres naturales u otros eventos externos provocados por atentados, vandalismo, orden público.
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Ejecución y administración de procesos**: pérdidas derivadas de errores en la ejecución y administración de procesos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- **Factores de riesgo**: son las fuentes generadoras de riesgos.
- **Fallas tecnológicas**: errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
- **Fraude externo**: pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la Entidad).
- **Fraude interno**: pérdida debido a actos de fraude, actuaciones irregulares, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
- **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.
- **Gestión del Riesgo Fiscal**: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
- **Gestor Público**: es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales.
- **Impacto**: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad**: propiedad de exactitud y completitud.
- **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.
- **Punto de Riesgo**: actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.

- **Reducir el Riesgo**: el nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.
- **Recurso público**: para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.
- **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.
- **Riesgos para la integridad pública**: posibilidad de afectación económica o reputacional para la entidad u organización por no ejercer con integridad el servicio público debido a comportamientos y prácticas que atenten contra la moralidad administrativa o aquellas relacionadas con la corrupción, entre las que se encuentran el fraude, el soborno y la no declaración de conflictos de interés.
- **Riesgos de LA/FT/FP**: posibilidad de afectación económica o reputacional para la entidad u organización por ser utilizada, en forma directa o indirecta, como instrumento

para lavado de activos (LA), financiación del terrorismo (FE) y la proliferación de armas de destrucción masiva (FP).

- **Riesgo de seguridad digital**: posibilidad de 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.
- **Riesgo Inherente**: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel de riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo fiscal**: es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial1.
- **Riesgos tecnológicos**: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una 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.
- **SGSPI**: Sistema de Gestión de Seguridad y Privacidad de la Información.
- **Tratamiento del riesgo**: es un rol de primera línea de defensa; 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. El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.
- **Valoración del riesgo**: establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).
- **Vulnerabilidad**: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2. ESQUEMA DE LÍNEAS DE DEFENSA DE LA CRC

A partir del esquema de líneas de defensa establecido dentro del Modelo Integrado de Planeación y Gestión - Dimensión 7 Control Interno, se establecen para la CRC las responsabilidades en el marco de la Administración integral de riesgos y los componentes del Sistema de Control Interno (MECI).

Tabla 1. Esquema de Líneas de Defensa

Línea de Defensa	Integrantes	Responsabilidades y Actividades
Línea Estratégica	Alta dirección, Comité Institucional de Coordinación de Control Interno y Comité Institucional de Gestión y Desempeño. Alta Dirección: (Director Ejecutivo, Comisionados y Coordinador Ejecutivo). Comité Institucional de Coordinación de Control Interno. (Director Ejecutivo, Comisionados de Comunicaciones, Comisionados de Gestión Audiovisual y Pedagogía Regulatoria, Coordinador Ejecutivo, Coordinadores de los Grupos Internos de Trabajo y Jefe de la Oficina de Control Interno). Comité Institucional de Gestión y Desempeño. (Director Ejecutivo, Comisionados de Comunicaciones, Comisionados de Gestión Audiovisual y Pedagogía	Revisar y aprobar la política de administración del riesgo, previamente estructurada por parte de la Coordinación de Planeación y Gestión, como segunda línea de defensa en la entidad y evaluar su aplicación. La revisión se debe realizar cada vigencia y actualizar si es necesario. Analizar los riesgos y amenazas institucionales que pueden afectar el cumplimiento de los planes estratégicos. Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. Dar lineamientos, asesorar y tomar decisiones en temas de Control Interno. Articular el adecuado funcionamiento del Sistema de Control Interno en la entidad, para lo cual tendrán en cuenta los informes de la segunda y la tercera línea de defensa. Presentar el resultado de la evaluación del estado del sistema de control interno, acorde con la información generada por parte de las instancias de segunda línea identificadas y la actividad de control definida que materializa la línea de reporte en cada caso, acorde con el tema del cual son responsables, a fin de generar acciones y una toma de decisiones con enfoque preventivo. Responsable Oficina de Control Interno.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Integrantes	Responsabilidades y Actividades
	Regulatoria, Coordinador Ejecutivo, Coordinadores de los Grupos Internos de Trabajo y Jefe de la Oficina de Control Interno).	Revisar el cumplimiento de los objetivos institucionales ante el Comité Institucional de Gestión y Desempeño. 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 Tomar decisiones 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 CRC 147 de 2022. Garantizar recursos (humanos, financieros y tecnológicos) necesarios para el desarrollo de la Gestión del Riesgo.
Primera Línea	Todos los funcionarios de la entidad que ejecutan actividades como líderes de procesos, proyectos y/o actividades continuas.	Identificar, analizar, valorar, controlar, mitigar y evaluar continuamente los riesgos que pueden afectar el proceso, los programas, proyectos, planes y procedimientos a su cargo, a través del autocontrol. Para ello se debe apoyar en los puntos de control de los procedimientos. Así mismo, realizar actualización de los riesgos cuando se requiera. Ejecutar los controles de los riesgos del proceso a su cargo y hacer seguimiento continuo a los mismos. Realizar oportunamente reportes de seguimiento de los riesgos de acuerdo con las solicitudes de la segunda línea y soportar las evidencias de la operación de los controles durante el periodo. Realizar reporte inmediato a la segunda línea de defensa (Coordinación de Planeación y Gestión) de la materialización de los riesgos, de acuerdo como se indica en el presente documento. En caso de la materialización de un riesgo no identificado, este debe ser documentado e incluido en el mapa de riesgo del proceso correspondiente. Formular y ejecutar acciones correctivas para el tratamiento por la materialización de riesgos y contar con las evidencias.

Línea de Defensa	Integrantes	Responsabilidades y Actividades
		Reportar a la segunda línea de defensa en las reuniones de seguimiento de los procesos, la gestión de cada uno de los riesgos. Realizar seguimiento y verificación al cumplimiento de las metas, así como a los controles asociados a su proceso, generando los ajustes necesarios. Los servidores en general deben: Participar en el diseño de los controles que tienen a cargo. Ejecutar los controles a su cargo de la forma como están diseñados. Informar a su superior jerárquico sobre riesgos materializados o posibles situaciones de afectación al proceso, a fin de incorporar las acciones a que haya lugar. Proponer mejoras a los controles existentes. **NOTA:** El seguimiento y verificación que realizan los líderes de proceso como primera línea de defensa es a lo que se llama proceso de autocontrol y es la verificación gerencial operativa.
Segunda Línea	Las segundas líneas de defensa son cargos del nivel de la media gerencia hacia arriba, que responden por un tema transversal ante la Alta Dirección y lo evalúan de manera transversal. Hacen parte de la segunda línea de defensa: Coordinador de Planeación y Gestión. Coordinador de Gestión Administrativa y Financiera. Coordinador de Gestión Jurídica Coordinador de Diseño	Asesorar a la línea estratégica en el análisis del contexto interno y externo, para una adecuada definición de la política de administración del riesgo. Responsabilidad de la Coordinación de Planeación y Gestión cada vez que se requiera realizar ajustes. Asesorar y acompañar a la primera línea en la identificación, documentación de riesgos e implementación de la metodología de administración de riesgos de acuerdo con las directrices institucionales. Responsabilidad de la Coordinación de Planeación y Gestión y la Coordinación de Tecnologías y Sistemas de Información (riesgos del SGSPI), siempre que se requiera y cuando se den cambios en la metodología. Identificar cambios en el entorno (interno o externo) que afecten el apetito del riesgo en la entidad, para su análisis en el Comité Institucional de Coordinación de Control Interno (CICCI) y se adelanten los ajustes que correspondan a este aparte dentro de la presente política. Responsabilidad de todos los integrantes de la segunda línea de defensa.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Integrantes	Responsabilidades y Actividades
	Regulatorio. Coordinador de Gestión Audiovisual y Pedagogía Regulatoria. Coordinador de Tecnologías y Sistemas de Información. Coordinador de Relaciones con Grupos de Valor. Coordinador de Implementación Regulatoria e Innovación. Coordinador de Analítica de Datos. Coordinador de Prospectiva Estratégica -Líderes de los Sistemas (Gestión de Calidad, Gestión Ambiental, Seguridad y Salud en el Trabajo, Gestión de Seguridad y Privacidad de la Información).	Informar a la primera línea de defensa la materialización de un riesgo no identificado para que sea documentado e incluido en el mapa de riesgo institucional. La información se debe reportar desde la Coordinación de Planeación y Gestión, haciendo claridad que el riesgo materializado puede ser identificado desde cualquier responsable de la segunda línea de defensa, incluidos los riesgos fiscales, teniendo en cuenta los puntos de riesgo según catalogo anexo al presente documento. Generar recomendaciones y/o alertas con alcance preventivo a la línea estratégica, a fin de incorporar acciones inmediatas a los temas críticos identificados. Responsabilidad de la segunda línea de defensa. Asesorar y acompañar a la Alta Dirección en la incorporación de estrategias y metodologías para la gestión de riesgo, acorde con las actualizaciones en materia de riesgos de corrupción, fiscales y otros que se definan en normas nacionales. Responsabilidad de la Coordinación de Planeación y Gestión. Revisar que los controles y los planes de acción (tratamiento reducir) para la mitigación de los riesgos, estén diseñados de manera adecuada y ejecutándose continuamente; así mismo, hacer recomendaciones de mejora, seguimiento y fortalecimiento. Responsabilidad de la Coordinación de Planeación y Gestión. Realizar seguimiento trimestral a la primera línea de defensa sobre la aplicación de los controles asociados a los riesgos de cada proceso (gestión, corrupción, fiscal). Responsabilidad de la Coordinación de Planeación y Gestión. Reportar trimestralmente desde la segunda línea de defensa a la Línea Estratégica, sobre los resultados del aseguramiento, generación de alertas y presentación de recomendaciones sobre la gestión de riesgos en los procesos a su cargo a través de presentaciones que se llevan al Comité Institucional de Coordinación de Control Interno. Liderar la gestión de riesgos de seguridad y privacidad de la información en la entidad. Asimismo, asesorar a los líderes de proceso en la identificación, evaluación, clasificación y tratamiento de los riesgos de seguridad y privacidad de la información. Responsabilidad de la Coordinación de Tecnologías y Sistemas de Información.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Integrantes	Responsabilidades y Actividades
		Gestionar la atención y documentación de los incidentes de seguridad y privacidad de la información que se presenten en la CRC, teniendo en cuenta los riesgos y su relación, asimismo, realizar la propuesta de identificación de nuevos riesgos en caso de no tenerlos formalizados. Responsabilidad de la Coordinación de Tecnologías y Sistemas de Información. Presentar ante el Comité Institucional de Gestión y Desempeño un informe del análisis de los riesgos de seguridad y privacidad de la información, su comportamiento y gestión de los planes de tratamiento. Responsabilidad de la Coordinación de Tecnologías y Sistemas de Información. Proponer al Comité Institucional de Gestión y Desempeño las medidas y mecanismos para mejorar la gestión de seguridad y privacidad de la información. Responsabilidad de la Coordinación de Tecnologías y Sistemas de Información y la coordinación de Planeación y Gestión. Verificar el avance en los programas y proyectos desagregados por tema y recursos asociados a TSI, generando alertas sobre retrasos o posibles incumplimientos, a fin de tomar las acciones necesarias. El reporte se realiza para ser analizado por el Comité Institucional de Gestión y Desempeño, y definir acciones de mejora. Responsabilidad de la Coordinación de Tecnologías y Sistemas de Información. Realizar trimestralmente reportes de avances del Plan Anual de Adquisiciones, de acuerdo con cada modalidad de contratación, generando alertas frente a retrasos o posibles incumplimientos en los planes, programas o proyectos a los cuales se encuentran asociados los contratos analizados. El reporte se analiza en el Comité Institucional de Gestión y Desempeño, para definir acciones de mejora o intervenciones necesarias. Responsabilidad de la Coordinación Ejecutiva. Realizar reporte ejecutivo del Plan Institucional de Capacitación (PIC), Bienestar, Incentivos y temas de convivencia laboral, mediante un análisis de variables relacionadas con la ejecución de cada uno de estos mecanismos, que permita generar alertas en la ejecución de recursos. En el tema de convivencia generar información sobre quejas reiteradas de acoso laboral y conflictos internos que no ha sido posible resolver. Así mismo, la ejecución del Plan Institucional Estratégico de Talento Humano y cumplimiento de la política de integridad. El reporte se analiza en el Comité

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Integrantes	Responsabilidades y Actividades
		Institucional de Gestión y Desempeño para definir acciones de mejora. Responsabilidad de la Coordinación de Gestión Administrativa y Financiera. Evaluar reporte de la prestación del servicio a los grupos de valor, mediante el análisis de las PQRSD y la evaluación de percepción de los usuarios por los diferentes medios de atención, generando alertas en semáforo sobre incumplimiento en términos, reiteraciones de consultas, quejas, que se hayan presentado o que estén en curso. Se debe reportar mensualmente en caso de presentar alertas significativas que requieran análisis y toma de acciones, de lo contrario, se debe realizar reporte trimestral a la Alta Dirección. Responsabilidad de la Coordinación de Relaciones con Grupos de Valor. Verificar el seguimiento a la gestión judicial adelantada generando información sobre alertas en los procesos que se encuentran abiertos y las cuantías asociadas. Se deben reportar alertas trimestralmente para ser analizado por la Alta Dirección. Responsabilidad de la Coordinación de Gestión Jurídica Los riesgos fiscales son el efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, en este sentido, los coordinadores, ejecutores del gasto, pagadores, responsables de gestión contractual, supervisores, administradores de bienes, entre otros, deben acompañar la identificación de los posibles riesgos fiscales, teniendo en cuenta el catálogo de puntos de riesgo anexo al presente documento. Así mismo, reportar oportunamente la materialización de los riesgos fiscales identificados y no identificados. Reportar alertas en el marco de la declaración y tratamiento de conflicto de intereses. Responsabilidad de la Coordinación de Gestión Jurídica Reportar ante el Comité Institucional de Gestión y Desempeño, alertas que limiten alcanzar los objetivos y metas de los Sistemas de Calidad, Gestión Ambiental, Seguridad y Salud en el Trabajo, con la finalidad de analizar y tomar acciones oportunamente. Responsabilidad de los líderes de los diferentes Sistemas. **NOTA**: los seguimientos que realizan las segundas líneas de defensa sobre los temas transversales por los cuales responden se

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Integrantes	Responsabilidades y Actividades
		constituyen en Autoevaluación Institucional.
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, especialmente con el Coordinador de Planeación y Gestión. 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 Institucional de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. Revisar la efectividad y la aplicación de controles 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 de articular de manera efectiva los riesgos. Trabajar de manera coordinada con las segundas líneas de defensa establecidas en la entidad. Llevar a cabo la evaluación independiente a los riesgos registrados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional de Coordinación de Control Interno. Para lo anterior se tendrán en cuenta los resultados de los seguimientos aplicados por parte de la Coordinación de Planeación y Gestión, así como del Oficial de Seguridad, con el fin de contar con información de base para sus evaluaciones y generar recomendaciones a estas instancias. Generar recomendaciones y/o alertas con alcance preventivo a la línea estratégica, con el fin de incorporar acciones inmediatas a los temas críticos identificados. Presentar oportunamente ante el Comité Institucional de Coordinación de Control Interno, los resultados de la evaluación por medio del informe parametrizado semestral del Sistema de Control Interno, con la finalidad de analizar y

Línea de Defensa	Integrantes	Responsabilidades y Actividades
		tomar acciones de mejora oportunas de acuerdo con el cumplimiento programado. **NOTA:** Las actividades realizadas por la Oficina de Control Interno son de evaluación independiente a través del desarrollo de seguimientos y auditorías.

3. MARCO NORMATIVO

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

Tabla 2. 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.
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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

NORMA	DESCRIPCIÓN
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.
Ley 1581 de 2012	La Ley de Protección de Datos Personales reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
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	Este Decreto señala o establece la metodología para elaborar la estrategia de lucha contra la corrupción, entre otros, la gestión de riesgos como primer componente del Plan Anticorrupción y de Atención al Ciudadano.
Decreto 1083 de 2015	Este Decreto compila y racionaliza en un sólo cuerpo normativo los decretos reglamentarios vigentes de competencia del sector de la función pública, incluidos los atinentes a las siguientes materias entre otras: empleo público, modelo integrado de planeación y gestión, sistema de gestión de calidad y trámites.
Decreto 648 de 2017	"Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentaria Único del Sector de la Función Pública en cuanto al régimen de ingreso, administración de personal, situaciones administrativas y retiro de los empleados públicos"

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

NORMA	DESCRIPCIÓN
Decreto 1499 de 2017	Articula el Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades. Actualiza el Modelo Estándar de Control Interno para el Estado Colombiano – MECI a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG (correspondiendo a la 7° Dimensión de MIPG).
Guía para la Administración de Riesgo y el Diseño de controles en Entidades Públicas Vigente.	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 Vigente.
CONPES 3995 de 2020	La Política Nacional de Confianza y Seguridad Digital, señala el objetivo de establecer medidas para desarrollar la confianza digital a través de la mejora en la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.
Resolución 500 de 2021	Resolución expedida por el MinTIC, estableció los lineamientos y estándares para la estrategia de seguridad digital y la adopción del modelo de seguridad y privacidad, como habilitador de la política de Gobierno Digital. En consecuencia, la seguridad y privacidad de la información y el Modelo de Seguridad y Privacidad de la Información adoptado mediante el acto administrativo en mención, y las normas que lo desarrollan, son un pilar fundamental para la configuración y desarrollo del habilitador de Seguridad y Privacidad de la Información de que trata el Decreto 767 de 16 de mayo de 2022.

NORMA	DESCRIPCIÓN
Decreto 1122 de 2024	Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública.
Decreto 1600 de 2024	Por el cual se modifica el Capítulo 1 y 3 del Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, Decreto Reglamentario Único del Sector Presidencia de la República, en lo relacionado con las Subcomisiones Técnicas de la Comisión Nacional de Moralización y la Estrategia Nacional de Lucha Contra la Corrupción.

4. OBJETIVOS

4.1 Objetivo General

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

4.2. Objetivos Específicos

- Formalizar al interior de la CRC una metodología para administrar los riesgos de toda naturaleza a los que se enfrenta la entidad: gestión, corrupción, seguridad digital y fiscales.
- Establecer pautas para la identificación de los factores que representan amenazas u oportunidades para el cumplimiento de los objetivos.
- Definir los roles y responsabilidades en marco de la administración de riesgos y el Sistema de Control Interno, bajo el esquema de las líneas de Defensa en la CRC.
- Establecer desde el direccionamiento estratégico el análisis del entorno externo e interno de la entidad, que sirve de base para la identificación de los posibles riesgos, así como los factores de riesgo.

- 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 el Departamento Administrativo de la Función Pública.
- Establecer los lineamientos para el diseño de los controles.
- Establecer los seguimientos y la periodicidad que deben realizar las líneas de defensa, así como los seguimientos a los mapas de riesgos por parte de la segunda línea de defensa (Coordinación de Planeación y Gestión).
- Establecer los lineamientos para la gestión de eventos (materialización de los riesgos) su manejo, análisis conducentes a la toma de decisiones.
- Estipular las reglas para la identificación de las actividades de control que minimicen la ocurrencia e impacto de los factores de riesgo.
- Caracterizar el instrumento para la administración del riesgo de acuerdo con los requisitos establecidos en la Guía vigente para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.
- Cumplir con los principios del Modelo Integrado de Planeación y Gestión – MIPG, Modelo Estándar de Control Interno y el Sistema Integrado 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.
- Establecer responsabilidades en el marco del Sistema de Control Interno Institucional.
- Definir el ciclo metodológico de la administración de riesgos institucional.

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

La presente política aplica a todos los procesos, planes 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 Viva Engage, 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 GPR-PR-01 Diseño y Desarrollo de la Entidad.

Es de aclarar que, para los riesgos de seguridad y privacidad de la información, se siguen los criterios definidos en el Modelo de Seguridad y Privacidad de la información MSPI[1] y de la guía para la administración del riesgo y el diseño de controles en entidades públicas vigente.

6. ALINEACIÓN CON EL PLAN ESTRATÉGICO 2021-2025

La Comisión de Regulación de Comunicaciones (CRC) ha definido el siguiente Plan Estratégico Institucional para el periodo 2025–2029, el cual orienta su gestión y constituye el marco de referencia para el fortalecimiento del Sistema de Control Interno:

Propósito Superior

Dinamizar los mercados de servicios de comunicaciones, promoviendo su eficiencia, pluralidad e innovación, para impulsar el bienestar y el desarrollo de los colombianos.

Misión

Promover la competencia, la inversión, el pluralismo informativo y la protección de los derechos de los usuarios y audiencias[2] en los mercados de servicios de comunicaciones, evitando el abuso de posición dominante, para que los servicios sean económicamente eficientes y reflejen altos niveles de calidad.

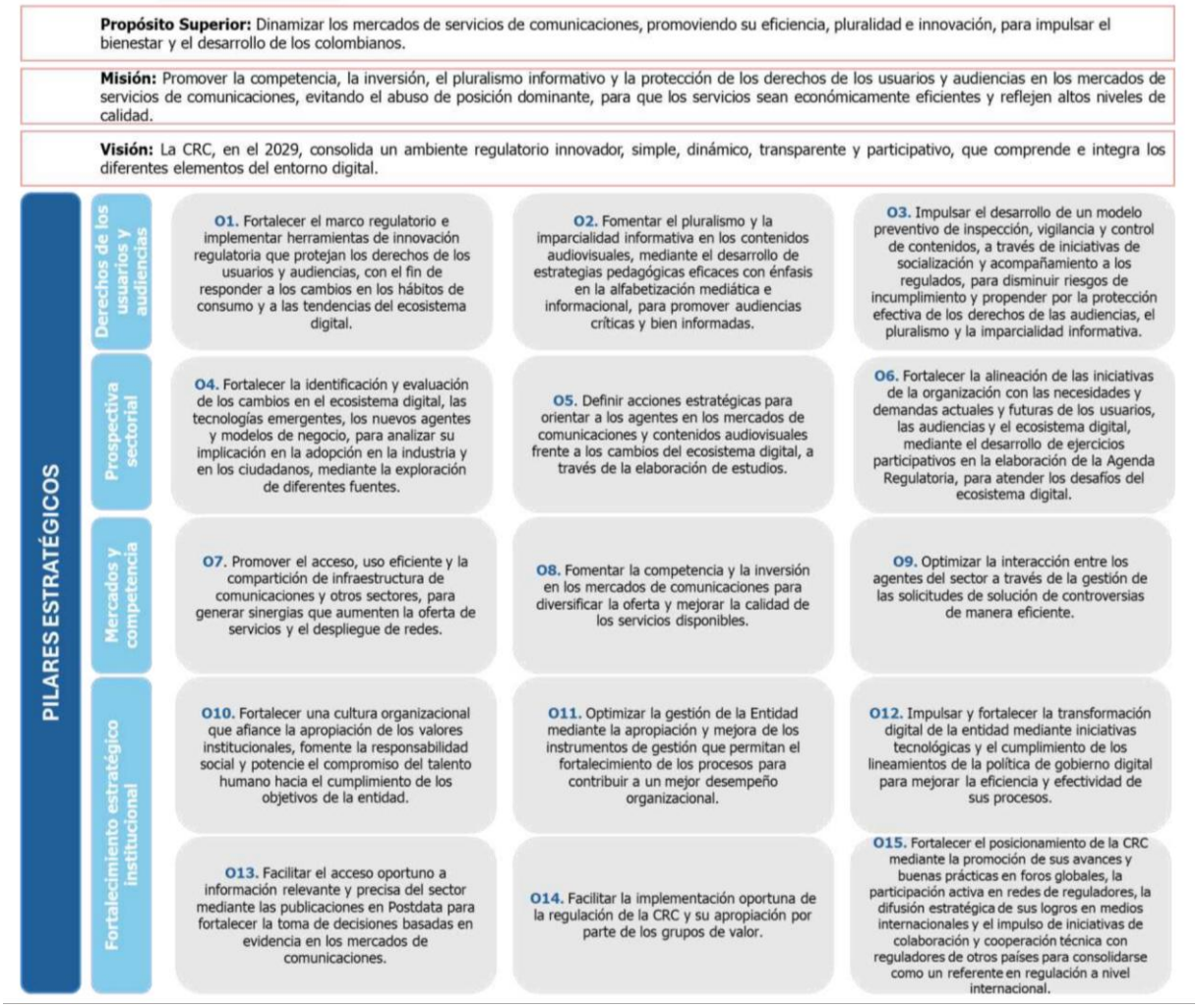
Visión

La CRC, en el 2029, consolida un ambiente regulatorio innovador, simple, dinámico, transparente y participativo, que comprende e integra los diferentes elementos del entorno digital.

[1] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
[2] Audiencias: entendida como un grupo de personas que hacen parte de los receptores de un mensaje transmitido, a través de un medio de comunicación masiva y que, en su papel de ciudadanos tienen la posibilidad de interactuar con el medio.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Mapa Estratégico CRC 2025 – 2029

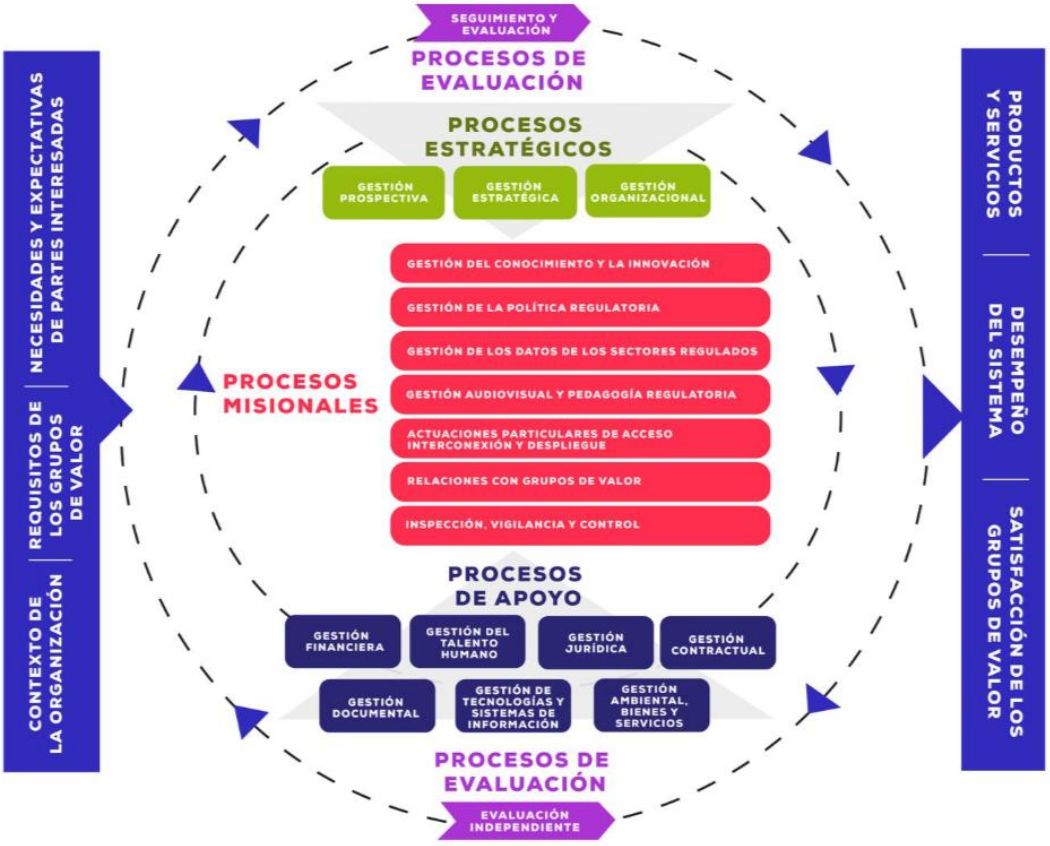


Fuente: Elaboración propia CRC.

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 institucional, así como con el Sistema Integrado de Gestión, el cual está conformado 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



Fuente: Elaboración propia CRC.

Se identifican riesgos de gestión para cada uno de los procesos establecidos para el Sistema Integrado 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 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. Adicionalmente, la línea estratégica define la gestión del riesgo con la aprobación de la presente Política, en el Comité Institucional de Coordinación de Control Interno.

7. FACTORES DE RIESGO

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 actualmente en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, teniendo en cuenta que estos criterios continúan vigentes y son pauta para establecer el contexto en la identificación de los riesgos:

7.1 Contexto Externo

- **Económicos**: disponibilidad de capital,liquidez, mercados financieros, desempleo, competencia.
- **Políticos**: cambios de gobierno, legislación, políticas públicas, regulación.
- **Sociales**: demografía, responsabilidad social, orden público, 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 Integrado de Gestión (Este criterio se incluye como recomendación del Departamento Administrativo de la Función Pública – DAFP resultados FURAG 2021).
- **Evento externo**: situaciones externas que afectan la entidad.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.2 Contexto Interno

- **Financieros**: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
- **Personal**: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
- **Procesos**: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
- **Tecnología**: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
- **Estratégicos**: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
- **Comunicación Interna**: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
- **Auditorías Internas**: evaluaciones llevadas a cabo por la Oficina de Control Interno y resultados de las auditorías internas al Sistema Integrado de Gestión.
- **Talento Humano**: se analiza posible dolo e intención frente a la corrupción (hurto de activos, posibles comportamientos no éticos, fraude interno de corrupción o soborno).

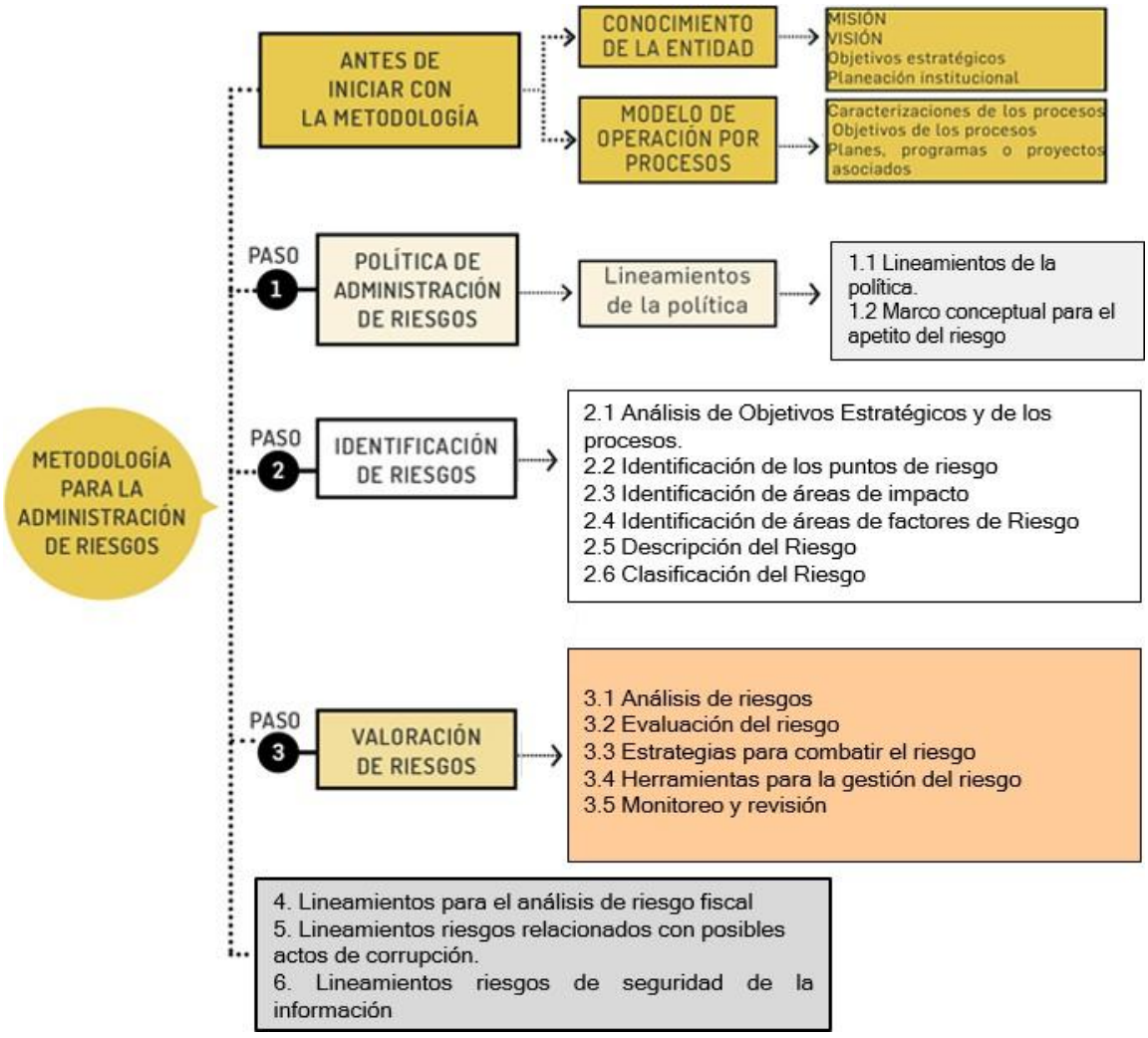
8. METODOLOGÍA DE GESTIÓN DE RIESGOS EN LA CRC

La metodología de administración de riesgos en la CRC se ha diseñado según las especificaciones contenidas en la Guía para la Administración del Riesgo Vigente. 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 6, noviembre de 2022.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Metodología para la administración del riesgo



Fuente: Guía de Administración del Riesgo, DAFP. Versión 6. 2022.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

8.1 Ciclo Metodológico de Administración de riesgos de la CRC.

Fuente: Elaboración propia CRC

(Fase Previa) Análisis de Contexto Estratégico: antes de iniciar con la aplicación de la metodología, se debe realizar un análisis del contexto estratégico institucional. Cada proceso debe identificar su alineación con la misión, visión y objetivos estratégicos de la Entidad, así como los factores internos y externos que puedan impactar la gestión, incluyendo sus causas y consecuencias. Esta fase proporciona los insumos necesarios para una identificación adecuada de los riesgos.

1. **Política de Administración de Riesgos**: es la directriz a nivel institucional que contempla la adaptación de los lineamientos externos en marco de la metodología de administración de riesgos, la política se debe revisar cada vigencia y actualizarse si es necesario, y su revisión y aprobación se realiza en el Comité Institucional de Coordinación de Control Interno. Debe ser publicada y socializada a los colaboradores de la entidad.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2. **Identificación de los Riesgos**: se realiza la identificación de puntos de riesgo y se describe el de acuerdo con la metodología y clase. Así mismo se determina la clasificación de este.

3. **Análisis de los Riesgos**: en esta fase se realiza tanto análisis de probabilidad como del impacto, de acuerdo con las tablas contempladas en la política de administración de riesgos institucional, a partir de este análisis se obtiene el nivel de riesgo inherente.

4. **Documentación y aplicación de controles**: en esta fase se establecen controles que permiten mitigar el riesgo. Los controles deben ser documentados de acuerdo con la estructura que se contempla en la política de administración de riesgos.

5. **Evaluación y Valoración de los Riesgos**: una vez identificados los controles se debe establecer la tipología del control y valorar los atributos de cada control, como se orienta en la política de administración de riesgos, obteniendo como resultado el nivel de Riesgo Residual.

6. **Manejo de los Riesgos**: el manejo del riesgo se establece de acuerdo con las opciones de tratamiento y los niveles de aceptación de riesgo contemplados en la política de administración de riesgos institucionales, teniendo en cuenta que los riesgos de corrupción no se aceptan.

7. **Seguimiento de los riesgos**: el seguimiento de los riesgos se debe realizar a partir de las responsabilidades de la primera línea de defensa, donde permanentemente los responsables de los riesgos deben realizar monitoreo y seguimiento a la adecuada operación de los controles de cada proceso. Así mismo, los responsables de los riesgos deben reportar trimestralmente el seguimiento de acuerdo con la solicitud realizada por parte de la segunda línea de defensa (Coordinación de Planeación y Gestión), los reportes se deben realizar de manera detallada y con las evidencias de las actividades que permiten evidenciar la adecuada operación de los controles. La Coordinación de Planeación y Gestión realiza informe y remite a la línea estratégica.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

8. **Evaluación de Riesgos**: la evaluación de los riesgos es realizada por la Oficina de Control Interno y por la línea estratégica de acuerdo con los reportes y alertas emitidas desde la segunda línea de defensa.

9. **Cierre de vigencia de los riesgos**: el cierre de vigencia de los riesgos consiste en realizar una revisión por parte del responsable del riesgo y determinar si se mantiene para la próxima vigencia, si los controles han operado con normalidad, si se actualiza, si las acciones de tratamiento se han ejecutado, si los niveles de valoración inherente y residual cambian. Este paso del ciclo permite realizar desde la primera línea de defensa revisión de la pertinencia del riesgo y realizar ajustes oportunos de acuerdo con la trazabilidad de la gestión del riesgo.

9. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

9.1 Identificación de los riesgos

Para la identificación general de los riesgos de gestión, corrupción, fiscal y de seguridad y privacidad de la información, 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.

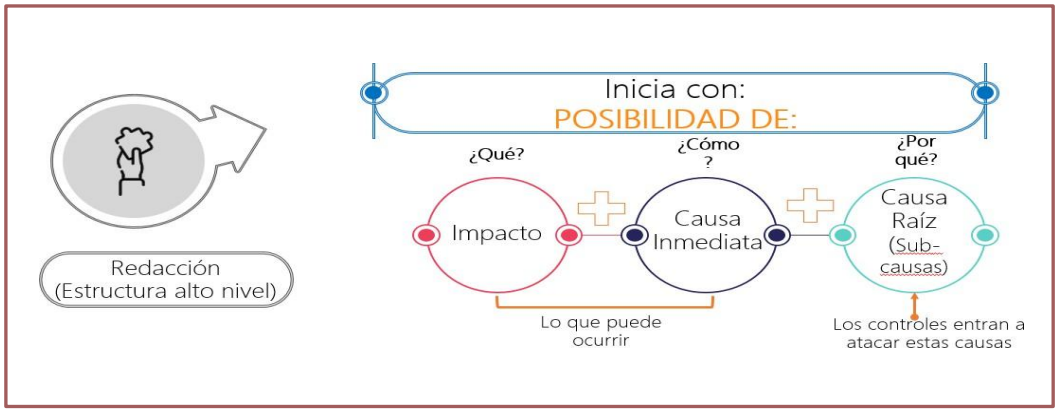
Se deben identificar las fuentes generadoras del riesgo, es decir, las causas del riesgo, para ello se deben utilizar preguntas de referencia: ¿cómo puede suceder?, ¿por qué puede suceder? y, posteriormente identificar ¿qué consecuencias tendría su materialización?

Asimismo, se debe incluir la descripción del riesgo que contenga todos los detalles necesarios para que se pueda entender, y 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?).

9.1.1 Identificación de riesgo de gestión y riesgo fiscal

Para la descripción de riesgos de gestión, se debe realizar de acuerdo con la siguiente estructura metodológica:

Fuente: Función Pública - Presentación Gestión de Riesgo DAFP



De acuerdo con la estructura anterior, se describen los elementos a tener en cuenta:

Impacto: son las consecuencias que puede ocasionar a la organización la materialización del riesgo. Para los riesgos de gestión se basa considerando la pérdida reputacional y/o la afectación económica y presupuestal. Para el riesgo fiscal corresponde al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Para en riesgo fiscal se denomina **circunstancia inmediata** que corresponde al cómo y, se refiere a aquella situación por la que se presenta el riesgo, pero no constituye la causa principal o causa raíz para que se presente el riesgo.

Causa raíz: es la causa principal o básica y, corresponde a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o subcausas que pueden ser analizadas. Para el riesgo fiscal, corresponde al evento de acción u omisión que de presentarse es el causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

Ejemplo de Riesgo de Gestión:

Fuente: Función Pública – Presentación Gestión de Riesgo DAFP

Ejemplo de Riesgo Fiscal:

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	A causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Fuente: Función Pública – Presentación Gestión de Riesgo DAFP

Se anexa al presente documento el "CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS" diseñado por el Departamento Administrativo de Función Pública, que permitirá ser referente y orientador en la identificación y documentación de riesgos fiscales.

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.

9.1.2 Identificación de riesgo de corrupción

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Es necesario que la descripción del riesgo sea clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio del privado.

Descripción del Riesgo	Acción u Omisión	Uso es poder	Desviar la gestión de lo publico	Beneficio Privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato	X	X	X	X

De acuerdo con el ejemplo anterior, de marcarse con una X todos los componentes, quiere decir que se trata de un riesgo de corrupción.

9.1.3 Identificación de riesgo en el marco del Programa de Transparencia y Ética Pública (PTEP) – Decreto 1122 de 2024.

En el marco del Programa de Transparencia y Ética Pública (PTEP), los riesgos deben ser gestionados de forma proactiva, permitiendo a la entidad anticiparse a situaciones que puedan comprometer la ética pública, la confianza ciudadana y el uso adecuado de los recursos públicos.

Se entiende por riesgo la posibilidad de que ocurra un evento que impacte negativamente el cumplimiento de los objetivos institucionales, la integridad pública, la transparencia, la legalidad o la gestión de los recursos del Estado.

La identificación de estos riesgos implica describir con claridad y precisión los eventos que podrían materializarse, generando afectaciones económicas, reputacionales o legales. Su gestión abarca la definición de controles, responsables, acciones de mitigación y el seguimiento permanente.

De acuerdo con el Anexo Técnico del Decreto 1122 de 2024, las entidades deben identificar y gestionar, los siguientes tipos de riesgo:

- Riesgos para la integridad pública: Gestionar la posibilidad de afectación económica o reputacional para la entidad por no ejercer con integridad el servicio público debido a comportamientos y prácticas que atenten contra la moralidad administrativa o aquellas relacionadas con la corrupción, entre las que se encuentran el fraude, el soborno y la no declaración de conflictos de interés.

- Riesgos de LA/FT/FPA: Gestionar la posibilidad de afectación económica o reputacional para la entidad u organización por ser utilizada, en forma directa o indirecta, como instrumento para lavado de activos (LA), financiación del terrorismo (FE) y la proliferación de armas de destrucción masiva (FP).

- Riesgos por canales de denuncia inadecuados: Controlar los riesgos para la integridad pública y de LA/FT/FP mediante un canal institucional de denuncias que garantice el tratamiento de los reportes recibidos y la protección del denunciante.

- Riesgos por debida diligencia insuficiente: Controlar los riesgos para la integridad pública y de LA/FT/FP mediante procesos de debida diligencia que permitan el conocimiento de la contraparte con la que se está relacionando la entidad u organización.

9.1.4 Identificación de riesgo de Seguridad y Privacidad de la Información

Para identificar 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) + la combinación entre Vulnerabilidad(es) y 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 6, 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**: pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la Entidad).
c. Fraude interno: pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
d. **Fallas tecnológicas**: errores de hardware, software, interrupción de servicios.
e. **Relaciones laborales**: pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
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.

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**.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Determinar la Probabilidad: para riesgos de gestión, fiscal y seguridad y privacidad de la información, 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:

Tabla 3. Calificación de probabilidad riesgos de gestión y fiscal

	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 6. 2022

Para los riesgos de seguridad y privacidad de la información , se tendrán en cuenta los siguientes criterios para medir la probabilidad, los cuales tendrán en cuenta los factores históricos, a través del conocimiento adquirido en la gestión de incidentes de seguridad de la información de los últimos cinco (5) años y la prospectiva en los casos que no se tenga información previa, para este caso, se requiere del conocimiento de los colaboradores responsables de los activos de información asociados a los riesgos, el contexto interno y externo:

Tabla 4. Calificación de Probabilidad riesgos de seguridad Digital

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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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:

Para los riesgos de gestión, fiscal y seguridad y privacidad de la información, 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:

Tabla 5. Calificación de impacto riesgos de gestión y fiscal

Fuente: Guía de Administración de Riesgos. DAFP. Versión 6. 2022

	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

Para los riesgos de seguridad y privacidad de la información, se tendrán en cuenta las siguientes variables para valorar el impacto, las cuales se han dividido en cuantitativas y cualitativas de acuerdo con las principales consecuencias que se tienen cuando se materializa

un riesgo. Debido a la variedad en las tipologías de activos de información, se puede presentar una o varias:

Tabla 6. Calificación de impacto de riesgos de seguridad y privacidad de la información

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.
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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Nivel	Descriptor	Consecuencias Cuantitativas	Consecuencias Cualitativas
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. • 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.

Determinar la Probabilidad de Riesgos de Corrupción

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia se refiere al número de eventos en un periodo determinado. Se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Factibilidad implica analizar la presencia de factores internos y externos que pueden proporcionar el riesgo. Se trata de un hecho que no se ha presentado, pero es posible que suceda.

Tabla 7. Calificación de probabilidad y frecuencia para riesgos de corrupción

NIVEL	ESCALA	DESCRIPCIÓN	FRECUENCIA
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento	Al menos una vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos cinco años.
1	Rara vez	El evento puede Ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.

Tabla 8. Calificación probabilidad factibilidad para riesgos de corrupción

NIVEL	ESCALA	FACTIBILIDAD	APLICACIÓN
1	Rara Vez	Excepcionalmente Ocurriría	Nada Común o frecuente
2	Improbable	Alguna vez podría ocurrir	Difícil o poco probable que ocurra
3	Posible	Existe una posibilidad media que suceda	Existe la posibilidad de ocurrencia
4	Probable	Existe una alta posibilidad que suceda	Muy probable que ocurra
5	Casi Seguro	Es seguro que suceda	Es muy seguro que se presente

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 los cuales se mantienen en la Versión 6 y se debe dar respuesta a las siguientes preguntas:

Tabla 9. Preguntas calificación impacto riesgo de corrupción

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

Fuente: Guía de Administración de Riesgos. DAFP. Versión 4 - 2018 y versión 6 - 2022

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

Tabla 10. Calificación impacto riesgo de corrupción

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 6. 2022

Determinar el nivel del Riesgo

Luego de realizar la identificación de la probabilidad y el impacto de cada riesgo, se deberá determinar el valor o criticidad de cada riesgo haciendo un cruce entre los valores

seleccionados para ubicarlo en el mapa de calor institucional, para de esta forma determinar el tratamiento según su severidad.

Probabilidad	Insignificante (1)	Menor (2)	Moderado (3)	Alto (4)	Catastrófico (5)
Casi Seguro (5)	15	16	23	24	25
Probable (4)	9	13	14	21	22
Posible (3)	5	8	12	19	20
Improbable (2)	3	4	7	11	18
Rara vez (1)	1	2	6	10	17

Impacto

Fuente: Elaboración propia CRC

9.4 Evaluación del Riesgo:

La evaluación es la etapa en la cual se identifican los controles que permiten reducir o mitigar el riesgo por parte del responsable de cada proceso y su equipo de trabajo. Conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo.

9.4.1 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.

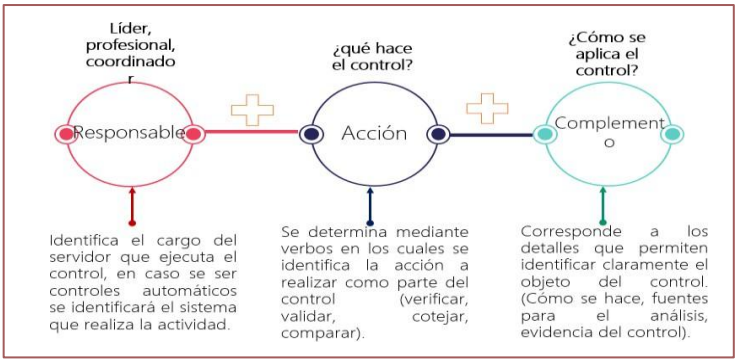
Adicionalmente, los controles según la forma como se realizan se clasifican en:

Control manual: son controles ejecutados por personas.

Control automático: son ejecutados por un sistema.

Estructura para la documentación de controles

Para una adecuada redacción del control se debe tener en cuenta la siguiente estructura:



Fuente: Función Pública - Presentación Gestión de Riesgo DAFP

Ejemplo de redacción de control

El profesional de contratación verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Valoración de controles según atributos

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

Eficiencia

Tabla 11. Valoración de atributos de controles – eficiencia

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación	Automático	25%
	Manual	15%

Fuente: Guía de Administración de Riesgos. DAFP. Versión 6. 2022

Atributos Informativos

Tabla 12. Valoración de atributos de controles - informativos

Formalización del Control	
Documentación	Procedimientos
	Otros esquemas
Frecuencia (adecuada para detectar o prevenir el riesgo)	Continua
	Aleatoria
Evidencia (trazabilidad de la ejecución)	Con Registro físico manual
	Con Registro electrónico
Ejecución	Interna
(Fuentes de información que sean confiables)	Externa
	Mixta

Fuente: Guía de Administración de Riesgos. DAFP. Versión 6. 2022

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 de riesgos y diseño de controles para entidades públicas DAFP. Versión 6).

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

NOTA: Para los riesgos de seguridad y privacidad de la información, se tendrá en cuenta la parametrización de la herramienta definida para tal fin en cuanto a los controles, su valoración y alineación con el Anexo A de la NTC-ISO/IEC 27001.

9.5 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, de acuerdo con lo establecido en la guía de Administración de riesgos y diseño de controles para entidades públicas, en su versión vigente "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: De acuerdo con lo establecido en la guía de Administración de riesgos y diseño de controles para entidades públicas, en su versión vigente "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: De acuerdo con lo establecido en la guía de Administración de riesgos y diseño de controles para entidades públicas, en su versión vigente "Se abandonan las actividades que dan lugar al riesgo, es decir no iniciar o no continuar con la actividad que lo provoca". Para la CRC no se aplicará la estrategia de Evitar para mitigar el riesgo

Compartir el riesgo: De acuerdo con lo establecido en la Administración de riesgos y diseño de controles para entidades públicas, en su versión vigente "se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad". Para la CRC no se aplicará la estrategia de compartir para mitigar los riesgos identificados en los procesos. Solo aplicará en caso de identificar riesgos institucionales de responsabilidad compartida.

9.6 Tratamiento según nivel severidad del riesgo

La Comisión de Regulación de Comunicaciones, determina que, para los riesgos residuales de gestión y fiscal, acepta el riesgo y no se requiere documentar plan de acción. Sin embargo, se debe realizar seguimiento permanente por parte del responsable del riesgo y trimestralmente por parte de la segunda línea de defensa.

Tabla 13. Tratamiento de riesgos de gestión y fiscales

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

Fuente: Elaboración propia CRC.

NOTA: Para los riesgos de seguridad y privacidad de la información en el nivel moderado se deberán tratar o reducir, no se pueden aceptar.

Para los riesgos de corrupción la tolerancia es inaceptable.

Para los riesgos de seguridad y privacidad de la información, se aceptan los riesgos que en su nivel residual se encuentre en bajo, los niveles moderado, alto y catastrófico después de controles, se deben tomar acciones que permitan fortalecer los controles.

Tabla 14. Tratamiento de riesgos de seguridad y privacidad de la información

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

Fuente: Elaboración propia CRC.

9.7 Seguimiento de la gestión de riesgos de la CRC

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

De acuerdo con el ciclo metodológico de la administración de riesgos institucional, anualmente se realiza un cierre de vigencia de los riesgos, que consiste en realizar una revisión de los riesgos documentados, determinar si se mantiene, si se ajusta y se requiere identificar nuevos riesgos. Esta actividad la debe realizar el responsable del riesgo (primera línea de defensa) de acuerdo con plazos establecidos para la actualización y publicación del mapa de riesgos de Corrupción, para realizar esta actividad se deben tomar como insumo las auditorías realizadas por la Oficina de Control Interno y Organismos de Control, así como lo reportado en las diferentes Reuniones de Análisis Estratégico -RAE e informes de desempeño presentados por los diferentes procesos. Para el desarrollo de esta actividad se realizará de manera conjunta por los equipos de trabajo y los coordinadores de los diferentes Grupos Internos de Trabajo. Una vez el Coordinador responsable remita la información de cierre de vigencia y los riesgos ajustados (si aplica), el Asesor del Sistema Integrado de Gestión como parte de la segunda línea de defensa debe realizar revisión metodológica y consolidar el mapa de riesgos.

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 y Gestión 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 Integrado de Gestión, quien debe diligenciar el cuadro maestro de registro de control de cambios de los documentos del Sistema Integrado de Gestión. No obstante, en el presente documento se comenzará a registrar el control de cambios para mayor facilidad en la identificación de la trazabilidad del documento.

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

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

a. El seguimiento se realizará trimestralmente así: reporte del estado de los controles de los riesgos a través del formato establecido en el manual de Líneas de Defensa, documento que deberá anexarse a los informes de desempeño de cada Grupo Interno de Trabajo con los resultados del periodo.
   Responsable: cada uno de los Coordinadores de los Grupos Internos de Trabajo en su rol de segunda línea de defensa.

b. Ante los eventos (materialización) de los riesgos de gestión, la primera línea de defensa debe hacer revisión inmediata de los controles, previa identificación de las causas generadoras, aplicar los planes de contingencia y reportar a la línea estratégica a través del Comité Institucional de Coordinación de Control Interno.

   NOTA: para la materialización de los riesgos de seguridad digital o de la información, se tratarán como incidentes de seguridad y privacidad de la información y se deberán informar al Coordinador de Tecnologías y Sistemas de Información o al Oficial de seguridad y privacidad de la información. Igualmente, les aplica los reportes establecidos en el manual de líneas de defensa.

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

c. Igualmente, al identificar los eventos (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.

d. Ante los eventos (materialización) de riesgos no identificados en el ejercicio, se debe determinar el proceso al que pertenece, incluir en el mapa de riesgos y surtir todas las etapas de identificación, valoración, diseño de controles, calificación de los controles y establecimiento del riesgo residual, así como la periodicidad de su seguimiento.
Responsable: primera línea de defensa responsable de la gestión del riesgo, coordinador de Planeación y Gestión y líder del proceso donde se presentó el evento.

e. Desde el grupo interno de trabajo de Planeación y Gestión, como segunda línea de defensa, se deben 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 Integrado 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 y Gestión.

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 y Gestión 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 internos de trabajo de Planeación y Gestión y Relaciones con Grupos de Valor.

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 SEV-PR-06 "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 de 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.

9.8 Reporte de eventos de materialización de Riesgos

Los riesgos materializados deben ser reportados inmediatamente por el responsable del riesgo. El reporte se debe hacer a la segunda línea de defensa. En caso de riesgos de gestión, corrupción y fiscales a la Coordinación de Planeación y Gestión y los riesgos de seguridad y privacidad de la información a la Coordinación de Tecnologías y Sistemas de Información. En caso de ser un riesgo materializado se debe reportar a la Coordinación de Planeación y Gestión, con la finalidad de orientar su documentación del riesgo con la dependencia responsable.

El reporte de la materialización se debe realizar en el mecanismo dispuesto para este fin, donde se debe describir de manera completa y clara la siguiente información.

1. Riesgo materializado
2. Fecha de materialización
3. Descripción de la materialización
4. ¿Qué causó la materialización?
5. ¿Qué controles no fueron efectivos para evitar la materialización del riesgo?
6. ¿Qué impacto genera para el proceso y/o entidad, la materialización del riesgo?
7. ¿Qué acciones correctivas se van a realizar para mitigar la materialización?

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

10. ANEXO

Este anexo es tomado de las herramientas proporcionadas por el Departamento Administrativo de Función Pública, para la implementación de la metodología de Administración de riesgo.

CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS

Introducción

Como resultado de la metodología de investigación que ha venido implementando el Semillero de Investigación de la Academia de la Gestión Pública desde el año 2018, fue posible identificar los principales puntos de riesgo fiscal y circunstancias inmediatas de dichos riesgos, mediante el estudio de: i) los avances que los diferentes órganos de control tienen frente a la definición de riesgo fiscal y la identificación de los principales riesgos fiscales en sus sujetos vigilados, ii) el estudio de fallos con responsabilidad fiscal en firme, emitidos tanto por contralorías territoriales como por la Contraloría General de la República.

Así las cosas, los puntos de riesgo fiscal que se enuncian en este catálogo indicativo y enunciativo corresponden a actividades que representan gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública y que potencialmente pueden generar un efecto dañoso al patrimonio público.

Este listado enunciativo y no restrictivo, y posibilita identificar y conocer las Circunstancias Inmediatas más comunes en la gestión pública, que se derivan de los Puntos de Riesgo Fiscal. Como resultado del análisis de más de 130 fallos con responsabilidad fiscal tanto de contralorías territoriales como de la Contraloría General de la República, fue posible identificar 50 puntos de riesgo fiscal e igual número de circunstancias inmediatas, así:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Id Referencia	**Puntos de Riesgo Fiscal** Actividad en la que potencialmente se origina el riesgo fiscal	**Circunstancia Inmediata** Situación **por la que** se presenta el riesgo
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Id Referencia	**Puntos de Riesgo Fiscal** Actividad en la que potencialmente se origina el riesgo fiscal	**Circunstancia Inmediata** Situación **por la que** se presenta el riesgo
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron
19	Suscripción de contratos	No incluir en el contrato de seguros - amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Id Referencia	**Puntos de Riesgo Fiscal** Actividad en la que potencialmente se origina el riesgo fiscal	**Circunstancia Inmediata** Situación **por la que** se presenta el riesgo
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
44	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
45	Predios adquiridos	Adquisición de predios sin las

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Id Referencia	Puntos de Riesgo Fiscal Actividad en la que potencialmente se origina el riesgo fiscal	Circunstancia Inmediata Situación **por la que** se presenta el riesgo
		especificaciones técnicas requeridas
46	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
47	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
50	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
51	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional DAFP. 2022[4]

[4] Este catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias Inmediatas, es el resultado del análisis de investigaciones previas y del estudio detallado de información sobre:
(i) Fallos con responsabilidad fiscal, en firme, emitidos en los últimos 3 años, por una muestra de 10 de las contralorías territoriales mejor calificadas en 2020, según el criterio de desempeño integral, el cual corresponde a evaluación realizada por la Auditoría General de la República.
(ii) Muestra aleatoria de fallos con responsabilidad fiscal, en firme, emitidos por la Contraloría General de la República en los últimos 3 años.
(iii) Listado de hallazgos fiscales por temáticas, consolidado por la Auditoría General de la República, 2021.