## 1. Derechos de autor



## 2. Acerca de este documento

El Decreto 1083 de 2015, Decreto único del Sector Función Pública, modificado por el Decreto 1499 de 2017, establece el Modelo Integrado de Planeación y Gestión - MIPG, el cual surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo Sistema de Gestión, y de la articulación de este con el Sistema de Control Interno.

Dando cumplimiento a lo anterior mediante la Resolución No. 0327 del 2022 "Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG, se conforma el Comité Institucional de Desempeño en Radio Televisión Nacional de Colombia – RTVC S.A.S y derogan las resoluciones 421 de 2020, 147 de 2018" , y teniendo en cuenta la incorporación de las políticas que la gestión y el desempeño permite asegurar de manera razonable la ejecución de obligaciones, actividades y tareas de acuerdo con lo planeado, contando con controles necesarios para la realización eficiente y efectiva de los planes, programas, proyectos, políticas operacionales y procesos de la entidad, que permitan evidenciar las posibles desviaciones y tomar las decisiones oportunas para el cumplimiento de objetivos, y así controlar la gestión de la entidad con integridad y calidad en el servicio a través del Modelo Integrado de Planeación y Gestión - MIPG.

## 3. Políticas de carácter general o transversal

Los siguientes aspectos descritos, son lineamientos transversales a todos los procesos y contribuyen al buen funcionamiento de la Entidad:

1. Todos los procesos realizan actividades de autocontrol, de acuerdo con el esquema de líneas de defensa indicado en el Modelo Integrado de Planeación y Gestión MIPG.
2. En RTVC SAS son responsables por la organización, conservación, uso y manejo de los documentos en cualquier soporte, todos los servidores y empleados públicos como los colaboradores, aplicarán las normas adoptadas para tal fin por la Entidad, las cuales están basadas en lo establecido por el Archivo General de la Nación[1].
3. Toda comunicación oficial (Comunicaciones recibidas o producidas en desarrollo de las funciones de una entidad, independiente del medio utilizado[2], enviada o recibida debe ser registrada en el sistema de gestión documental Orfeo para oficializar su trámite, asignándoles un consecutivo único de radicado y cumplir con los términos de vencimiento establecidos por la Ley[3].

[1] Artículo 2.8.2.5.3 Decreto 1080 de 2015 Ministerio de Cultura
[2] Acuerdo 027 de 2006 Archivo General de la Nación
[3] Acuerdo 060 de 2001 Archivo General de la Nación

4. En todas las reuniones que se realicen en las áreas, se debe llevar registro de asistencia o acta de reunión, de acuerdo con los formatos establecidos en el Sistema Integrado de Gestión - SIG, así mismo será viable realizar el registro a través de medios electrónico tales como:

    - Módulo de actas en el sistema de planeación y gestión kawak, apta para todo tipo de reuniones y una vez esta se encuentre aprobada, se debe archivar el documento electrónico en pdf.
    - Empleo del formato de "acta de reunión" publicado en el sistema de planeación y gestión kawak, el cual debe ser diligenciado digitalmente, y enviado y aceptado a través de correo electrónico.
    - Formato de asistencia a reuniones diligenciada y aceptadas a través de correo electrónico (este formato de acuerdo con las recomendaciones de la coordinación de talento humano y en el marco del protocolo de bioseguridad, se evitará en la medida de lo posible, ser diligenciado de manera física, esto hasta que dicha coordinación considere lo contrario).

5. Todas las áreas deben estar en constante actualización de la normatividad legal que les aplique para el desarrollo de sus funciones.
6. En todos los procesos de RTVC se da prioridad y estricto cumplimiento a los requerimientos de los órganos de control.
7. Todo trámite, diligencia o proceso adelantado por RTVC, se realiza de conformidad con la normatividad vigente y lo establecido en los diferentes manuales y procedimientos registrados en el sistema integrado de gestión
8. El monitoreo y revisión a los mapas de riesgos debe ser realizado por los responsables de los procesos, como parte del ejercicio de autocontrol; lo anterior, para identificar todas las situaciones o factores que pueden influir en la aplicación de las acciones preventivas.
9. Todas las personas y los procesos deben considerar y aplicar la política operacional de seguridad de la información y seguridad digital de RTVC dentro de sus actividades y como parte de sus responsabilidades para el buen manejo de la información de empresa.
10. Todas las personas y los procesos deben considerar y aplicar la política de protección de datos dentro de sus actividades y como parte de sus responsabilidades para el buen manejo de la información de empresa y de los terceros que tenga en su poder.
11. Todas las personas y los procesos deben considerar y aplicar la política gestión ambiental y los diferentes programas dentro de sus actividades y como parte de sus responsabilidades para el buen manejo de los recursos.

**Política operacional administración de riesgos**

## 4.1 Introducción

Las entidades en su día a día deben enfrentarse a factores internos y externos que pueden crear incertidumbre sobre el logro de sus objetivos. Así el efecto que dicha incertidumbre tiene en los objetivos de una organización se denomina "riesgo" de acuerdo con la Norma Técnica Colombiana NTC-ISO 31000.

El riesgo es un concepto que se puede considerar fundamental, por su vínculo con todo el que hacer. Casi se podría afirmar que no hay actividad de la vida, los negocios, o de cualquier asunto, que no incluya la palabra riesgo. Es por ello por lo que la humanidad desde sus inicios buscó maneras de protegerse contra las contingencias y desarrolló mecanismos para aceptar, evitar, reducir, compartir o asumir riesgos a través de acciones preventivas.

El DECRETO 1083 DE 2015 en el artículo 2.2.21.5.4 define la Administración de riesgos. "Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspecto tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos".

RTVC S.A.S. define su política del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión en los procesos, así como los del Modelo Estándar de Control Interno, en lo referente a las líneas de defensa, los lineamientos de la Guía para la administración del riesgo emitida por el Departamento Administrativo de la Función Pública, la cual articula los riesgos de gestión, fraude, corrupción, de seguridad digital y la estructura del Sistema Integrado de Gestión.

En todos los procesos se deben establecer los lineamientos que permitan la identificación, el análisis, la valoración, el monitoreo y el tratamiento de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales en el marco de los programas, proyectos, planes, procesos, tramites y servicios.

Esta guía de administración del riesgo establece los lineamientos por parte de RTVC S.A.S. para dar cumplimiento con la misión informar, formar y entretener a toda la población colombiana, desde la promoción de una cultura de paz y respeto por los derechos humanos, la diversidad étnica y cultural, la promoción del desarrollo sostenible, que satisfaga las necesidades de los ciudadanos, las audiencias y grupos de valor. La importancia de entender, analizar y comprender los impactos generados por los riesgos permite establecer los planes preventivos que facilitan el control de los riesgos y tener capacidad de respuesta ante su materialización.

## 4.2 Objetivo

Establecer lineamientos para garantizar el cumplimiento de la misión institucional, objetivos estratégicos y de procesos de la entidad a través de la identificación oportuna de riesgos, el análisis y valoración de controles, tipo de manejo y seguimiento de los riesgos aun nivel aceptable, de procesos o gestión, fiscal, de corrupción, de seguridad de la información y seguridad digital, por medio del esquema de líneas de defensa y normatividad aplicable vigente.

Nota: los riesgos y peligros identificados en el marco del sistema de seguridad y salud en el trabajo serán gestionados con los lineamientos definidos por la Coordinación de Talento Humano y normatividad legal vigente, así como los aspectos e impactos identificados en el marco del sistema Gestión Ambiental serán gestionados con los lineamientos definidos por Gestión de relación con los grupos de interés y normatividad legal vigente.

## 4.3 Alcance

Aplica a todos los procesos, programas, proyectos, planes, procesos, trámites y servicios conforme a cada tipo y clasificación de riesgo, inicia desde el análisis de contextos alineados a los objetivos estratégicos y/o de procesos, la identificación, el análisis, valoración de controles, tipo de manejo hasta el seguimiento o monitoreo de estos de acuerdo con el rol y responsabilidad del esquema de líneas de defensa.

Nota: los riesgos y peligros identificados en el marco del sistema de seguridad y salud en el trabajo serán gestionados con los lineamientos definidos por la Coordinación de Talento Humano y normatividad legal vigente, así como los aspectos e impactos identificados en el marco del sistema Gestión Ambiental serán gestionados con los lineamientos definidos por Gestión de relación con los grupos de interés y normatividad legal vigente

## 4.4 Declaración de la Política

Radio Televisión Nacional de Colombia RTVC S.A.S, conscientes de garantizar el cumplimiento de la misión institucional, objetivos estratégicos y de los objetivos de los procesos, se compromete de forma oportuna identificar los riesgos, el análisis, la valoración de controles, el tipo de manejo y seguimiento de los riesgos de procesos o gestión, fiscal, de corrupción, de seguridad de la información y seguridad digital a los que está expuesta, por medio del diseño y ejecución de controles preventivos y detectivos alineados al esquema de líneas de defensa y normatividad aplicable vigente.

## 4.5 Responsabilidades de las Líneas de Defensa

Es la definición de los roles y responsabilidades de la gestión del riesgo y control, a través de los componentes del MECI para evaluar la efectividad de la estructura de control (diseño y ejecución de los controles) aplicables para la entidad.

| ESQUEMA LÍNEAS DE DEFENSA | | | |
|---|---|---|---|
| **LÍNEAS DE DEFENSA** | **RESPONSABLE** | **ROL PRINCIPAL** | **RESPONSABILIDAD** |
| **Estratégica** | Alta Dirección<br><br>Comité de Gestión y Desempeño Institucional<br><br>Comité Institucional de Coordinación de Control Interno | Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad | Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico. |
| | | | Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo) |
| | | | Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. |
| | | | Realizar seguimiento y análisis periódico a los riesgos institucionales, que puedan afectar el cumplimiento de los planes estratégicos |
| | | | Retroalimentar al Comité de Gestión y Desempeño Institucional sobre los ajustes que se deban hacer frente a la gestión del riesgo. |
| | | | Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este. |
| | | | Fortalecimiento del Comité Institucional de Coordinación de Control Interno incrementando su periodicidad para las reuniones. |
| | | | Definición de líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. |
| | | | Evaluación de la política de gestión estratégica del Talento Humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar). |
| | | | Evaluación de la forma como funciona el Esquema de Líneas de Defensa, incluyendo la línea estratégica. |
| **Primera línea de Defensa** | Líderes de programas, procesos y proyectos y sus equipos de trabajo (en general servidores públicos en todos los niveles de la organización) | Mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol" | Identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol". que pueden afectar los programas, proyectos, planes y procesos a su cargo. |
| | | | Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineado con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso, teniendo en cuenta el diseño de dichos controles, evitando la materialización de los riesgos. |
| | | | Realizar el seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda. |
| | | | Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. |
| | | | Informar a la segunda línea, según aplique (Media y Alta Gerencia: Jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, gerencias de riesgos (donde existan), áreas de |

| ESQUEMA LÍNEAS DE DEFENSA | | | |
|---|---|---|---|
| **LÍNEAS DE DEFENSA** | **RESPONSABLE** | **ROL PRINCIPAL** | **RESPONSABILIDAD** |
| | | | contratación, áreas financieras, de TIC, entre otros que generen información para el Aseguramiento de la operación y aporten información para la toma de decisiones), sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo y el plan de mejoramiento aplicado. |
| | | | Realizar seguimiento y análisis a los riesgos y acciones según periodicidad establecida y reportar las evidencias de la gestión de los riesgos a cargo del proceso asociado. |
| | | | Actualizar el mapa de riesgos cuando la administración de estos lo requiera. |
| | | | Conocer y apropiar las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. |
| | | | Formular planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. |
| | | | Coordinar con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa. |
| | | | Aprobar los niveles de aceptación y los controles definidos para mitigar los riesgos en seguridad de la información y seguridad digital.<br>Definir un plan de tratamiento de riesgos para aquellos riesgos que no están en los niveles aceptables. |
| | | | Cuando se presenten materialización de los riesgos mencionados en la política (gestión, corrupción, fiscales, seguridad de la información y seguridad digital); la primera línea de defensa deberá notificar a la segunda y tercera línea de defensa para el correspondiente seguimiento o acciones pertinentes en cada caso. |
| **Segunda línea de Defensa** | Media y Alta Gerencia: jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, áreas de contratación, áreas financieras, de | Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de | Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. |
| | | | Consolidar el Mapa de riesgos institucional y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. |
| | | | Presentar al Comité Institucional de Coordinación de Control Interno el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad. |
| | | | Acompañar y orientar a los líderes de procesos en la identificación, análisis y valoración del riesgo. |

| ESQUEMA LÍNEAS DE DEFENSA | | | |
|---|---|---|---|
| **LÍNEAS DE DEFENSA** | **RESPONSABLE** | **ROL PRINCIPAL** | **RESPONSABILIDAD** |
| | TIC, entre otros que generen información para el Aseguramiento de la operación y aporten información transversal para la toma de decisiones. | prácticas de gestión de riesgo eficaces; así mismo, consolidar y analizar información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos, todo lo anterior enmarcado en la "autogestión". | Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada. |
| | | | Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones. |
| | | | Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. |
| | | | Pertenecer a la media o alta gerencia: Dentro del Organigrama aquellos cargos que dependen del Representante Legal (Alta Gerencia), Para Media Gerencia, aquellos que se desprenden de los cargos anteriormente mencionados. |
| | | | Consolidar y analizar la información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. |
| | | | Trabajar coordinadamente con las oficinas de control interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno. |
| | | | Establecimiento de los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora). |
| | | | Asesoría a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos. |
| | | | Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. |
| | Director de la Dirección de Tecnologías Convergentes | Oficial de Seguridad de la Información | El oficial de seguridad de la información deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes, Primer Línea de Defensa y la coordinación de Tecnologías de la Información -TI, ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado, adicionalmente el oficial de seguridad de la información realiza el seguimiento a la implementación y efectividad de los planes de tratamiento definidos, así como evaluar la eficacia de los controles implementados. Se deben tomar en cuenta eventos o incidentes de |

| ESQUEMA LÍNEAS DE DEFENSA | | | |
|---|---|---|---|
| **LÍNEAS DE DEFENSA** | **RESPONSABLE** | **ROL PRINCIPAL** | **RESPONSABILIDAD** |
| | | | seguridad que hayan afectado a la entidad como insumo para los planes de mejora. |
| **Tercera línea de Defensa** | Jefes de control interno | Liderazgo estratégico, con enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento. todo lo anterior enmarcado en "Evaluación independiente". | Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. |
| | | | Generar a través de su rol de asesoría una orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Planeación |
| | | | Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. |
| | | | Recomendar mejoras a la política de administración del riesgo. |
| | | | Brindar un nivel de asesoría proactiva y estratégica, frente a la Alta Dirección y los líderes de proceso. |
| | | | Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. |
| | | | Informar los hallazgos y proporcionar recomendaciones de forma independiente. |

Tabla 1. Responsabilidades Sobre el esquema de Líneas de Defensa

## 4.6 Mecanismos de Comunicación

RTVC S.A.S. ha establecido a través de las caracterizaciones y/o cartas descriptivas mediante la página web, intranet y la herramienta vigente para la implementación del sistema de gestión vigente. Así como el manual de comunicaciones vigente.

## 4.7 Contexto Estratégico

RTVC S.A.S ha establecido el formato E-F-12 Formato Análisis de Contextos e Identificación de Riesgos, la presente actividad se realiza cada 2 años, con el objetivo de realizar en el primer año el ejercicio de diligenciamiento y en el segundo año se realizará implementación de mejoras y si se presenta la creación de riesgos de gestión y/o corrupción. Lo anterior aplica a todos los procesos y se analiza el contexto externo, interno y del proceso alineado al objetivo del proceso, el Plan Estratégico Institucional y demás factores considerados dentro del documento, con el objetivo de identificar nuevos posibles riesgos y oportunidades de mejora; así mismo se realizará un documento en donde se consigne los resultados generales desde el proceso de Gestión por procesos e innovación, como también servirá de insumo al análisis DOFA, diseñado por la coordinación de planeación para realizar la actualización del plan de acción y/o estratégico.

## 4.8 Herramienta Para la Gestión de Riesgos

RTVC S.A.S. determina que el módulo de riesgos del sistema de Administración y Mantenimiento de Sistemas de Gestión - KAWAK -, es la herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción, fiscal para lo cual la Coordinación de planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento y cargue de información, su funcionamiento está explicado en el instructivo E-I-6 en la versión que se encuentre vigente.

**Nota**: la metodología (identificación, evaluación, valoración) está en el documento Guía código E-G-2

## 4.9 Niveles de Aceptación – Apetito Del Riesgo, Tolerancia del Riesgo y Capacidad del Riesgo

De acuerdo con el apetito al riesgo RTVC S.A.S determina que, para los riesgos residuales de **gestión, fiscal, seguridad de la información y seguridad digital** que se encuentren en zonas de riesgo moderada y baja, está dispuesto a aceptar y/o tolerar el riesgo y no se requiere la documentación de plan de tratamiento, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Los riesgos residuales de **gestión, fiscal, Corrupción, seguridad de la información y seguridad digital** que se encuentren en zonas de riesgo extrema y alta (capacidad del riesgo), **NO** está dispuesto a aceptar el riesgo y de acuerdo con las causas analizar posibles acciones de mejora por medio del plan de tratamiento, de acuerdo con lo indicado en el proceso de segundo nivel E-P-5 Mejoramiento Continuo, así como su monitoreo conforme a la periodicidad establecida para así evitar la materialización sobre los objetivos del proceso y estratégicos.

Los riesgos de corrupción NO TIENEN nivel de aceptación.

## 4.10 Estructura Redacción De Riesgos

A continuación, se describe la redacción de las 4 (cuatro) tipologías de riesgos descritas en esta política:

| | |
|---|---|
| **RIESGO DE GESTIÓN** | Posibilidad de (impacto) + (circunstancia inmediata) + ( causa raíz ) + subcausas<br>¿Qué? ¿Cómo? ¿Por qué? |
| **RIESGO DE CORRUPCIÓN** | Posibilidad de acción u omisión + uso del poder + desviación de la gestión de lo público + para beneficio privado + subcausas |
| **RIESGO FISCAL** | Posibilidad de efecto dañoso sobre (impacto Bienes/Recursos/Intereses Patrimoniales) + ¿Qué?<br>por (circunstancia inmediata) + a casusa de (causa raíz Acción u Omisión) + subcausas<br>¿Cómo? ¿Por qué? |

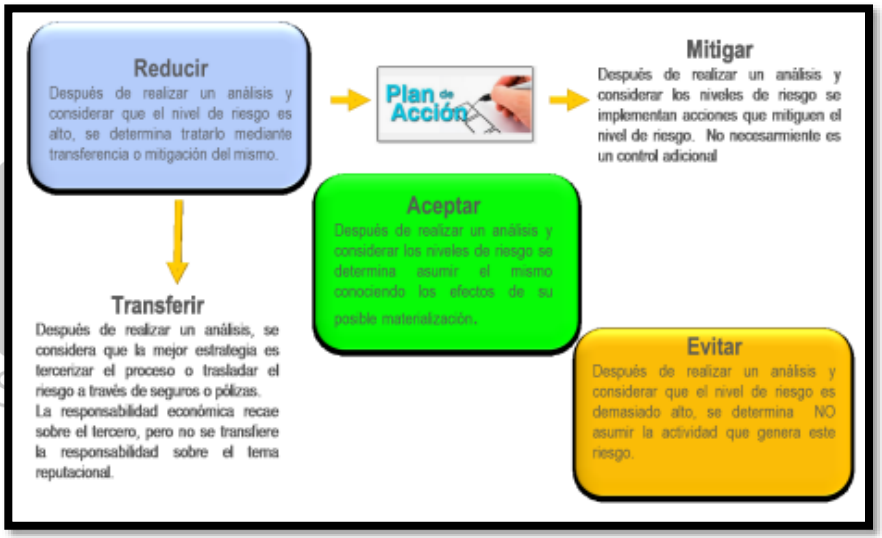
| | |
|---|---|
| **RIESGO DE SEGURIDAD DE LA INFORMACIÓN** | Posibilidad de pérdida de confidencialidad o integridad o disponibilidad + por explotación de la(s) amenaza(s) identificada(s) + debido a (descripción de la(s) vulnerabilidad(es) |

*Tabla 2. Estructura para redacción de cada tipología de Riesgos.*

## 4.11 Tratamiento del riesgo

El tratamiento del riesgo se define como las medidas que toma la entidad para prevenir, mitigar o eliminar el riesgo de acuerdo con las posibilidades de gestión, capacidades de recursos y la naturaleza del riesgo.

Las opciones de tratamiento son: reducir, aceptar, evitar y compartir, tenga en cuenta los lineamientos indicados en la siguiente figura.




Riesgos de gestión, Fiscal, Seguridad de la información y Seguridad Digital:

B: ZONA DE RIESGO BAJA: Aceptar el riesgo.
M: ZONA DE RIESGO MODERADA: Aceptar, reducir o evitar el riesgo
A: ZONA DE RIESGO ALTA: Reducir, evitar el riesgo
E: ZONA DE RIESGO EXTREMA: Reducir, evitar el riesgo

**Para los Riesgos de Seguridad de la información y Seguridad Digital**, cuando se define la opción de reducir el riesgo, se requerirá la definición de un plan de tratamiento que especifique lo siguiente:

1. Responsable
2. Fecha de implementación
3. Fecha de seguimiento

La selección de las opciones para el tratamiento del riesgo debe realizarse de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles.

**Para los riesgos de corrupción,** la respuesta será evitar, compartir o reducir el riesgo. **(Ningún riesgo de corrupción podrá ser aceptado).**

**M → ZONA DE RIESGO MODERADA:** reducir o evitar el riesgo.
**A → ZONA DE RIESGO ALTA:** Reducir, evitar el riesgo.
**E → ZONA DE RIESGO EXTREMA:** Reducir, evitar el riesgo.

En el caso en que se identifique la necesidad de establecer un plan de acción, que es generar acciones para fortalecer el riesgo y sus controles, resúltate de la calificación "reducir" de acuerdo con el estado del riesgo se debe realizar un plan de tratamiento, se indica en el capítulo 4.18.

## 4.12 Realizar Monitoreo - Primera Línea de Defensa

Una vez se han realizado las etapas de identificación, análisis, valoración y manejo de las diferentes tipologías de los riesgos de Gestión, corrupción y Fiscal, será responsabilidad del líder del proceso y su equipo de trabajo de acuerdo al esquema de líneas de defensa al rol y responsabilidad garantizar que se carguen los soportes y/o se indique la ruta en donde están las evidencias de la ejecución de cada control en la plataforma como parte del autocontrol, así mismo realizar el monitoreo conforme a la periodicidad indicada para cada control alineado al riesgo. Cuando realice el monitoreo tenga en cuenta lo siguiente:

- Indicar si se ha o no presentada materialización del riesgo
- Indicar si los controles siguen vigentes y funcionando
- Indicar cuando sean riesgos de corrupción si se han presentado conflictos de intereses
- No olvidar si no va a cargar adjunto como evidencia del control por favor coloque el link y/o enlace de la carpeta compartida en donde se pueda evidenciar los soportes por un tercero, el link no debe estar alineado a persona si no al proceso.

## 4.13 Realizar Seguimiento - Segunda Línea De Defensa – Gestión, Corrupción y Fiscales.

La periodicidad para el seguimiento a los riesgos de gestión, corrupción y Fiscales identificados por parte de los dueños de proceso se realizará así:

a) Riesgos catalogados en la zona Alta y Extrema de manera CUATRIMESTRAL
b) Riesgos catalogados en la zona Moderada de manera SEMESTRAL
c) Riesgos catalogados en la zona Baja de manera ANUAL

### 4.14 Realizar Seguimiento - Segunda Línea De Defensa - Seguridad de la Información y Seguridad Digital.

Coordinación de T.I. programa el seguimiento de la matriz de riesgos de seguridad de la información y seguridad digital y dejan reporte del acompañamiento en el formato de asistencia a reuniones con base en la información suministrada por el líder del proceso y/o su equipo de trabajo.
El seguimiento y la revisión de la matriz de riesgos de seguridad de la información y seguridad digital deben ser realizados por los líderes de procesos con sus equipos de trabajo periódicamente. Si se identifican mejoras como resultado de esta revisión se deben realizar los ajustes correspondientes con el oficial de seguridad de la información.

La Coordinación de T.I a través del oficial de seguridad de la información programa el seguimiento del cumplimiento de la matriz de riesgos de seguridad de la información y seguridad digital y dejan reporte del acompañamiento en el formato de asistencia a reuniones con base en la información suministrada por el líder del proceso y/o su equipo de trabajo, así mismo, presentan al Comité Institucional de Gestión y Desempeño del estado de avance en el desarrollo de esta actividad. Internamente los contratistas que estén asignados a esta actividad reportan a la Coordinación de T.I.; sobre el estado de avance.

Durante el primer semestre de cada vigencia, el colaborador que presta servicios profesionales de la coordinación de T.I., asignado por el coordinador de esta área o de acuerdo con la asignación contractual, programará con el líder del proceso, las fechas en las cual se realizará el acompañamiento al seguimiento de las matrices de riesgos de seguridad de la información y seguridad digital, este acompañamiento no genera evaluaciones positivas o negativas sobre el cumplimiento de los controles o planes de tratamiento, pero si una alerta sobre su ejecución.

| | Matriz de riesgos de Seguridad de la información y Seguridad Digital | |
|---|---|---|
| **Responsable** | La Coordinación de T.I. asigna un responsable de la Seguridad de la información y Seguridad Digital, con las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad de la información y seguridad digital. | |
| **Frecuencia** | Dos veces al año | El seguimiento se realiza 2 veces al año en las siguientes fechas:<br>1. Corte 30 de junio con publicación del seguimiento dentro de los primeros 15 días del mes de julio.<br>2. Corte 31 de diciembre con publicación de seguimiento dentro de los primeros 15 días del mes de enero |
| **Resultado de la revisión** | A partir del resultado generado y del seguimiento al mapa de riesgos de seguridad de la información y seguridad digital, deberá generar un plan de mejoramiento. | |

*Tabla 3. Matriz de riesgos de Seguridad de la información y Seguridad Digital*

Durante el primer semestre de cada vigencia, la Coordinación de T.I., debe suministrar a través de correo electrónico al Coordinador de planeación, el nombre de los profesionales de dicha oficina que serán asignados

al seguimiento de los planes de tratamiento definidos en la matriz de riesgos de seguridad de la información y seguridad digital.

Descripción de las actividades y el responsable:

| ACTIVIDAD | RESPONSABLE |
|---|---|
| Hacer seguimiento a la ejecución de los controles y los eventos de riesgo de Seguridad de la Información y Seguridad Digital | Líder del proceso y colaborador que presta servicios de la gestión de riesgos de seguridad de la información y seguridad digital o quien haga sus veces |
| Revisar y presentar las evidencias de los soportes documentales de la ejecución de los controles | Líder del proceso |
| Revisar e implementar los controles de seguridad de la información según la declaración de aplicabilidad | Colaborador que presta servicios de la gestión de riesgos de seguridad de la información y seguridad digital o quien haga sus veces y la Coordinación de T.I. |
| Realizar Auditorías internas de acuerdo con el Plan anual de auditorias | Asesor de Oficina de Control Interno |

*Tabla 4. Actividades de Seguimiento*

La homologación de la calificación se aclarará en el formato de asistencia a reunión o en el soporte diseñado para el análisis de probabilidad e impacto y se consignará la información en el campo “comentarios” dispuesta por el aplicativo



### 4.14.1 Planes de tratamiento de Riesgos de Seguridad de la Información e Indicadores para la Gestión Del Riesgo

Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se deberán generar como lo indica el Esquema 9. Consolidación de los Planes de Tratamiento de Riesgos, de la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas” emitida por el DAFP.

### 4.15 Realizar seguimiento Independiente - Tercera Línea De Defensa

Para mantener un seguimiento efectivo de la matriz de riesgos de gestión, corrupción, fiscal, seguridad de la información y seguridad digital, se considerarán los siguientes aspectos:

El asesor de Control Interno o quien haga sus veces, en su rol asesor, comunicará y presentará los resultados de seguimiento y evaluación al Mapa de Riesgos de Corrupción, junto con las recomendaciones o acciones de mejora para abordar las situaciones identificadas, conforme al programa anual de auditoría.
Este seguimiento se llevará a cabo de la siguiente manera:

Para los Riesgos de Gestión, fiscales, seguridad de la información y seguridad digital; se realizará seguimiento por medio de auditorías internas establecidas en el programa anual de auditorías. Asimismo, para los riesgos de corrupción, el seguimiento se realizará tres (3) veces al año en las siguientes fechas, acorde a la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas vigente:

1. Corte 30 de abril con publicación del seguimiento dentro de los primeros diez (10) días hábiles del mes de mayo.
2. Corte 31 de agosto con publicación del seguimiento dentro de los primeros diez (10) días hábiles del mes de septiembre.
3. Con corte 31 de diciembre con publicación del seguimiento dentro de los primeros diez (10) días hábiles del mes de enero.

La oficina de control interno deberá adelantar las siguientes actividades:

- Verificar la publicación del mapa de riesgos de corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Evaluar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

## 4.16 Registrar Materialización y/o Eventos

Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas económicas y/o reputacional a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Nota: Tener en cuenta que independientemente del estado del riesgo si se llegara a materializar se debe registrar de forma inmediata la materialización de este por parte de líder o persona asignada por el proceso con acompañamiento del enlace del sistema Integrado de gestión.

Tener en cuenta:

- Se debe revisar el riesgo, las causas y/o controles existentes que se hayan materializaron o identificar si es una nueva causa por la cual se haya materializado el riesgo; así mismo si es necesario ajustar (crear o actualizar) los controles del riesgo y crear una acción correctiva en la opción del plan de tratamiento y actualizar el plan de contingencia de acuerdo con lo evidenciado en la materialización.

## 4.17 Inactivar Riesgos

Si el proceso de acuerdo con necesidad desea inactivar un riesgo de gestión, corrupción y/o fiscal deberá justificar los motivos y la decisión estará a cargo para aprobación del equipo SIG, así mismo deberá quedar como documento un acta de evidencia del análisis y decisión junto con los líderes de los procesos.

### 4.18 Generar Plan de Tratamiento

Se debe implementar un plan de tratamiento cuando: el riesgo se materialice, de acuerdo con el apetito al riesgo cuando estén los riesgos en estado extremo y alto, cuando las causas denoten debilidad en tema documental u otro aspecto que de conformidad con el proceso y la segunda línea de defensa analicen en común acuerdo su creación. (ver instructivo E-I-6 en la versión que se encuentre vigente).

### 4.19 Publicación

La Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. Así mismo se publican de forma consolidada con los riesgos de gestión y fiscal.

Por otra parte, se deberá publicar con corte a 30 de junio (julio) y 30 de diciembre (diciembre) el mapa de riesgos institucional consolidado (Gestión, Corrupción y Fiscal) en la página web de la entidad.

La publicación del mapa de riesgos de seguridad de la información y seguridad digital se realiza en la intranet de RTVC S.A.S., se actualizará durante el primer semestre del año y su fecha de publicación límite en la intranet será el 31 de agosto de cada vigencia.

La publicación de los informes de seguimiento por parte de la tercera línea de defensa a los riesgos de corrupción, se realizarán los 10 (diez) primeros días hábiles en los meses de mayo, septiembre y enero; acorde a lineamientos de la guía para la administración del riesgo y el diseño de controles en entidades públicas.

### 4.20 Socialización

Desde la coordinación de Planeación se realizará las siguientes actividades para socializar el informe y el mapa de riesgos consolidado (gestión, corrupción y Fiscal):

- ✓ El equipo de planeación notificará a través de correo electrónico institucional a toda la entidad que ya se encuentra publicado para su respectiva consulta.

- ✓ En el marco del comité institucional de gestión y desempeño, se presentará el estado, alertas, conclusiones y recomendaciones para la mejora continua.

- ✓ Anualmente la coordinación de planeación realizará una actividad de participación ciudadana con el apoyo de la coordinación de comunicaciones, para invitar interna y externamente a la ciudadanía a realizar la revisión del informe y el mapa de riesgos y recibir sus sugerencias y/o aportes y realizar acciones de mejora.

- ✓ Realizar como mínimo una vez al año una reunión con los enlaces de los procesos, líderes y personal asignado para socializar el informe y los mapas de riesgos.

- ✓ En los procesos de inducción/reinducción y entrenamiento de los colaboradores y servidores de RTVC S.A.S. se expondrá la importancia de conocer los riesgos, de identificarlos, valorarlos y controlarlos.

- ✓ Realizar 2 veces al año el respectivo informe con sus anexos y mapas de riesgos institucionales.

### 4.21 Control de Cambios

Ver historial de cambios en el aplicativo kawak - Modulo riesgos.

**Nota: La presente política fue aprobada en el comité Institucional de Coordinación de Control Interno (CICCI), fecha 11 de diciembre del 2024.**