COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Política para la Gestión Integral de Riesgos de la CRC

Proceso de Seguimiento y Evaluación

Coordinación de Planeación y Gestión
Coordinadora: Diana Wilches (E)

Mayo de 2026

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS DE LA CRC

INTRODUCCIÓN

Para la COMISIÓN DE REGULACIÓN DE COMUNICACIONES – CRC, la gestión integral de riesgos constituye una herramienta gerencial estratégica para asegurar el cumplimiento de su misión institucional y el desarrollo de sus funciones mediante el logro de los objetivos definidos en el Plan Estratégico Institucional, en articulación con el Sistema Integrado de Gestión y el Modelo Integrado de Planeación y Gestión – MIPG.

Los riesgos se entienden como la posibilidad de ocurrencia de situaciones que pueden afectar el normal desarrollo de los procesos y comprometer el cumplimiento de los objetivos estratégicos. En este contexto, la CRC adopta un enfoque integral para la identificación, análisis, valoración, tratamiento, monitoreo y mejora continua de los riesgos, así como para el diseño, implementación, seguimiento y evaluación de la efectividad de los controles, incorporando los lineamientos de la dimensión de Direccionamiento Estratégico y Planeación y de la dimensión de Control Interno del MIPG.

Para garantizar la continuidad y fortalecimiento de la gestión institucional, se establecen criterios orientadores para el tratamiento de los riesgos identificados, con el propósito de mitigar sus posibles efectos, reducir la probabilidad de materialización y minimizar su impacto, contribuyendo al cumplimiento de los objetivos institucionales y al adecuado uso de los recursos públicos.

La presente política define los lineamientos de la Alta Dirección para la gestión integral de los riesgos institucionales en todos los niveles de la Entidad, integrando su administración al esquema de Líneas de Defensa y al Sistema de Control Interno, con el fin de fortalecer la

cultura de control, promover la gestión preventiva y asegurar el monitoreo permanente y la evaluación independiente.

Esta política se encuentra alineada con la Guía Gestión Integral del Riesgo – Versión 7, expedida por el Departamento Administrativo de la Función Pública, así como con los principios establecidos en el estándar ISO 31000:2018, integrando las categorías de riesgos de gestión, fiscales, integridad pública y de seguridad y privacidad de la información.

Con la presente política, la CRC documenta el marco institucional para la gestión integral de riesgos, consolidando la orientación estratégica y el desarrollo metodológico necesario para fortalecer el Sistema de Control Interno, promover la mejora continua y garantizar su adecuada divulgación y apropiación por parte de funcionarios y contratistas.

1. OBJETIVOS

1.1 Objetivo General

Establecer los lineamientos institucionales para la gestión integral de riesgos en la Comisión de Regulación de Comunicaciones – CRC, orientando la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales, contribuyendo al fortalecimiento del Sistema de Control Interno y a la mejora continua de la gestión institucional.

1.2 Objetivos Específicos

- Promover la gestión integral de riesgos en los procesos, planes, programas y proyectos de la Comisión de Regulación de Comunicaciones – CRC.
- Establecer los lineamientos institucionales para la identificación, análisis, valoración, tratamiento, monitoreo y comunicación de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales.

- Definir los roles y responsabilidades para la gestión de riesgos, en articulación con el Sistema de Control Interno, bajo el esquema de las líneas de Defensa en la CRC.
- Orientar el análisis del contexto interno y externo de la Entidad como base para la identificación y gestión de los riesgos.
- Establecer las escalas y criterios de valoración para determinar la probabilidad de ocurrencia y el impacto de los riesgos identificados, de acuerdo con la metodología definida por el Departamento Administrativo de la Función Pública.
- Definir lineamientos para el diseño e implementación de controles que permitan prevenir, mitigar o reducir la materialización de los riesgos.
- Establecer mecanismos de seguimiento, monitoreo y reporte de los riesgos institucionales, que permitan apoyar la toma de decisiones y fortalecer la gestión institucional.

2. ALCANCE DE LA POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS EN LA CRC.

La presente política aplica a todos los procesos, planes y proyectos y actividades desarrollados por la Comisión de Regulación de Comunicaciones - CRC, así como a las actuaciones realizadas por los funcionarios y contratistas durante el ejercicio de sus funciones u obligaciones.

La gestión integral de riesgos deberá ser aplicada en todos los niveles de la Entidad, como parte del Sistema de Control Interno y del Sistema Integrado de Gestión, con el fin de contribuir al cumplimiento de los objetivos institucionales.

De acuerdo con la naturaleza de la Entidad, el alcance de la política también considera aquellos riesgos derivados de actividades desarrolladas a través de terceros, convenios interinstitucionales o relaciones con actores externos, cuando estas puedan afectar el cumplimiento de los objetivos institucionales o la adecuada prestación del servicio.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

3. MARCO NORMATIVO

La gestión integral de riesgos en la Comisión de Regulación de Comunicaciones – CRC se fundamenta en el siguiente marco normativo:

Tabla 1. 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. Define los objetivos del Sistema de Control Interno, entre ellos proteger los recursos de la organización y establecer medidas para prevenir riesgos que puedan afectar el cumplimiento de los objetivos institucionales.
Ley 489 de 1998	Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Establece el Sistema Nacional de Control Interno y la responsabilidad de las entidades públicas en la implementación de mecanismos de control para el cumplimiento de sus objetivos.
Ley 1474 de 2011	Estatuto Anticorrupción. Establece disposiciones orientadas a prevenir, investigar y sancionar actos de corrupción en las entidades públicas. En su artículo 73, modificado por la Ley 2195 de 2022, establece la obligación de implementar estrategias para la prevención de la corrupción y la promoción de la transparencia, incluyendo la gestión de riesgos de corrupción en las entidades públicas.
Decreto 4637 de 2011	Crea la Secretaría de Transparencia en el Departamento Administrativo de la Presidencia de la República, encargada de apoyar el diseño e implementación de políticas y estrategias para la prevención y lucha contra la corrupción.
Ley 1581 de 2012	Establece disposiciones generales para la protección de datos personales y reconoce el derecho de las personas a conocer, actualizar y rectificar las informaciones que repose en bases de datos

NORMA	DESCRIPCIÓN
	o archivos administrados por entidades públicas o privadas.
Decreto 1649 de 2014	Define las funciones de la Secretaría de Transparencia, entre ellas señalar metodologías para diseñar y hacer seguimiento a las estrategias de lucha contra la corrupción y de atención al ciudadano en las entidades públicas.
Decreto 1081 de 2015	Decreto Único Reglamentario del Sector Presidencia de la República, que establece disposiciones relacionadas con las estrategias de lucha contra la corrupción, la transparencia y la gestión de riesgos en las entidades públicas. Este decreto desarrolla, entre otros aspectos, los lineamientos para la formulación de estrategias institucionales orientadas a prevenir la corrupción, posteriormente fortalecidas mediante los Programas de Transparencia y Ética Pública reglamentados por el Decreto 1122 de 2024.
Decreto 1083 de 2015	Decreto Único Reglamentario del Sector de Función Pública. Compila las disposiciones relacionadas con el empleo público, el Modelo Integrado de Planeación y Gestión – MIPG y el Sistema de Control Interno en las entidades públicas.
Decreto 648 de 2017	Modifica y adiciona el Decreto 1083 de 2015 en aspectos relacionados con la administración del talento humano en el sector público y fortalece el rol de las Oficinas de Control Interno dentro del Sistema de Control Interno.
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).

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

NORMA	DESCRIPCIÓN
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital, que establece lineamientos para fortalecer la seguridad digital y la gestión de riesgos asociados a tecnologías de la información en las entidades públicas.
Resolución 500 de 2021	Establece lineamientos y estándares para la adopción del Modelo de Seguridad y Privacidad de la Información en el marco de la Política de Gobierno Digital.
Ley 2195 de 2022	Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones. Fortalece la integridad pública y modifica el artículo 73 de la Ley 1474 de 2011 en lo relacionado con los Programas de Transparencia y Ética Pública.
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	Modifica disposiciones del Decreto 1081 de 2015 relacionadas con las Subcomisiones Técnicas de la Comisión Nacional de Moralización y la Estrategia Nacional de Lucha contra la Corrupción.
Resolución 02277 del 3 de junio de 2025	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia. La Resolución 02277 del 3 de junio de 2025, emitida por el Ministerio TIC, actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI) en Colombia. Esta norma ajusta el Anexo 1 de la Resolución 500 de 2021, fortaleciendo la estrategia de seguridad digital del Estado y la protección de activos de información

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4. LINEAMIENTOS GENERALES DE LA POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS DE LA CRC

4.1 Código de Integridad

La Comisión de Regulación de Comunicaciones – CRC cuenta con un Código de Integridad, el cual establece los principios y reglas de comportamiento que orientan la conducta de los servidores de la Entidad.

A través de este instrumento se busca que sus integrantes interioricen los valores institucionales como parte inherente al desarrollo cotidiano de sus funciones, con el propósito de prestar un mejor servicio a la ciudadanía, actuar con transparencia, hacer un adecuado uso de los recursos públicos y contribuir al fortalecimiento de la imagen y el posicionamiento institucional.

4.2 Propósito de la Dirección con esta Política

La Alta Dirección de la Comisión de Regulación de Comunicaciones – CRC reconoce la gestión integral de riesgos como un elemento fundamental para el adecuado funcionamiento del Sistema de Control Interno y para el cumplimiento de los objetivos institucionales.
En este sentido, la Alta Dirección orienta la gestión institucional hacia la identificación, análisis, tratamiento y seguimiento de los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, promoviendo una cultura de control, transparencia y responsabilidad en el manejo de los recursos públicos, así como la toma de decisiones informadas frente a los riesgos que puedan impactar la operación y los resultados de la Entidad.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4.3 Apetito del riesgo

El apetito del riesgo corresponde al nivel de riesgo que la Comisión de Regulación de Comunicaciones – CRC está dispuesta a asumir en el desarrollo de sus procesos, planes, programas y proyectos para el cumplimiento de sus objetivos estratégicos.

La definición del apetito del riesgo es responsabilidad de la Alta Dirección o Línea Estratégica de la entidad, en el marco del Comité Institucional de Coordinación de Control Interno u otras instancias del mismo nivel jerárquico, teniendo en cuenta la misión, visión, objetivos institucionales y el contexto interno y externo de la entidad.

El establecimiento del apetito del riesgo permite orientar la gestión institucional frente a la identificación, análisis, valoración y tratamiento de los riesgos, así como la toma de decisiones estratégicas, con el fin de mantener los niveles de riesgo dentro de rangos aceptables y contribuir al logro de los objetivos institucionales.

En el marco de la gestión integral del riesgo, la CRC definirá los niveles de aceptación y tolerancia al riesgo de acuerdo con la naturaleza de cada tipología de riesgo, su impacto sobre los objetivos institucionales y los lineamientos establecidos por la Alta Dirección.

5. CONTEXTO PARA LA GESTIÓN INTEGRAL DE RIESGOS

5.1 Direccionamiento estratégico institucional

La gestión integral de riesgos en la Comisión de Regulación de Comunicaciones – CRC se desarrolla en coherencia con el direccionamiento estratégico institucional y con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión – MIPG, el Sistema de Control Interno y el Sistema Integrado de Gestión de la Entidad.

La CRC ha definido su Plan Estratégico Institucional para el periodo 2025–2029, el cual orienta la gestión institucional y constituye el marco de referencia para el cumplimiento de sus objetivos misionales y estratégicos.

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[1] 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.

El direccionamiento estratégico de la Entidad se materializa a través del Mapa Estratégico CRC 2025–2029, el cual orienta la planeación institucional y la gestión de los procesos.

[1] 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

Ilustración 1. Mapa Estratégico CRC 2025–2029

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 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.

PILARES ESTRATÉGICOS

Derechos de los usuarios y audiencias	**O1.** Fortalecer el marco regulatorio e implementar herramientas de innovación regulatoria que protejan los derechos de los usuarios y audiencias, con el fin de responder a los cambios en los hábitos de consumo y a las tendencias del ecosistema digital.	**O2.** Fomentar el pluralismo y la imparcialidad informativa en los contenidos audiovisuales, mediante el desarrollo de estrategias pedagógicas eficaces con énfasis en la alfabetización mediática e informacional, para promover audiencias críticas y bien informadas.	**O3.** Impulsar el desarrollo de un modelo preventivo de inspección, vigilancia y control de contenidos, a través de iniciativas de socialización y acompañamiento a los regulados, para disminuir riesgos de incumplimiento y propender por la protección efectiva de los derechos de las audiencias, el pluralismo y la imparcialidad informativa.
Prospectiva sectorial	**O4.** Fortalecer la identificación y evaluación de los cambios en el ecosistema digital, las tecnologías emergentes, los nuevos agentes y modelos de negocio, para analizar su implicación en la adopción en la industria y en los ciudadanos, mediante la exploración de diferentes fuentes.	**O5.** Definir acciones estratégicas para orientar a los agentes en los mercados de comunicaciones y contenidos audiovisuales frente a los cambios del ecosistema digital, a través de la elaboración de estudios.	**O6.** Fortalecer la alineación de las iniciativas de la organización con las necesidades y demandas actuales y futuras de los usuarios, las audiencias y el ecosistema digital, mediante el desarrollo de ejercicios participativos en la elaboración de la Agenda Regulatoria, para atender los desafíos del ecosistema digital.
Mercados y competencia	**O7.** Promover el acceso, uso eficiente y la compartición de infraestructura de comunicaciones y otros sectores, para generar sinergias que aumenten la oferta de servicios y el despliegue de redes.	**O8.** Fomentar la competencia y la inversión en los mercados de comunicaciones para diversificar la oferta y mejorar la calidad de los servicios disponibles.	**O9.** Optimizar la interacción entre los agentes del sector a través de la gestión de las solicitudes de solución de controversias de manera eficiente.
Fortalecimiento estratégico institucional	**O10.** Fortalecer una cultura organizacional que afiance la apropiación de los valores institucionales, fomente la responsabilidad social y potencie el compromiso del talento humano hacia el cumplimiento de los objetivos de la entidad.	**O11.** Optimizar la gestión de la Entidad mediante la apropiación y mejora de los instrumentos de gestión que permitan el fortalecimiento de los procesos para contribuir a un mejor desempeño organizacional.	**O12.** Impulsar y fortalecer la transformación digital de la entidad mediante iniciativas tecnológicas y el cumplimiento de los lineamientos de la política de gobierno digital para mejorar la eficiencia y efectividad de sus procesos.
	O13. Facilitar el acceso oportuno a información relevante y precisa del sector mediante las publicaciones en Postdata para fortalecer la toma de decisiones basadas en evidencia en los mercados de comunicaciones.	**O14.** Facilitar la implementación oportuna de la regulación de la CRC y su apropiación por parte de los grupos de valor.	**O15.** Fortalecer el posicionamiento de la CRC mediante la promoción de sus avances y buenas prácticas en foros globales, la participación activa en redes de reguladores, la difusión estratégica de sus logros en medios internacionales y el impulso de iniciativas de colaboración y cooperación técnica con reguladores de otros países para consolidarse como un referente en regulación a nivel internacional.

Fuente: Elaboración propia CRC

La gestión integral de riesgos en la CRC se encuentra articulada con el direccionamiento estratégico institucional, el Sistema Integrado de Gestión y el modelo de operación por procesos, con el fin de contribuir al cumplimiento de los objetivos estratégicos y fortalecer el control institucional.

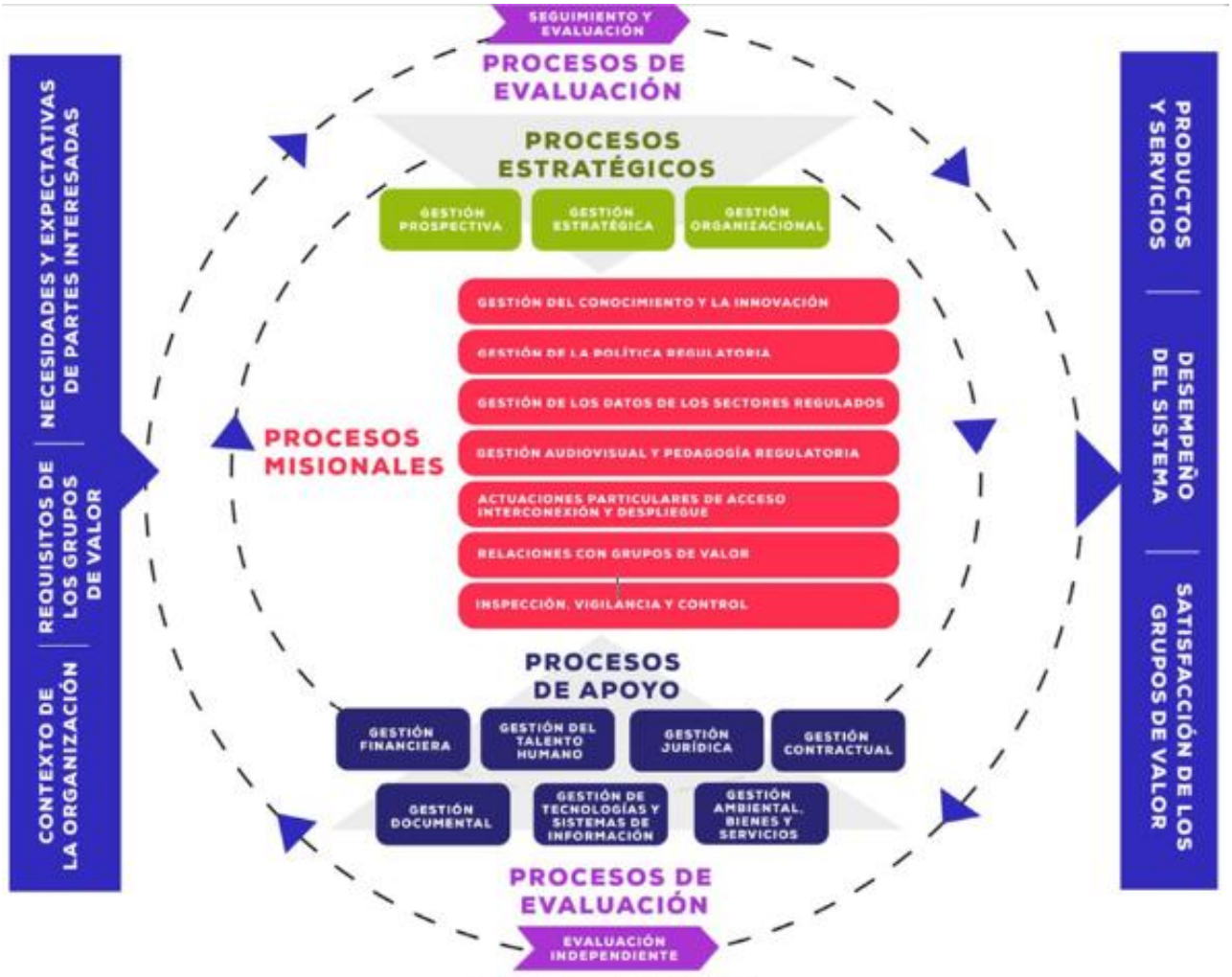
En este sentido, la presente política se armoniza con la misión y visión institucional, así como con el Sistema Integrado de Gestión de la Entidad, el cual está conformado por las normas ISO 9001, NTC ISO 14001, NTC-ISO/IEC 27001, NTC-ISO/IEC 27701 y el Sistema de Gestión de Seguridad y Salud en el Trabajo, de conformidad con el Decreto 1072 de 2015 y la Resolución 312 de 2019 del Ministerio del Trabajo.

5.2 Articulación con el Sistema Integrado de Gestión y el modelo de operación por procesos

La gestión integral de riesgos se articula con el modelo de operación por procesos definido por la CRC, el cual se representa en el siguiente mapa de procesos:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 2. Mapa de procesos de la CRC



Fuente: Elaboración propia CRC.

La identificación y gestión de los riesgos se realiza en cada uno de los procesos institucionales, asegurando su alineación con el direccionamiento estratégico y con los objetivos institucionales.

El seguimiento a la gestión de los riesgos, la operación de los controles y la ejecución de los planes de tratamiento se desarrolla a través del esquema de líneas de defensa, de acuerdo con los mecanismos, herramientas y lineamientos definidos institucionalmente por la CRC para la gestión integral del riesgo.

Adicionalmente, el Comité Institucional de Coordinación de Control Interno realiza seguimiento y emite recomendaciones frente a la gestión integral del riesgo, en el marco de las funciones establecidas en la normatividad vigente.

5.3 Contexto Interno y Externo para la Gestión Integral de Riesgo

La gestión integral de riesgos en la Comisión de Regulación de Comunicaciones – CRC parte del análisis del contexto interno y externo de la Entidad, con el fin de identificar factores y condiciones que puedan incidir en el cumplimiento de los objetivos institucionales y en el desarrollo de los procesos.

El análisis del contexto permite reconocer condiciones internas y externas que pueden influir en la materialización de eventos de riesgo, constituyéndose en un insumo fundamental para la identificación, análisis y valoración de los riesgos institucionales.

5.3.1 Contexto Externo

Corresponde a las condiciones del entorno que pueden influir en el cumplimiento de los objetivos institucionales y en el desarrollo de los procesos de la Entidad, entre los principales elementos del contexto externo se encuentran:

- **Económicos**: disponibilidad de capital, liquidez, mercados financieros, desempleo y condiciones de competencia.

- **Políticos**: cambios de gobierno, legislación, políticas públicas y regulación aplicable al sector de comunicaciones.
- **Sociales**: demografía, responsabilidad social, orden público y condiciones de salud pública.
- **Tecnológicos**: avances tecnológicos, acceso a sistemas de información externos y desarrollo del gobierno digital.
- **Medioambientales**: emisiones y residuos, uso de energía, eventos naturales, desarrollo sostenible y cambio climático.
- **Legales y regulatorios**: leyes, decretos, y demás disposiciones normativas aplicables a la Entidad.
- **Auditorías externas**: evaluaciones realizadas por organismos de control, como la Contraloría General de la República, así como auditorías externas al Sistema Integrado de Gestión.
- **Evento externo**: situaciones o acontecimientos externos que puedan afectar el cumplimiento de los objetivos institucionales.

5.3.2 Contexto Interno

Corresponde a las condiciones propias de la organización que pueden incidir en el cumplimiento de los objetivos institucionales y en el desarrollo de los procesos, entre los principales elementos del contexto interno se consideran:

- **Financieros**: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
- **Personal**: competencias del personal, disponibilidad del talento humano y condiciones de seguridad y salud en el trabajo.
- **Procesos**: diseño, capacidad, y ejecución de los procesos institucionales, gestión del conocimiento, proveedores, entradas y salidas de los procesos.
- **Tecnología**: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.

- **Estratégicos**: direccionamiento estratégico, planeación institucional, liderazgo y 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**: competencias, clima organizacional, cultura ética y posibles situaciones que puedan afectar la integridad pública.

6. NIVELES DE RESPONSABILIDAD PARA LA GESTIÓN DEL RIESGO – ESQUEMA DE LÍNEAS DE DEFENSA

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 2. Esquema de Líneas de Defensa

Línea de Defensa	Responsables	Responsabilidades y Actividades
Línea Estratégica	Alta Dirección (Dirección Ejecutiva, Comisionados y Coordinador Ejecutivo). Comité Institucional de Coordinación de Control Interno. Comité Institucional de Gestión y Desempeño.	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 puedan afectar el cumplimiento de los objetivos estratégicos. Analizar cambios en el contexto interno y externo que puedan impactar la operación de la entidad y modificar la estructura de riesgos y controles. Definir lineamientos estratégicos para la gestión del riesgo y

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Responsables	Responsabilidades y Actividades
		el fortalecimiento del Sistema 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. 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 y tomar decisiones orientadas al cumplimiento de los resultados institucionales, incluyendo el ajuste de los procesos que intervienen en su logro, así como la reorganización de equipos de trabajo y recursos, 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. 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

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Responsables	Responsabilidades y Actividades
		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. Reportar a la segunda línea de defensa en los mecanismos establecidos, 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	Asesorar a la línea estratégica en el análisis del contexto interno y externo, para una adecuada definición de la política para la gestión integral 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

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Responsables	Responsabilidades y Actividades
	línea de defensa: Coordinador de Planeación y Gestión. Coordinador de Gestión Administrativa y Financiera. Coordinador de Gestión Jurídica Coordinador de Diseño Regulatorio. Coordinador de Gestión Audiovisual y Pedagogía Regulatoria. Coordinador de Tecnologías y Sistemas de Información. Coordinador de Relaciones con Grupos de Valor. Coordinador de Analítica de Datos. Coordinador de Prospectiva Estratégica e Innovación -Líderes de los Sistemas (Gestión de Calidad, Gestión Ambiental, Seguridad y Salud en el Trabajo, Gestión de Seguridad y Privacidad de la Información).	institucionales. Responsabilidad de la Coordinación de Planeación y Gestión, siempre que se requiera y cuando se den cambios en la metodología establecida. 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. 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. 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 gestión, integridad pública, fiscales, seguridad y privacidad de la información 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, integridad pública, fiscal y Seguridad y Privacidad de la información). Responsabilidad de la Coordinación de Planeación y Gestión. Reportar desde la segunda línea de defensa a la Línea Estratégica, los resultados del seguimiento y monitoreo de los riesgos,

Línea de Defensa	Responsables	Responsabilidades y Actividades
		así como la 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. Asesorar y acompañar a los líderes de proceso en la identificación, evaluación y tratamiento de los riesgos de seguridad y privacidad de la información, de conformidad con los lineamientos institucionales para la gestión integral del riesgo y las directrices definidas por la Entidad. Responsabilidad de la Coordinación de Planeación y Gestión. Así mismo 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 Coordinación de Control Interno el 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 Planeación y Gestión. 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

Línea de Defensa	Responsables	Responsabilidades y Actividades
		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 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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Responsables	Responsabilidades y Actividades
		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, Seguridad y Privacidad de la Información 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 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 riesgos de integridad pública 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

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Línea de Defensa	Responsables	Responsabilidades y Actividades
		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 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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ANEXO METODOLÓGICO

7. METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS EN LA CRC

Introducción

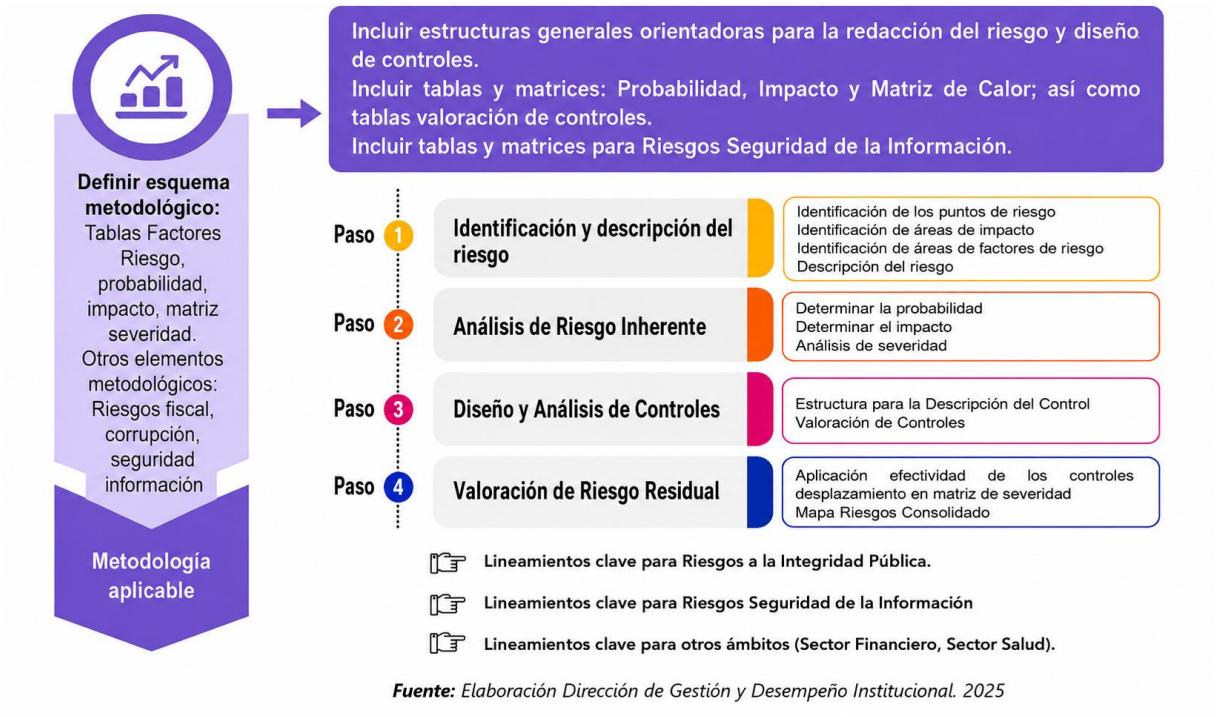
El presente anexo metodológico establece la metodología para la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos en la Comisión de Regulación de Comunicaciones – CRC, en desarrollo de lo dispuesto en la Política para la Gestión Integral de Riesgos de la Entidad.

La aplicación de esta metodología se realiza teniendo en cuenta el contexto interno y externo de la entidad, definido en la Política para la Gestión Integral de Riesgos de la CRC, el cual permite comprender el entorno institucional, normativo, sectorial y organizacional que puede incidir en el cumplimiento de los objetivos institucionales.

La presente metodología toma como referencia la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, expedida por el Departamento Administrativo de la Función Pública – DAFP, con el propósito de orientar de manera uniforme la gestión de los riesgos en los procesos de la Entidad y fortalecer el Sistema de Control Interno.

La metodología para la gestión integral de riesgos en la CRC se desarrolla tomando como referencia los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública – DAFP, versión 7, la cual orienta las etapas generales para la identificación, análisis, valoración y tratamiento de los riesgos institucionales.

Ilustración 3. Aspectos metodológicos



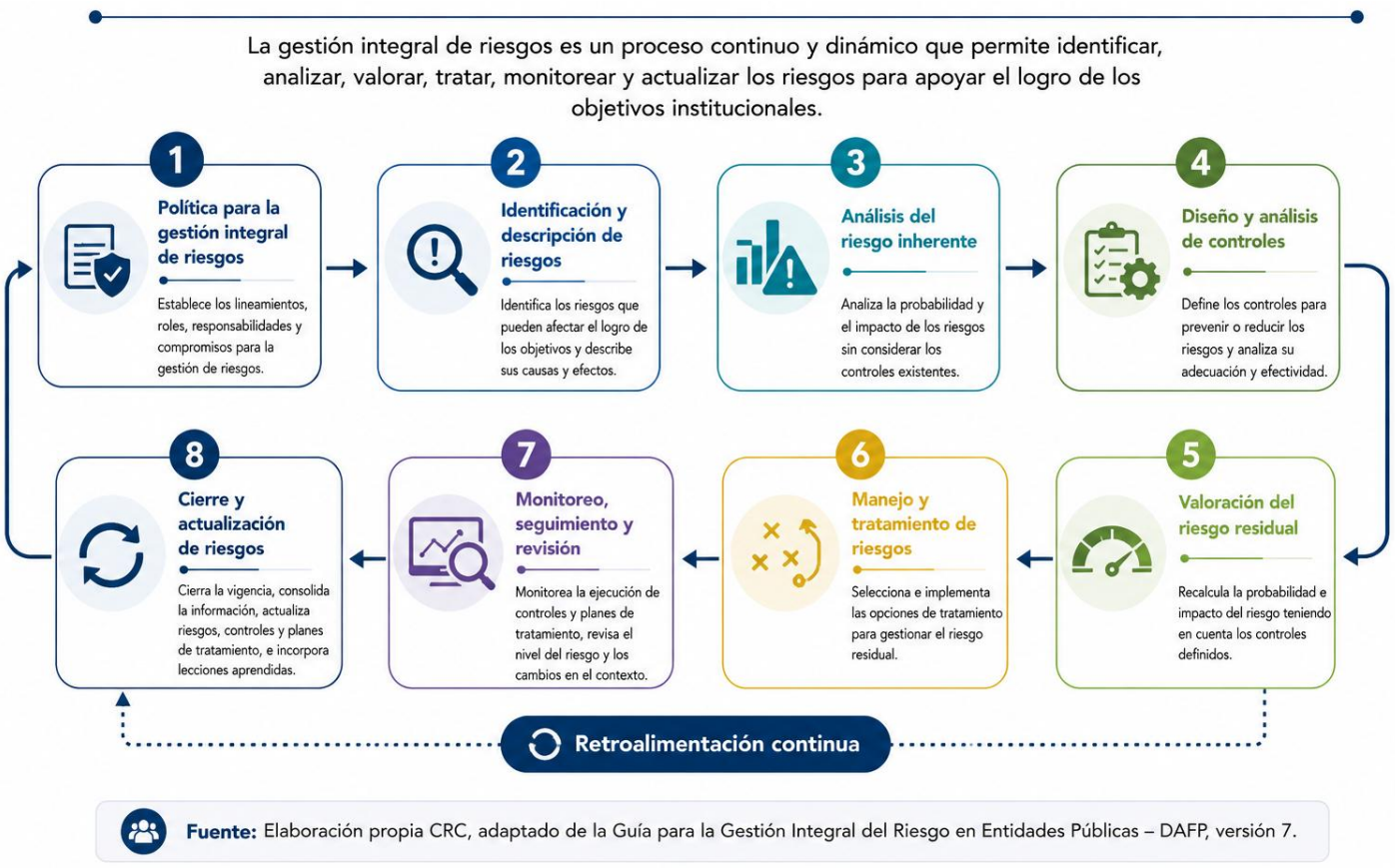
Fuente: *Elaboración Dirección de Gestión y Desempeño Institucional. 2025*

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 – DAFP 2025

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.1 Ciclo Metodológico para la Gestión Integral de Riesgos en la CRC

Ilustración 4. Ciclo metodológico para la gestión integral de riesgos en la CRC



Fuente: Elaboración propia CRC, adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – DAFP, versión 7.

Fase Previa. Análisis de Contexto Estratégico.

Antes de iniciar la aplicación de la metodología para la gestión integral de riesgos, se debe realizar el análisis del contexto estratégico institucional. Cada proceso deberá identificar su alineación con la misión, visión, objetivos estratégicos y modelo de operación de la Entidad, así como los factores internos y externos que puedan afectar el cumplimiento de los objetivos institucionales y de los procesos.

Este análisis permite identificar condiciones, causas y posibles consecuencias que pueden incidir en la materialización de eventos de riesgo y constituye un insumo fundamental para la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos institucionales.

7.1.1 Política para la Gestión Integral de Riesgos.

Corresponde a la directriz institucional mediante la cual la CRC adopta y adapta los lineamientos externos aplicables para la gestión integral de riesgos, definiendo criterios, responsabilidades y metodologías para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos institucionales.

La política deberá revisarse periódicamente y actualizarse cuando se requiera, considerando cambios normativos, metodológicos, estratégicos o institucionales. Su revisión y actualización se realizará en el marco del Comité Institucional de Coordinación de Control Interno, conforme a las funciones establecidas en la normatividad vigente, y deberá ser publicada y socializada a los colaboradores de la Entidad.

7.1.2 Identificación y descripción de los riesgos.

En esta etapa se identifican los puntos de riesgo asociados a los procesos, objetivos, actividades, proyectos o servicios de la Entidad, así como las posibles causas y consecuencias que puedan afectar el cumplimiento de los objetivos institucionales.

Así mismo, se realiza la descripción y clasificación del riesgo de acuerdo con la metodología y tipología definida en la Política para la Gestión Integral de Riesgos de la CRC.

7.1.3 Análisis del riesgo inherente.

En esta fase se realiza el análisis de probabilidad e impacto del riesgo sin considerar la existencia de controles, de acuerdo con las tablas y criterios definidos en la Política para la Gestión Integral de Riesgos.

Como resultado de este análisis se determina el nivel de riesgo inherente.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.1.4 Diseño y análisis de controles.

En esta etapa se diseñan, identifican y analizan los controles definidos para prevenir, detectar o mitigar la materialización de los riesgos identificados. Los controles deberán estructurarse y documentarse de acuerdo con los criterios definidos en la Política para la Gestión Integral de Riesgos, incluyendo su tipología, periodicidad, responsables, evidencia de ejecución y demás atributos metodológicos aplicables.

7.1.5 Valoración del riesgo residual:

Una vez identificados y analizados los controles, se deberá establecer la tipología del control y valorar sus atributos, de acuerdo con los criterios definidos en la Política para la Gestión Integral de Riesgos.

Como resultado de esta etapa se determina el nivel de riesgo residual.

7.1.6 Manejo de los Riesgos.

El manejo y tratamiento de los riesgos se definirá de acuerdo con las opciones de tratamiento y los niveles de aceptación del riesgo establecidos en la Política para la Gestión Integral de Riesgos.

Para los riesgos asociados a la integridad pública deberán implementarse controles, mecanismos de seguimiento y acciones orientadas a prevenir su materialización, independientemente del nivel de riesgo residual obtenido.

7.1.7 Monitoreo, seguimiento y revisión.

El monitoreo, seguimiento y revisión de los riesgos deberá realizarse de manera permanente por parte de la primera línea de defensa, verificando la adecuada operación de los controles, la ejecución de los planes de tratamiento y los posibles cambios en el contexto interno y externo que puedan afectar los riesgos identificados.

Los responsables de los riesgos deberán reportar periódicamente el seguimiento realizado, de acuerdo con los lineamientos definidos por la segunda línea de defensa (Coordinación de Planeación y Gestión), incluyendo las evidencias que permitan verificar la adecuada operación de los controles y la ejecución de las acciones definidas.

La Coordinación de Planeación y Gestión consolidará la información reportada y presentará los informes correspondientes a la línea estratégica y demás instancias institucionales definidas.

La Oficina de Control Interno, en el marco de sus funciones de evaluación independiente del Sistema de Control Interno, podrá realizar seguimiento y emitir recomendaciones frente a la gestión integral de riesgos y la efectividad de los controles implementados.

7.1.8 Cierre y actualización de riesgos.

El cierre y actualización de riesgos consiste en realizar la revisión periódica de los riesgos identificados, sus controles, valoraciones y acciones de tratamiento, con el fin de determinar su continuidad, actualización, ajuste o cierre para la siguiente vigencia.

En esta etapa se deberá verificar, entre otros aspectos:

- La adecuada operación de los controles.
- La ejecución de las acciones de tratamiento.
- La necesidad de actualizar causas, consecuencias o factores de riesgo.
- Cambios en los niveles de riesgo inherente o residual.
- La pertinencia y vigencia del riesgo identificado.

Esta etapa permite fortalecer la mejora continua de la gestión integral de riesgos y garantizar la trazabilidad de la información institucional.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.2 Desarrollo de las etapas metodológicas

7.2.1 Identificación de riesgos.

Para la identificación de los riesgos de gestión, riesgos fiscales, riesgos para la integridad pública y riesgos de seguridad y privacidad de la información, cada grupo interno de trabajo responsable de los procesos en la Comisión de Regulación de Comunicaciones – CRC realiza ejercicios de análisis con los equipos de trabajo, con el fin de identificar los eventos que puedan afectar el cumplimiento de los objetivos institucionales.

Durante esta etapa se analizan, entre otros, los siguientes elementos:

- objetivos del proceso
- contexto interno y externo
- factores de riesgo
- causas o fuentes generadoras del riesgo
- consecuencias o impactos potenciales

El paso inicial consiste en analizar los objetivos del proceso y verificar su alineación con los objetivos estratégicos de la Entidad. En caso de ser necesario, se deberán ajustar los objetivos del proceso. Estos deben incluir el qué, cómo, para qué, cuándo y cuánto, y cumplir con atributos mínimos de la metodología SMART (específicos, medibles, alcanzables, relevantes y definidos en el 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?).

Factores de riesgo.

Los factores de riesgo corresponden a circunstancias o condiciones que pueden incrementar la probabilidad de ocurrencia de un evento de riesgo. Estos factores constituyen elementos de análisis que facilitan la identificación de riesgos y permiten comprender el entorno en el que estos pueden materializarse.

Para la identificación de riesgos, la CRC considerará, entre otros, los siguientes factores de riesgo:

Tabla 3. Factores de riesgo

Factor	Descripción
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos institucionales.
Transacción u Operación Específica (aplica para LA/FT/FP)	Eventos relacionados con transacciones y operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la integridad pública.
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.
Eventos externos	Eventos por situaciones externas que afectan la entidad.

Fuente: Elaboración propia CRC

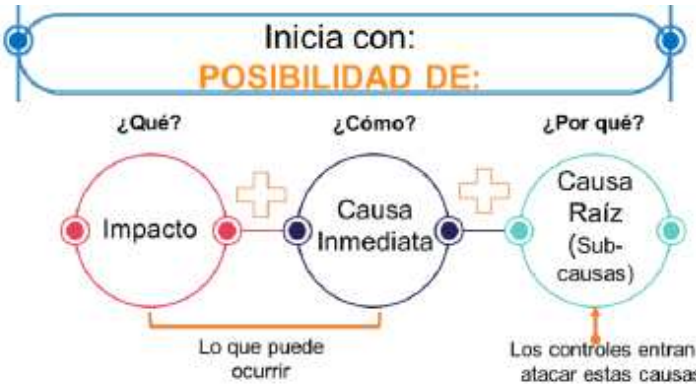
Nota: Los factores de riesgo constituyen una referencia para apoyar la identificación de riesgos. Cada proceso podrá analizar factores adicionales de acuerdo con las características de sus actividades, su contexto y las particularidades de la Entidad.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.2.2 Estructura para la descripción de riesgos.

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

Ilustración 5. Estructura para la redacción del riesgo



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 – DAFP 2025

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.

Para el 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 dañosos 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

La CRC podrá tomar como referencia el "Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas" elaborado por el Departamento Administrativo de la Función Pública – DAFP, como herramienta orientadora para 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, si existen riesgos transversales, existen causas transversales, pero el riesgo siempre debe contar con un proceso responsable.

7.2.3 Identificación de riesgo para la integridad pública.

Los riesgos para la integridad pública corresponden a la posibilidad de que se presenten eventos que generen afectaciones económicas o reputacionales para la entidad debido a comportamientos o prácticas que vulneren la integridad en el ejercicio del servicio público.

Dentro de esta tipología se consideran amenazas asociadas a la integridad pública, tales como:

- fraude
- soborno
- corrupción
- conflictos de interés no declarados
- lavado de activos (LA)
- financiación del terrorismo (FT)
- proliferación de armas de destrucción masiva (FP)

La identificación de estos riesgos permite anticipar situaciones que puedan afectar la confianza en la gestión institucional y fortalecer las acciones de prevención.

En el marco del Programa de Transparencia y Ética Pública (PTEP), establecido mediante el Decreto 1122 de 2024, la CRC deberá gestionar de manera proactiva los riesgos asociados a la integridad pública, permitiendo anticipar situaciones que puedan afectar la ética pública, la confianza ciudadana, la transparencia, la legalidad y el adecuado uso de los recursos públicos.

De acuerdo con el Anexo Técnico del Decreto 1122 de 2024, los siguientes 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/FP: 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 (FT) 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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.2.4 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 con criticidad alta, 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 integridad y/o disponibilidad del portal WEB de la CRC debido a ataques informáticos por configuraciones por defecto en el servidor.

7.3 Clasificación de los Riesgos

Los riesgos identificados en la Comisión de Regulación de Comunicaciones – CRC se clasifican de acuerdo con su tipología, con el fin de facilitar su identificación, análisis y gestión dentro de los procesos institucionales.

De conformidad con los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública – DAFP, los riesgos que gestiona la Entidad se agrupan en las siguientes categorías:

a. Riesgos de gestión

Corresponden a la posibilidad de que ocurran eventos que afecten el cumplimiento de los objetivos institucionales, los procesos o la prestación de los servicios de la entidad.

Estos riesgos pueden estar asociados a situaciones como:

- fallas en la ejecución de procesos

- errores en procedimientos o actividades
- debilidades en la gestión administrativa
- inadecuada gestión de recursos
- incumplimiento de metas o proyectos institucionales

b. Riesgos fiscales

Corresponden a la posibilidad de que se genere un daño o detrimento al patrimonio público como consecuencia de acciones u omisiones en el ejercicio de la gestión fiscal.
Estos riesgos pueden afectar los bienes, recursos o intereses patrimoniales de naturaleza pública administrados por la entidad.
La identificación de estos riesgos se realiza teniendo en cuenta los puntos de riesgo fiscal definidos por el Departamento Administrativo de la Función Pública y las situaciones que pueden generar posibles efectos dañosos sobre los recursos públicos.

c. Riesgos para la integridad pública

Corresponden a la posibilidad de que se presenten situaciones que afecten la transparencia, la ética pública, la moralidad administrativa o la confianza de la ciudadanía en la gestión institucional.

Dentro de esta categoría se consideran amenazas asociadas a la integridad pública, tales como:

- fraude
- soborno
- corrupción
- lavado de activos (LA)
- financiación del terrorismo (FT)
- proliferación de armas de destrucción masiva (FP)

Estos riesgos se gestionan en el marco del Programa de Transparencia y Ética Pública – PTEP, establecido mediante el Decreto 1122 de 2024.

d. Riesgos de seguridad y privacidad de la información

Corresponden a la posibilidad de que ocurran eventos que afecten la confidencialidad, integridad o disponibilidad de los activos de información de la entidad o en la privacidad de los datos personales.
La identificación y gestión de estos riesgos se realiza considerando los activos de información de la entidad, las amenazas y vulnerabilidades asociadas, y en articulación con los lineamientos del Modelo de Seguridad y Privacidad de la Información.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).

Tabla 4. Tabla de amenazas comunes

Tipo	Amenaza
Daño físico	• Fuego • Agua • Contaminación • Accidente Importante • Destrucción del equipo o medios • Polvo, corrosión, congelamiento
Eventos naturales	• Fenómenos climáticos • Fenómenos sísmicos • Fenómenos volcánicos • Fenómenos meteorológicos • Inundación
Perdida de los servicios esenciales	• Fallas en el sistema de suministro de agua o aire acondicionado • Perdida de suministro de energía • Falla en equipo de telecomunicaciones

Perturbación debida a la radiación	• Radiación electromagnética • Radiación térmica • Impulsos electromagnéticos
Compromiso de la información	• Interceptación de señales de interferencia comprometida • Espionaje remoto • Escucha encubierta • Hurto de medios o documentos • Hurto de equipo • Recuperación de medios reciclados o desechados • Divulgación • Datos provenientes de fuentes no confiables • Manipulación con hardware • Manipulación con software • Detección de la posición
Fallas técnicas	• Fallas del equipo • Mal funcionamiento del equipo • Saturación del sistema de información • Mal funcionamiento del software • Incumplimiento en el mantenimiento del sistema de información.
Acciones no autorizadas	• Uso no autorizado del equipo • Copia fraudulenta del software • Uso de software falso o copiado • Corrupción de los datos • Procesamiento ilegal de datos
Compromiso de las funciones	• Error en el uso • Abuso de derechos • Falsificación de derechos • Negación de acciones • Incumplimiento en la disponibilidad del personal

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 5. Tabla de Vulnerabilidades comunes

Tipo	Amenaza
Hardware	• Mantenimiento insuficiente • Ausencia de esquemas de reemplazo periódico • Sensibilidad a la radiación electromagnética • Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) • Almacenamiento sin protección • Falta de cuidado en la disposición final • Copia no controlada
Software	• Ausencia o insuficiencia de pruebas de software • Ausencia de terminación de sesión • Ausencia de registros de auditoría • Asignación errada de los derechos de acceso • Interfaz de usuario compleja • Ausencia de documentación • Fechas incorrectas • Ausencia de mecanismos de identificación y autenticación de usuarios • Contraseñas sin protección • Software nuevo o inmaduro
Red	• Ausencia de pruebas de envío o recepción de mensajes • Líneas de comunicación sin protección • Conexión deficiente de cableado • Tráfico sensible sin protección • Punto único de falla
Personal	• Ausencia del personal • Entrenamiento insuficiente • Falta de conciencia en seguridad • Ausencia de políticas de uso aceptable • Trabajo no supervisado de personal externo o de limpieza
Lugar	• Uso inadecuado de los controles de acceso al edificio

	• Áreas susceptibles a inundación • Red eléctrica inestable • Ausencia de protección en puertas o ventanas
Organización	• Ausencia de procedimiento de registro/retiro de usuarios • Ausencia de proceso para supervisión de derechos de acceso • Ausencia de control de los activos que se encuentran fuera de las instalaciones • Ausencia de acuerdos de nivel de servicio (ANS o SLA) • Ausencia de mecanismos de monitoreo para brechas en la seguridad • Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

NOTA: El proceso puede definir nuevas las amenazas y Vulnerabilidades que considere relevantes de acuerdo con su contexto.

7.4 Análisis de Riesgos

7.4.1 Generalidades.

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): corresponde al nivel de riesgo que permanece después de aplicar y valorar los controles definidos para su mitigación.

El análisis del riesgo inherente tiene como propósito determinar la probabilidad de ocurrencia y el impacto de los riesgos identificados, sin considerar la existencia de controles, con el fin de establecer el nivel de riesgo inherente.

7.4.2 Análisis de probabilidad

Para los riesgos de gestión y fiscales, la probabilidad corresponde a la posibilidad de ocurrencia de un evento que pueda afectar el cumplimiento de los objetivos institucionales y el desarrollo de los procesos de la Entidad.

La determinación de la probabilidad se realiza teniendo en cuenta los siguientes criterios:

Tabla 6. Criterios para definir el nivel de probabilidad de riesgos de gestión, fiscal e integridad pública

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas. DAFP. Versión 7. 2025

Para los riesgos de seguridad y privacidad de la información, la probabilidad se determinará considerando factores históricos y prospectivos, a partir del conocimiento adquirido mediante la gestión de incidentes de seguridad de la información de los últimos cinco (5) años. En los casos en que no se cuente con información histórica suficiente, se deberá considerar el conocimiento de los colaboradores responsables de los activos de información asociados a los riesgos identificados, así como el análisis del contexto interno y externo de la Entidad.

Tabla 7. Calificación de Probabilidad riesgos de SGSPI

Nivel	Descriptor	Histórico	Prospectiva
1	Muy baja	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	Baja	En los últimos cinco (5) años se ha materializado el riesgo al menos una vez	Se espera que el evento de riesgo se materialice más de una vez en los próximos cinco (5) años.
3	Media	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	Alta	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	Muy Alta	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.

Riesgos para la integridad pública:

Para los riesgos asociados a la integridad pública, la CRC aplicará la misma escala de probabilidad definida para los riesgos de gestión y fiscales, en concordancia con el enfoque de

gestión integral del riesgo establecido por el Departamento Administrativo de la Función Pública – DAFP.

7.4.3 Análisis de impacto

Para los riesgos de gestión y fiscal, 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 8. Criterios para definir el nivel de impacto de riesgos de gestión, fiscal e integridad pública

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

Fuente: Actualizada Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 – DAFP 2025

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:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 9. Calificación de impacto de riesgos de seguridad y privacidad de la información

Nivel	Descriptor	Consecuencias Cuantitativas	Consecuencias Cualitativas
1	**Insignificante**	• Afectación menor a 10 SMLMV. • 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. • El riesgo afecta la imagen de algún área de la entidad.
2	**Menor**	• Mayor a 10 SMLMV y Menor a 50 SMLMV. • 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. • El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Nivel	Descriptor	Consecuencias Cuantitativas	Consecuencias Cualitativas
3	**Moderado**	• Mayor a 50 SMLMV y Menor a 100 SMLMV. • 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. • El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
4	**Mayor**	• Mayor a 100 SMLMV y Menor a 500 SMLMV. • 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. • El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.

Nivel	Descriptor	Consecuencias Cuantitativas	Consecuencias Cualitativas
5	**Catastrófico**	• Mayor a 500 SMLMV. • 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. • El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Elaboración Propia CRC.

Probabilidad de Riesgos para la Integridad Pública

Para determinar la probabilidad de ocurrencia del riesgo se deben analizar las condiciones que pueden favorecer la materialización de eventos asociados a amenazas contra la integridad pública, tales como fraude, soborno, conflictos de interés no declarados o situaciones asociadas a lavado de activos, financiación del terrorismo o proliferación de armas de destrucción masiva.

La estimación de la probabilidad se realiza considerando aspectos tales como:

- antecedentes o eventos ocurridos previamente en la Entidad o en el sector;
- debilidades identificadas en los procesos o en los controles existentes;
- complejidad de las actividades o procesos;
- grado de exposición del proceso a terceros o actores externos;
- condiciones del entorno institucional.

De acuerdo con el enfoque de gestión integral del riesgo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – versión vigente del

Departamento Administrativo de la Función Pública, la CRC aplica la misma escala de probabilidad utilizada para los riesgos de gestión y riesgos fiscales, con el fin de mantener un enfoque metodológico integral en la valoración de los riesgos institucionales.
En consecuencia, la determinación de la probabilidad de los riesgos para la integridad pública se realizará utilizando la misma tabla de probabilidad definida en la metodología institucional para la gestión de riesgos, la cual permite estimar la frecuencia o posibilidad de ocurrencia del evento de riesgo.

7.4.4 Determinación del nivel del riesgo

El nivel del riesgo corresponde al resultado obtenido al relacionar la probabilidad de ocurrencia del riesgo con el impacto que podría generar su materialización.

Para determinar el nivel del riesgo se deben considerar los valores asignados previamente a la probabilidad y al impacto del evento de riesgo identificado. La combinación de estos dos elementos permite establecer el nivel de exposición de la Entidad frente al riesgo.

- El nivel del riesgo permite:
- identificar la magnitud del riesgo;
- priorizar los riesgos que requieren mayor atención;
- orientar la definición de controles y acciones de tratamiento;
- apoyar la toma de decisiones para la gestión del riesgo en los procesos.

La determinación del nivel del riesgo se realiza mediante la matriz de probabilidad e impacto definida en la metodología institucional para la gestión de riesgos, la cual permite establecer los diferentes niveles de riesgo.

De acuerdo con el enfoque de gestión integral del riesgo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – versión vigente, la CRC utiliza la misma matriz de valoración del riesgo para las diferentes tipologías de riesgos,

incluyendo:

- riesgos de gestión,
- riesgos fiscales,
- riesgos para la integridad pública,
- y riesgos asociados a la seguridad de la información.

La aplicación de esta matriz permite clasificar los riesgos en diferentes niveles, facilitando su análisis y la definición de las acciones necesarias para su gestión.

7.5 Diseño y análisis de controles

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.

7.5.1 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:

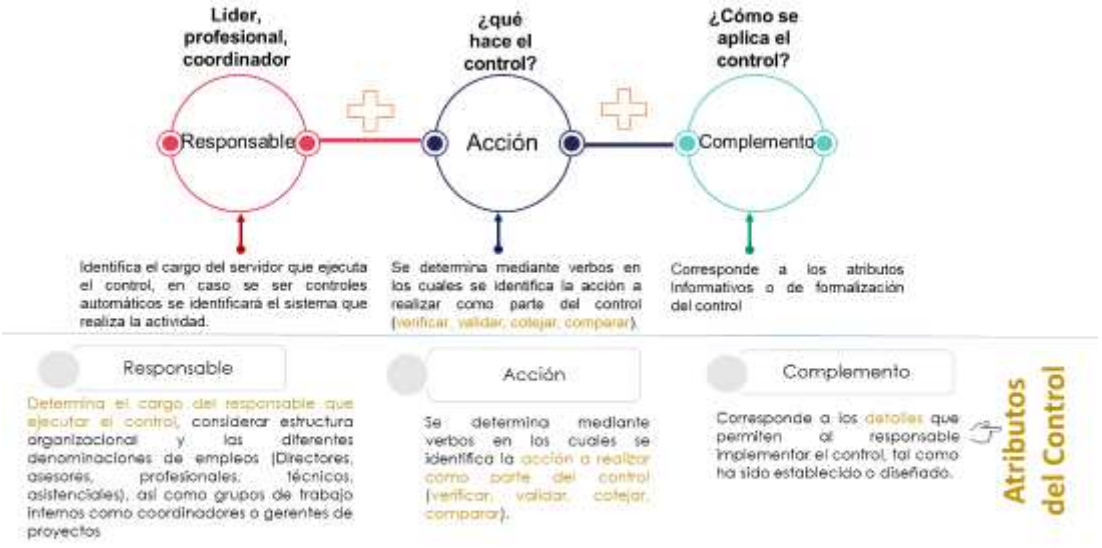
Control manual: son controles ejecutados por personas.

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:

Ilustración 6. Estructura para la redacción de controles



Fuente: *Elaboración Dirección de Gestión y Desempeño Institucional. 2025*

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 – DAFP 2025

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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.

Valoración de controles según atributos

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

Ilustración 7. Valoración de controles

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional, 2020.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 – DAFP 2025

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 8. Análisis atributos formalización del control

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, Departamento Administrativo de la Función Pública – DAFP, Versión 7, 2025.

La CRC podrá realizar adaptaciones metodológicas a los criterios de valoración de controles, siempre que estas mantengan coherencia con los lineamientos generales definidos por el DAFP y respondan a las necesidades operativas, tecnológicas y funcionales de la Entidad.

Para efectos de la valoración del atributo "Evidencia (Trazabilidad de la ejecución)", se entenderá como "Con registro electrónico" aquellos controles cuya evidencia o trazabilidad

repose en medios digitales o electrónicos, tales como correos electrónicos, documentos en control de cambios, actas digitales, plataformas colaborativas, sistemas de información, aplicativos o repositorios documentales, aun cuando la ejecución del control requiera intervención manual de los responsables.

El criterio "Con registro manual" aplicará cuando la evidencia del control repose exclusivamente en soportes físicos o registros manuales no administrados mediante herramientas digitales o electrónicas institucionales.

El criterio "Según necesidad" aplica cuando el control se ejecuta en función de eventos o situaciones específicas del proceso que requieren su aplicación, sin una periodicidad fija definida.

Posterior a identificar y calcular los controles, se realiza el cálculo para definir el valor del riesgo residual y, de esta manera, determinar su ubicación en la matriz de calor.
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.

7.6 Valoración del riesgo residual

Posterior a la identificación, diseño y valoración de los controles, se realiza la valoración del riesgo residual, con el fin de determinar el nivel de riesgo que permanece después de aplicar los controles definidos para su mitigación.

La valoración del riesgo residual permite establecer la ubicación final del riesgo dentro de la matriz de calor institucional y definir las acciones de tratamiento correspondientes, de acuerdo con los niveles de aceptación y tolerancia al riesgo definidos por la CRC.

Es importante tener presente que, cuando los controles identificados no son correctivos, el impacto residual corresponde al impacto inherente inicialmente calculado.

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

7.7 Tratamiento y aceptación de los Riesgos (Apetito del riesgo)

7.7.1 Opciones de tratamiento

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

Aceptar el riesgo: Corresponde a la decisión de no adoptar medidas adicionales que modifiquen la probabilidad o el impacto del riesgo, manteniendo los controles existentes.

En la CRC, cuando se acepta un riesgo, se ejecutan las actividades propias del proceso y los controles definidos, realizando el seguimiento correspondiente a través de los mecanismos institucionales de monitoreo.

Reducir el riesgo: Consiste en adoptar medidas orientadas a disminuir la probabilidad de ocurrencia del riesgo o mitigar su impacto, generalmente mediante la implementación o fortalecimiento de controles.

Cuando se determine esta opción de tratamiento se debe definir un plan de acción, el cual deberá contener:

- acción a implementar
- responsable
- fecha de implementación
- fecha de seguimiento
- estado de avance

Evitar el riesgo: Consiste en no iniciar o suspender las actividades que generan el riesgo, cuando estas representen una exposición que la Entidad no esté dispuesta a asumir.

En la CRC, esta estrategia se aplicará únicamente de manera excepcional, previo análisis técnico y operativo de la actividad que origina el riesgo.

Compartir el riesgo: Consiste en transferir o compartir parte del riesgo con terceros.
En el caso de los riesgos para la integridad pública, la responsabilidad institucional sobre el riesgo no puede ser transferida.

7.7.2 Tratamiento según nivel de severidad.

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.

Ilustración 9. 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.

La valoración de los riesgos asociados a la integridad pública se realiza utilizando la misma matriz de probabilidad e impacto aplicada para los riesgos de gestión y fiscales, en concordancia con el enfoque de gestión integral del riesgo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – versión vigente del Departamento Administrativo de la Función Pública.

No obstante, debido a la naturaleza de los riesgos asociados a la integridad pública y a las posibles afectaciones institucionales que pueden generar, la CRC adoptará medidas orientadas al fortalecimiento de los controles existentes, aun cuando el riesgo residual se ubique en niveles bajos o moderados dentro de la matriz de valoración.

Lo anterior con el propósito de prevenir la materialización de eventos que puedan afectar la transparencia, la integridad institucional y la confianza en la gestión pública.

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.

Ilustración 10. Tratamiento de riesgos de seguridad y privacidad de la información

BAJO	Aceptar/Evitar/Compartir/Reducir riesgo
MODERADO	Evitar/Compartir/Reducir riesgo
ALTO	Evitar/Compartir/ Reducir riesgo
EXTREMO	Evitar/Compartir/ Reducir riesgo

Fuente: Elaboración propia CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.8 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 gestión integral 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, 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 grupo interno de trabajo de planeación y 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 frente a la gestión integral de riesgos.

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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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 mediante el reporte del estado de los riesgos, la operación de los controles y el avance de los planes de tratamiento, a través de los mecanismos definidos para la gestión integral de riesgos.

   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.

   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 integridad pública 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 parte de la segunda línea de defensa, se deberán presentar dos (2) reportes sobre el estado de los riesgos, a través del Comité Institucional de Coordinación de Control Interno.

f. 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.

7.9 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, integridad pública y fiscales a la Coordinación de Planeación y Gestión. 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?

Para reportar la materialización de los riesgos de seguridad y privacidad de la información se envía un correo con el caso al correo Seguridad Digital CRC <seguridad.digital@crcom.gov.co> para activar el Procedimiento de Gestión incidentes de la coordinación de Tecnologías y Sistemas de Información.