METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES

CONTRALORIA GENERAL DE SANTIAGO DE CALI

Santiago de Cali
Distrito Especial

TABLA DE CONTENIDO

Pág.

0. PRESENTACIÓN

En el marco de la implementación de los Sistemas de Gestión de Calidad y del Modelo Integrado de Planeación y Gestión MIPG, en la Contraloría General de Santiago de Cali, en adelante CGSC, se plantea la necesidad de establecer la metodología, correspondiente al componente Administración de Riesgos; dicho componente tiene una importancia vital para el buen funcionamiento de las entidades del sector público y es por esto, que la metodología aquí planteada es acorde con el proceso de mejora de la administración pública; de esta forma se da cumplimiento a lineamientos nacionales sobre el control interno que deben ejecutar las organizaciones públicas.

La CGSC plantea y adopta la siguiente metodología, tomando como referencia la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas[1], lo cual conduce a una gestión pública más eficiente y sirve para que se cumpla con los objetivos institucionales.

La consigna es que la implementación de una Administración de Riesgos efectiva, eficiente y transparente, sea una práctica incorporada al interior de la Entidad como una política de gestión por parte de la alta dirección y cuente con la participación y respaldo de todos los servidores públicos; tarea que se facilitará con la implementación de la metodología aquí presentada, la cual permite prevenir los riesgos que en la CGSC amenacen sus objetivos y funcionamiento, fortaleciendo de esta manera el Sistema de Control Interno para lograr el más alto grado de eficiencia.

También, con ocasión de la entrada en vigencia del Modelo Integrado de Planeación y Gestión MIPG, que integra los Sistemas de Gestión de la Calidad y de Desarrollo Administrativo, crea un único Sistema de Gestión y lo articula con el Sistema de Control Interno, el cual se actualiza y alinea con los mejores estándares internacionales como son el Modelo COSO 2013, COSO ERM 2017 y el Modelo de las Tres Líneas de Defensa, con el fin de entregar a los ciudadanos, lo mejor de la gestión para producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción.

Objetivos.

- Unificar los lineamientos metodológicos para la administración de todo tipo de riesgos y fortalecer el enfoque preventivo con el fin de facilitar la identificación y tratamiento de cada uno de ellos.

- Suministrar una metodología que permita a todos los procesos de la entidad gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso.

- Ofrecer herramientas para identificar, analizar, mitigar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores de la entidad (Esquema de las Líneas de Defensa).

- Suministrar lineamientos basados en una adecuada gestión del riesgo y control que permitan a la alta dirección tener una seguridad razonable en el logro de sus objetivos.

[1] Versión 6 de 2022, elaborado por la Dirección de Gestión y Desempeño Institucional de la FUNCIÓN PÚBLICA.

Conceptos básicos relacionados con el Riesgo

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de Gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Gestión del Riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad

inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Mapa de Riesgos: Documento con la información resultante de la gestión del riesgo.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Control: Medida que modifica al riesgo (Procesos, políticas, dispositivos, prácticas u otras acciones)

Amenazas: Causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de exactitud y completitud.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Apetito al riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Tolerancia al riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

<u>Antes de Iniciar con la Metodología</u>

¿Qué establece MIPG?

El Modelo Integrado de Planeación y Gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, este modelo tiene el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio (Manual operativo MIPG).

El MIPG opera a través de 7 dimensiones (talento humano, direccionamiento estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y, finalmente, control interno) que agrupan las políticas de gestión y desempeño institucional y que, implementadas de manera articulada e interrelacionada, permitirán que el modelo funcione y opere adecuadamente.

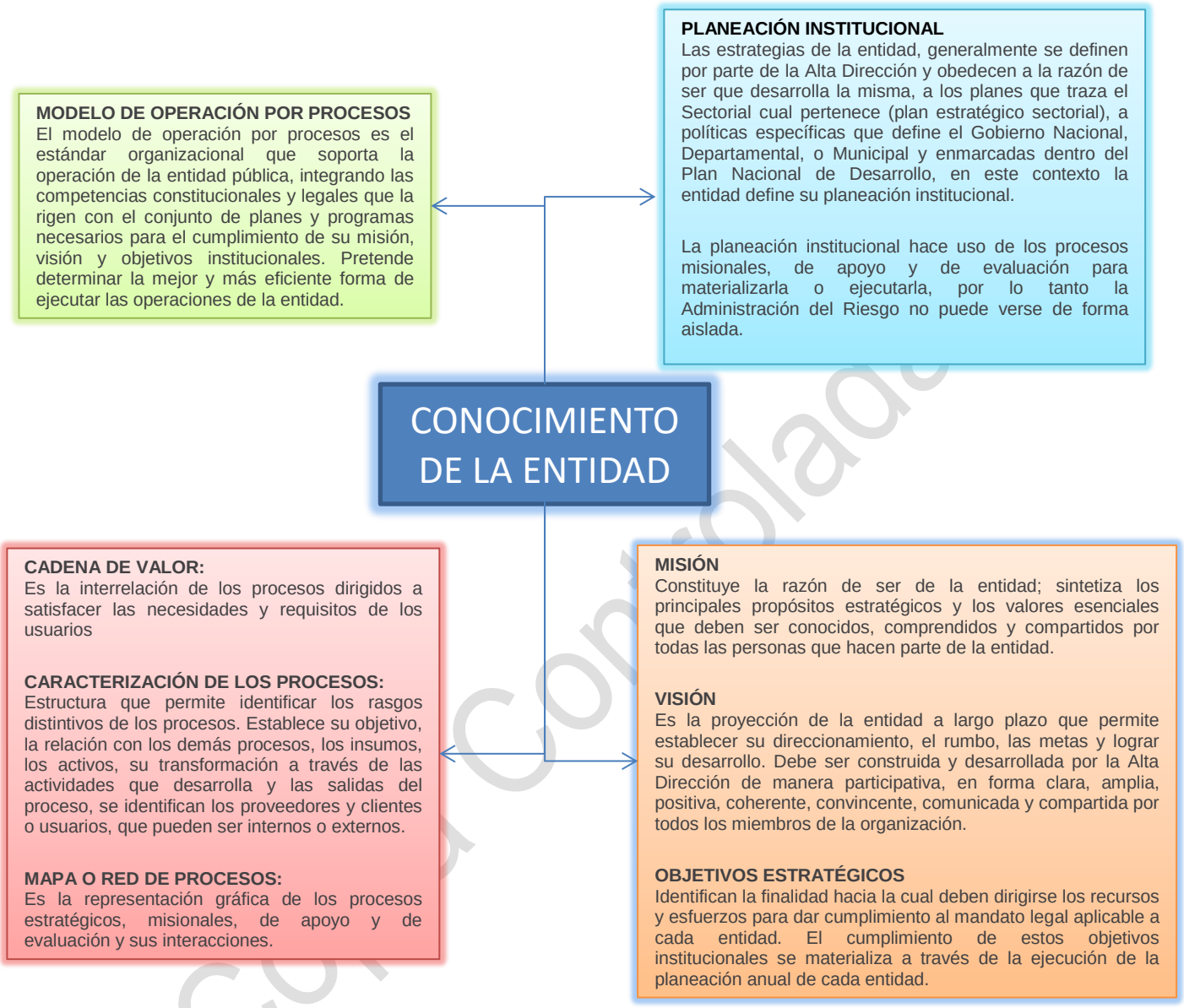
El numeral 2.2.1 “Política de Planeación institucional” de la dimensión “Direccionamiento Estratégico y Planeación” menciona que, para responder a la pregunta ¿cuáles son las prioridades identificadas por la entidad y señaladas en los planes de desarrollo nacionales y territoriales?, se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

De igual forma, se menciona en esta dimensión que, para llevar a cabo el ejercicio de planeación, la entidad debe documentar dicho ejercicio en donde se describa la parte conceptual u orientación estratégica; y la parte operativa en la que se señale de forma precisa los objetivos, las metas y resultados a lograr, las trayectorias de implantación o cursos de acción a seguir, cronogramas, responsables, indicadores para monitorear y evaluar su cumplimiento y los riesgos que pueden afectar tal cumplimiento y los controles para su mitigación.

Importante: En atención a lo que establece COSO 2013 y COSO ERM 2017, los planes, programas o proyectos deben contemplar los riesgos para su ejecución y logro de sus objetivos.

Una vez determinados estos lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos, planeación institucional, entre otros aspectos, permitiendo conocer y entender la entidad, y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

Esquema 1 Conocimiento de la entidad



Importante. Para los objetivos de los procesos como punto de partida fundamental para la identificación del riesgo tenga en cuenta lo siguiente:

OBJETIVO DEL PROCESO. Resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción por lo tanto debe iniciarse con un verbo fuerte como: Establecer, identificar, recopilar, investigar, registrar, buscar.

Los objetivos deben ser: Medibles, realistas y se deben evitar frases subjetivas en su construcción.

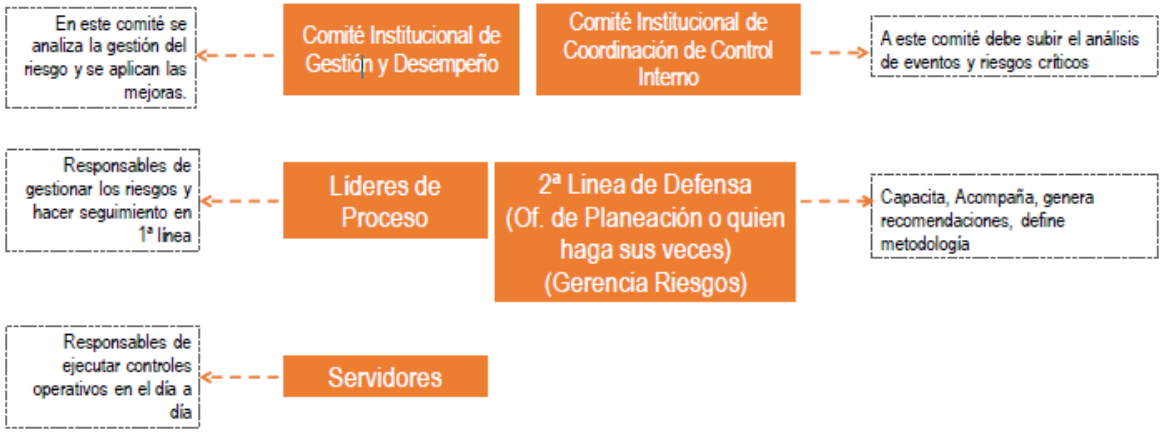
Acerca de la metodología

Una vez determinados estos lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos y planeación institucional, entre otros aspectos, esto permite conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

Institucionalidad

El modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

Esquema 2 Operatividad Institucionalidad para la Administración del Riesgo



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

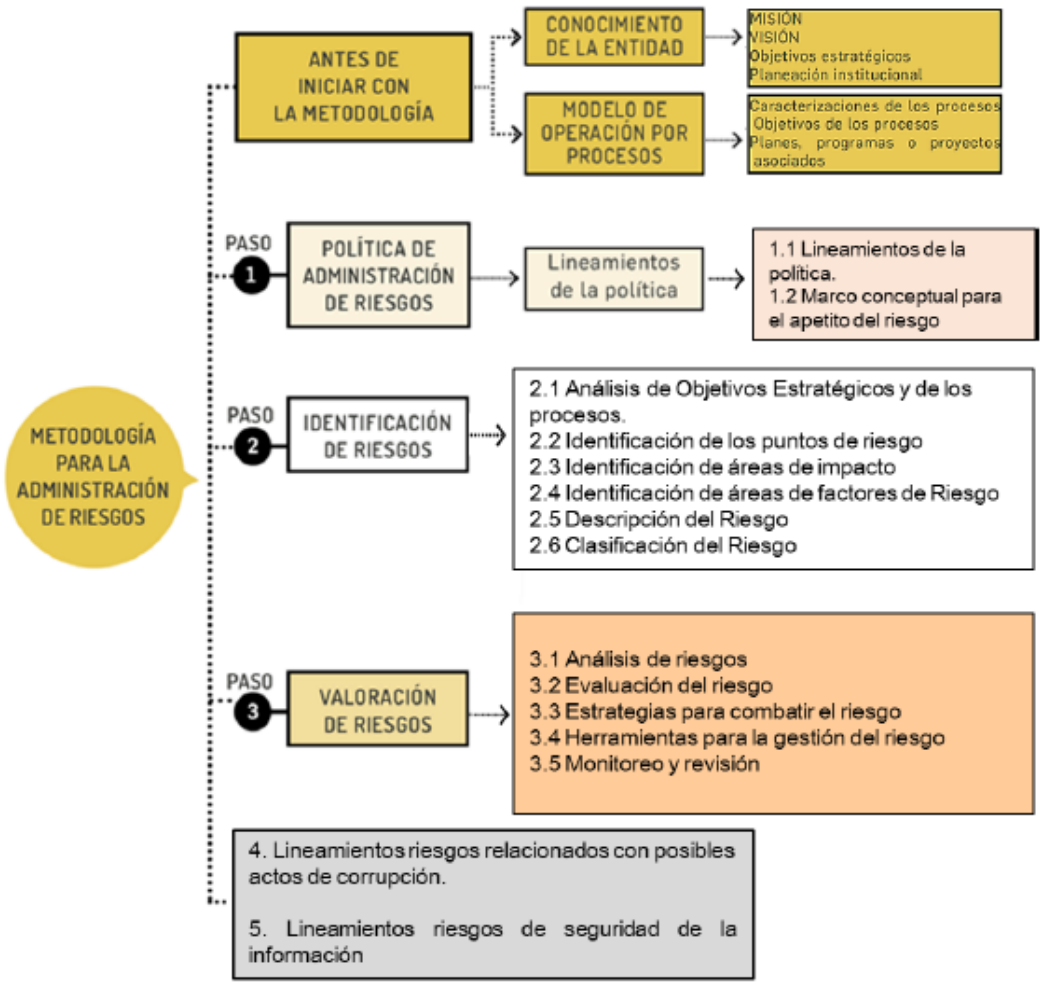
Beneficios

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones
- Garantizar la operación normal de la organización
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
- Fortalecimiento de la cultura de control de la organización
- Incrementa la capacidad de la entidad para alcanzar sus objetivos
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente

La metodología para la Administración del Riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, el conocimiento de esta desde un punto de vista estratégico, de la aplicación de tres (3) pasos básicos para su desarrollo y de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Esquema 3 Metodología para la Administración del Riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

PASO 1: POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

1.1 Lineamientos de la Política

Estructura de la política de administración de riesgos

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

¿QUÉ ES?

Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

¿QUIÉN LA ESTABLECE?

La Alta Dirección de la entidad
Con el liderazgo del representante legal
Con la participación del Comité Institucional de Coordinación de Control Interno

¿QUÉ SE DEBE TENER EN CUENTA?

Objetivos estratégicos de la entidad
Niveles de responsabilidad frente al manejo de riesgos
Mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad

¿QUÉ DEBE CONTENER?

Objetivo:	Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.
Alcance:	La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información (ver caja de herramientas)
Niveles de aceptación al riesgo:	Decisión informada de tomar un riesgo particular (NTC GTC137, Numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.
Niveles para calificar el impacto:	Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario coniderar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos).
Tratamiento de riesgos:	Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1.).
Periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual.	

Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de la Administración del riesgo, a su vez transmite la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad. Estas se fundamentan en las medidas de respuesta que se derivan de las diferentes zonas de riesgo identificadas en la matriz de riesgo.

Para la consolidación de las Políticas de Administración de Riesgos se deben tener en cuenta todas las etapas consideradas en la Guía Metodológica de administración de riesgos.

Con la entrada en vigencia del decreto 1499 de 2017 del Modelo Integrado de Planeación y Gestión (MIPG), que integra los Sistemas de Gestión de la Calidad y de Desarrollo Administrativo, crea un único Sistema de Gestión y, lo articula con el Sistema de Control Interno, el cual se actualiza y alinea con los mejores estándares internacionales como son el Modelo COSO 2013, COSO ERM 2017 y el Modelo de las Tres Líneas de Defensa, con el fin de entregar a los ciudadanos, lo mejor de la gestión para producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción.

La política de administración de riesgo establece las guías de acción necesarias a los funcionarios de la Contraloría General de Santiago de Cali, para coordinar y administrar los eventos que pueden inhibir el logro de los objetivos de la entidad, capacitándolos y habilitándolos para ello.

Identifica las opciones para tratar y manejar los riesgos que basadas en la valoración, permiten tomar decisiones adecuadas acerca de si se acepta, se elimina, se evita, se reduce, se comparte un riesgo o se transfiere legalmente el impacto. Trasmiten la posición de la dirección respecto al manejo de los riesgos y fijan lineamientos sobre los conceptos de calificación de riesgos, las prioridades en la respuesta, la forma de administrarlos y la protección de los recursos.

Apetito del riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Aceptar un riesgo: significa asumirlo, porque su frecuencia es muy baja y no representa ningún peligro para la entidad.

Reducir el riesgo: implica tomar medidas encaminadas a disminuir tanto la frecuencia (medidas de prevención), como el impacto (medidas de protección).

Compartir el riesgo: reduce su efecto a través de la transferencia de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

Evitar o Eliminar el riesgo: cuando su frecuencia y gravedad son altas.

Cabe señalar que para los riesgos de corrupción, de fraude y fiscales las acciones que debe tener en cuenta la alta dirección para su administración son:

Evitar o Eliminar el riesgo: "Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas".

Reducir el riesgo: Implica tomar las medidas encaminadas a disminuir la probabilidad (medidas de prevención). "La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles".

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: La implementación de las políticas de administración de riesgos que se presentan en este documento.

OBJETIVO GENERAL

Establecer las políticas para el manejo de Administración de Riesgos de la Contraloría General de Santiago de Cali, de acuerdo a los lineamientos establecidos por el Departamento Administrativo de la Función Pública, Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, con el fin de aplicar medidas necesarias que permitan administrar los riesgos identificados, prevenirlos y corregir las desviaciones que puedan afectar el logro de los objetivos institucionales y de proceso.

OBJETIVOS ESPECÍFICOS

- Proteger los recursos de la Contraloría General de Santiago de Cali, resguardándolos contra la materialización de los riesgos.

- Revisar y ajustar dentro de los procesos y procedimientos las acciones de mitigación resultado de la administración del riesgo.

- Involucrar y comprometer a todos los servidores de la Contraloría General de Santiago de Cali, en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.

- Asegurar el cumplimiento de normas, leyes y regulaciones.

METAS DE LA ADMINISTRACIÓN DE RIESGOS

Lograr una eficaz, eficiente y efectiva administración de las acciones conducentes a la mitigación, control y prevención de materialización de los riesgos.

ALCANCE DE LA ADMINISTRACIÓN DE RIESGOS

La administración de riesgos en la Contraloría General de Santiago de Cali, abarca la totalidad de los procesos descritos en el documento “Mapa de procesos” código FOR-P2-92.

ESTRATEGIAS PARA EL LOGRO DE LOS OBJETIVOS

- Evaluar periódicamente los eventos negativos tanto internos como externos que puedan afectar la administración de la Contraloría General de Santiago de Cali.

- Monitorear permanentemente por medio del aplicativo www.mecicalidad.com, las acciones de mitigación de los riesgos y los controles preventivos de los mismos, por parte de los procesos.

- Realizar seguimiento y evaluación por parte de la Oficina de Control Interno, (tercera línea de defensa) a las acciones de mitigación de los riesgos mediante las cuales se implementan o fortalecen los controles preventivos y correctivos, validando que la línea estratégica, la primera línea y segunda línea de defensa cumpla con sus responsabilidades.

- Fortalecer la cultura del autocontrol, involucrando a todos los servidores de la Entidad (comités de coordinación y seguimiento), en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.

- Involucrar al Equipo Operativo MIPG dentro de los temas a tratar referente a la administración de los riesgos.

- Actualizar al personal de la Entidad, en desarrollo normativo y legal, en cumplimiento del principio de la autorregulación.

POLÍTICA GENERAL

Con el fin de garantizar el logro misional de la Contraloría General de Santiago de Cali, se ha definido que la Administración de Riesgos tendrá un carácter prioritario y estratégico asociado al Modelo de Operación por Procesos y El Modelo Integrado de Planeación y Gestión- (MIPG).

La Contraloría General de Santiago de Cali se compromete a ejercer el control efectivo de los eventos de riesgo que puedan impedir el cumplimiento de la misión y objetivos institucionales y de proceso a través del diagnóstico, identificación, análisis, valoración y administración del riesgo, orientado al mejoramiento continuo de los procesos gerenciales, misionales, de apoyo y de evaluación de la entidad.

POLÍTICAS ESPECÍFICAS

Generar una visión sistémica acerca de la administración y evaluación de riesgos, consolidada en un ambiente de control que estimule la cultura de la identificación y prevención del riesgo, definiendo las políticas, propiciando los espacios y asignando los recursos necesarios, con canales directos de comunicación y el apoyo a todas los responsables de los procesos de la entidad que permitan propiciar las condiciones necesarias para la aplicación de las siguientes políticas:

- Fortalecer la implementación y desarrollo de la política de administración del riesgo, a través del adecuado tratamiento de los riesgos para garantizar el cumplimiento de la misión y los objetivos institucionales y de proceso, mejorando el desempeño de la entidad.

- Promover la cultura del autocontrol y de la identificación y prevención del riesgo.

- Identificar las acciones para administrar los riesgos con base en su valoración, que permitan tomar decisiones adecuadas para evitar, reducir, compartir, transferir o asumir los riesgos. Para el caso de los riesgos de corrupción los criterios de evaluación para la toma de decisiones adecuadas son eliminar o reducir, evitar o reducir el riesgo.

- El monitoreo está a cargo de los responsables de cada proceso, (Primera línea de defensa) y lo realizan mensualmente en los Comités de Coordinación y Seguimiento, evaluando la eficacia de las acciones adelantadas durante dicho periodo y el registro de la materialización lo consignan en los formatos “Seguimiento actividades de control mapa de riesgos FOR-P02-157 y Registro de materialización de riesgos FOR-P02-158 y los remiten bimestralmente (con corte a febrero 28, abril 30, junio 30, agosto 30, octubre 31 y diciembre 31) a la Oficina Asesora de Planeación, Normalización y Calidad.

- Para el seguimiento a los riesgos de corrupción, el Jefe de Control Interno o quien haga sus veces, (Tercera Línea de Defensa) debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- La Oficina de Control Interno (Tercera Línea de Defensa) realizará seguimiento (tres) 3 veces al año, así: Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo. Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre. Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

- La Oficina Asesora de Planeación, Normalización y Calidad (Segunda Línea de Defensa) socializa a todos los Servidores públicos de la Contraloría General de Santiago de Cali CGSC la metodología de control de riesgos, que contiene la política para su administración en capítulo aparte y el mapa de riesgos y su constante actualización a través de las herramientas de comunicación interna, como su publicación en la página WEB de la entidad.

CRITERIOS DE EVALUACIÓN

De acuerdo con la Metodología para la Administración de Riesgos adoptada y la matriz de riesgos generada para la entidad a partir de la aplicación de la metodología, se establecen los siguientes criterios de evaluación de los riesgos en cada una de las zonas así:

- Los riesgos que se encuentran en **Zona Baja** implican que se debe **Aceptar el riesgo**, significa asumirlo, porque su frecuencia es muy baja y no representa ningún peligro para la entidad.

- Los riesgos que se encuentran en **Zona Moderada** significan que se debe Reducir el riesgo, lo que implica tomar medidas encaminadas a disminuir tanto la frecuencia con medidas de prevención, como reducir la gravedad del impacto adoptando medidas de protección.

- Los riesgos que se encuentran en **Zona Alta** significan que se debe **Compartir el riesgo**, reduce su efecto a través de la transferencia de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

- Los riesgos que se encuentran en **Zona Extrema** significan que se debe **Evitar o Eliminar el riesgo**, cuando su frecuencia y gravedad son altas. Dándole un manejo prioritario a las acciones y recursos que se demanden para su gestión.

Los riesgos de corrupción se encuentran en la Zona Moderada, Zona Alta y Zona Extrema, debido a que el impacto siempre será negativo.

RESPONSABILIDAD

La administración de riesgos es responsabilidad de todos los servidores públicos de Contraloría General de Santiago de Cali, la entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Planeación y Gestión- (MIPG) en la dimensión 7 “Control Interno” desarrolla a través de las Líneas de Defensa la responsabilidad de la gestión del riesgo y control.

¿Cómo se define el modelo de las líneas de defensa?

Es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

¿Quiénes son los asignados para monitorear y revisar la gestión de riesgos y cuáles son sus roles?

El monitoreo y revisión de la gestión de riesgos, está alineado con la dimensión del MIPG de “Control Interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue:

Línea Estratégica: Define el marco general para la gestión del riesgo, el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

1ª. Línea de defensa: Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los líderes de los procesos.

2ª. Línea de defensa: Asiste y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los Riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar, tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.

3ª. Línea de defensa: Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Está conformada por la Oficina de Control Interno.

MAPA DE RIESGOS

El mapa de riesgos es la herramienta conceptual y metodológica que permite valorar y monitorear los riesgos al interior de la Contraloría y estará compuesto por los riesgos de Gestión, Corrupción y Seguridad Digital definidos conforme a la metodología adoptada por Contraloría General de Santiago de Cali.

En caso de modificarse el contexto estratégico, los objetivos estratégicos o de Proceso, se deben ajustar o identificar nuevos riesgos. Para el ajuste o identificación de estos, las propuestas se harán por parte de los líderes de cada proceso (Primera Línea) siguiendo la metodología de administración de riesgos y se presentarán al área de Planeación, Normalización y Calidad, (Segunda Línea) la cual los consolidara y presentara posteriormente al Comité Institucional de Gestión y Desempeño para su aprobación.

Para el ajuste o identificación de nuevos riesgos, se realizará en el comité de Coordinación y Seguimiento de cada área y/o proceso correspondiente (Primera Línea), teniendo en cuenta la metodología de administración de riesgos y se remiten al área de Planeación, Normalización y Calidad, (Segunda Línea) para actualización del mapa de riesgos.

SEGUIMIENTO

El monitoreo y seguimiento es esencial para asegurar que las acciones se están llevando a cabo y evaluar la efectividad de cada uno de los controles existentes en términos de la materialización o no de los riesgos.

El monitoreo está a cargo de los responsables de los procesos, (Primera Línea) la cual se encargará de diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.

La oficina de planeación, (Segunda línea) monitoreara la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

La Oficina de Control Interno, (Tercera Línea) Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

Importante: Los riesgos de corrupción no admiten aceptación del riesgo, siempre debe conducir a un tratamiento. Todos los procesos son susceptibles frente a los riegos de corrupción.

PERIODO DE REVISIÓN DEL RIESGOS INSTITUCIONALES

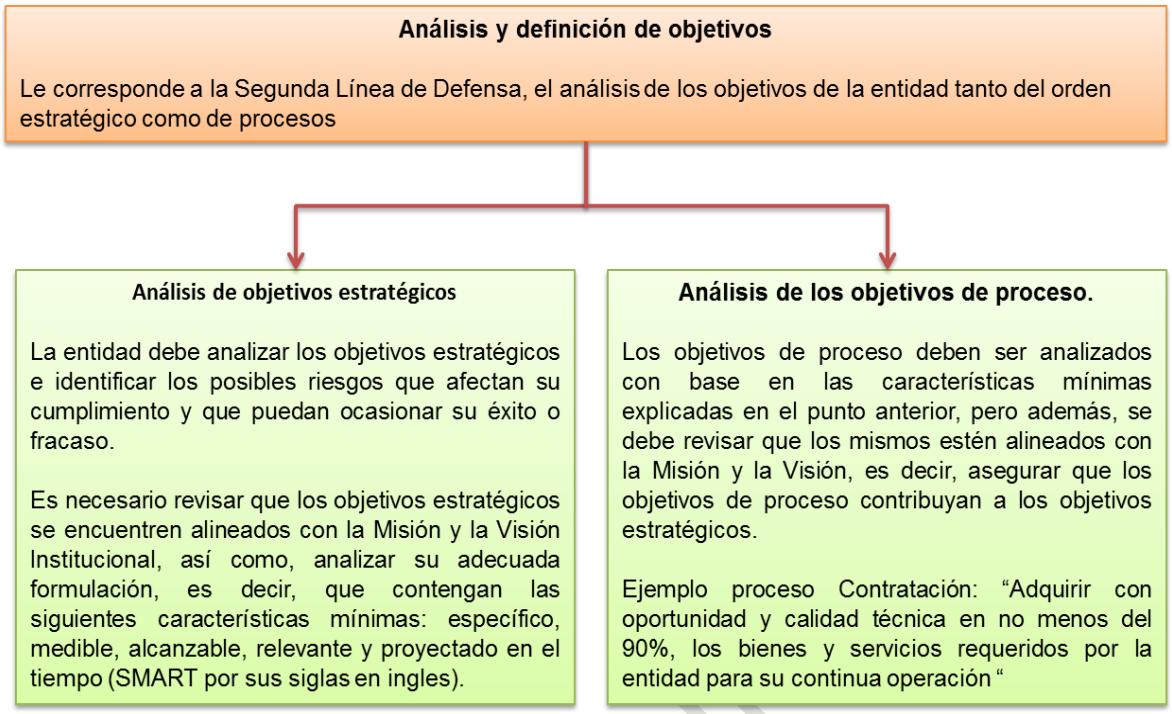
Los riesgos asociados al logro de los objetivos de los procesos institucionales, se identifican y/o validan en cada vigencia por los líderes de proceso con sus respectivos equipos de trabajo con el acompañamiento de la Oficina Asesora de Planeación a través de la metodología propia de la CGSC.

ELIMINACIÓN RIESGOS IDENTIFICADOS

Los riesgos que se encuentren en nivel de aceptación BAJO, que soporten documentación de sus controles en sus procedimientos y evidencien implementación de sus controles existentes y no presenten materialización durante los últimos 5 años, pueden ser considerados para su eliminación.

Importante. Concluida la vigencia, se realiza revisión del periodo anual de monitoreo, analizando los datos por diferentes fuentes de información, de la frecuencia de eventos adversos y materialización de riegos, para establecer el desplazamiento de cada riesgo en el mapa de calor: una casilla hacia abajo en eje de probabilidad en caso de no materializarse o una casilla hacia arriba en caso contrario. Para los riesgos que cuentan con plan de contingencia para mitigación de los impactos el desplazamiento se aplicaría también para el eje de impacto hacia la izquierda en iguales condiciones.

PASO 2: IDENTIFICACIÓN DE RIESGOS



Fuente: Comité of Sponsoring Orgizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio Pág. 73. 2013

Importante: Los objetivos deben incluir el "qué", "cómo", "para qué", "cuándo", "cuánto". Si no están bien definidos los objetivos, no se puede continuar con la metodología de gestión del riesgo.

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características SMART[2], cuya estructura se explica a continuación:

[2] Hace referencia a las siglas en inglés que responden a: specific (específico); mensurable (medible); achievable (alcanzable); relevant; (relevante); timely (temporal)

S ***Specific* (específico):** Lo importante es resolver cuestiones como: qué, cuándo, cómo, dónde, con qué, quién. Considerar el orden y los necesarios para el cumplimiento de la misión.

M ***Mensurable* (medible):** Para ello es necesario involucrar algunos números en su definición, por ejemplo, porcentajes o cantidades exactas (cuando aplique).

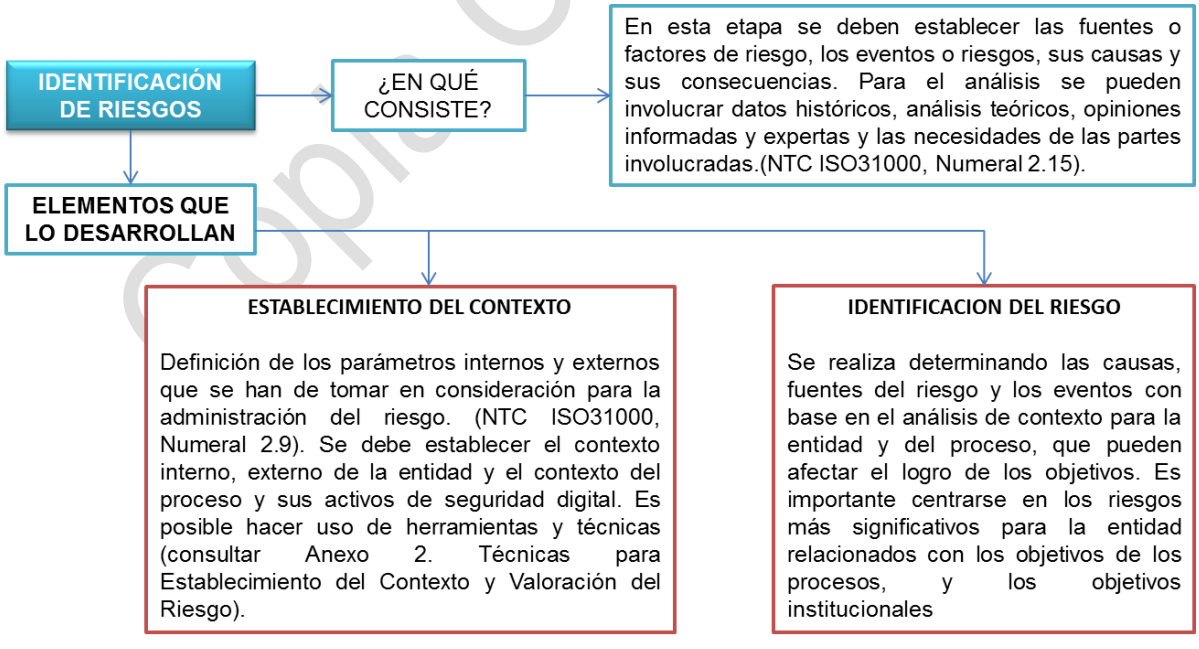
A ***Achievable* (alcanzable);** Para hacer alcanzable un objetivo se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudará a saber si lo que se propone es posible o cómo resultaría mejor.

R ***Relevant* (relevante):** Considerar recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación.

T ***Timely* (temporal):** Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Esquema 4. Aspectos a desarrollar en la Identificación del Riesgo



Importante: Debe analizarse en cada entidad el contexto particular al que se enfrentan los procesos ante los riesgos de corrupción, conforme a la misionalidad

2. Análisis del contexto externo, interno y del proceso

2.1 Establecimiento del Contexto

Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC-ISO 31000). A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

2.1.1 Establecimiento del contexto interno

Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos. Se pueden considerar factores como:

- **Financieros:** Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
- **Personal:** Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
- **Procesos:** Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
- **Tecnología:** Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
- **Estratégicos:** Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
- **Comunicación interna:** Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

2.1.2 Establecimiento del contexto externo

Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:

- **Económicos:** Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
- **Políticos:** Cambios de gobierno, legislación, políticas públicas, regulación.
- **Sociales:** Demografía, responsabilidad social, orden público.
- **Tecnológicos:** Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
- **Medioambientales:** Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.

- **Comunicación externa:** Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.

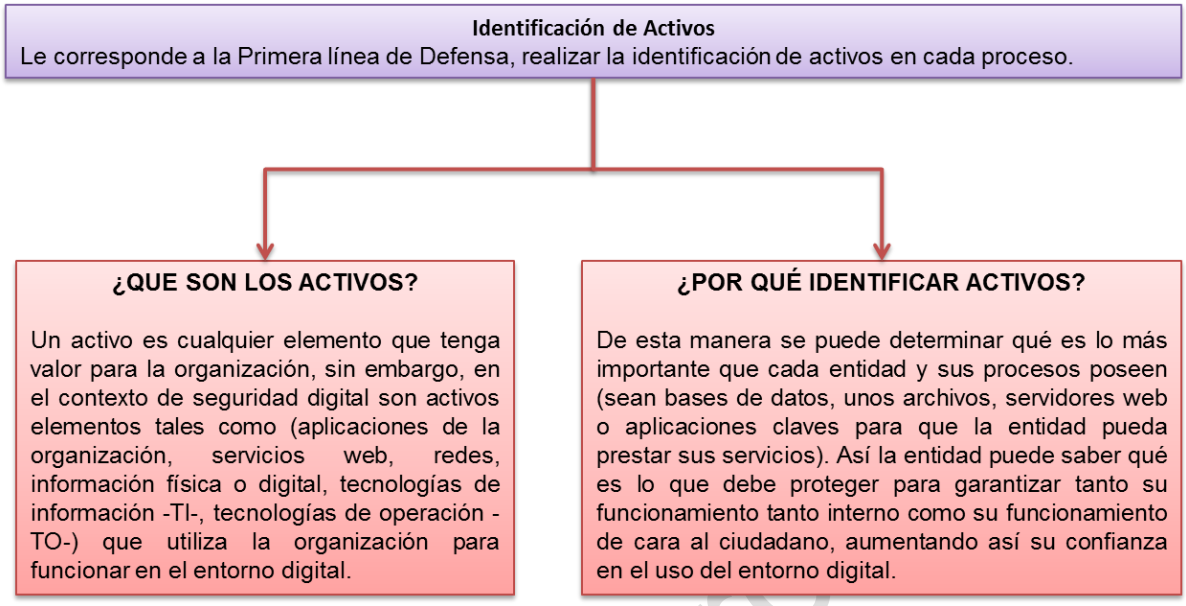
2.1.3 Establecimiento del contexto del proceso

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como:

- **Diseño del proceso:** Claridad en la descripción del alcance y objetivo del proceso.
- **Interacciones con otros procesos:** Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- **Transversalidad:** Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
- **Procedimientos asociados:** Pertinencia en los procedimientos que desarrollan los procesos.
- **Responsables del proceso:** Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- **Comunicación entre los procesos:** Efectividad en los flujos de información determinados en la interacción de los procesos.
- **Activos de seguridad digital del proceso**: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso.

Importante: Como herramienta básica para el análisis del contexto del proceso se sugiere utilizar las caracterizaciones de estos, donde es posible contar con este panorama. Si estos documentos están desactualizados o no se han elaborado, es importante actualizarlos o elaborarlos antes de continuar con la metodología de administración del riesgo.

2.1.4 Identificación de Activos de seguridad de la información



Importante: Todo lo que no está plenamente identificado, no está debidamente asegurado.

¿Cómo Identificar los Activos?

Importante: Para realizar la identificación de activos y la gestión (relacionados con seguridad digital), deberá remitirse a la “Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas”, que hace parte de la presente metodología.

2.2 Identificación de los puntos de riesgos - Técnicas para la identificaron del riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

La identificación del riesgo se realiza determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del Proceso o estratégicos.

Las preguntas claves para la identificación del riesgo permiten determinar:

¿Qué puede suceder? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿Cómo puede suceder? Establecer las causas a partir de los factores determinados en el contexto

¿Cuándo puede suceder? Determinar de acuerdo al desarrollo del proceso

¿Qué consecuencias tendría su materialización? Determinar los posibles efectos por la materialización del riesgo.

Importante: En la descripción del riesgo se deben tener en cuenta las respuestas a las preguntas arriba mencionadas.

2.3 Identificación de áreas de impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

2.4 Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la Tabla 1 encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

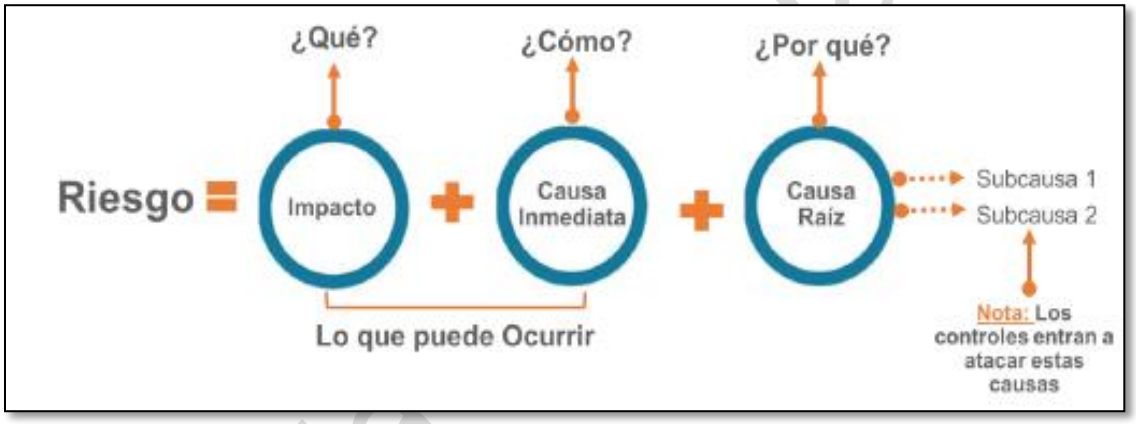
Tabla 1. Factores de Riesgo

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

2.5 Descripción del riesgo

la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:



La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **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.

- **Causa raíz:** es la causa principal o básica, corresponden 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 pueden existir más de una causa o subcausas que pueden ser analizadas.

Ejemplo:

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Alcance: inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisidores) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:

Premisas para una adecuada redacción del riesgo

- No describir como riesgos omisiones ni desviaciones del control. Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.
-
- No describir causas como riesgos. Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

- No describir riesgos como la negación de un control. Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

- No existen riesgos transversales, lo que pueden existir son causas transversales. Ejemplo: pérdida de expedientes.

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

2.6 Clasificación del riesgo

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 2. Clasificación del Riesgo

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Teniendo en cuenta que en la Tabla 2 se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

Relación ente factores de riesgo y clasificación del riesgo

RIESGO DE CORRUPCIÓN

Definición de riesgo de corrupción

Riesgo de Corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma decisiones y la administración de los bienes públicos". (CONPES N° 167 de 2013)

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

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

Los riesgos de corrupción se establecen sobre **procesos**.

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.

Con el fin de facilitar la identificación de riesgos de corrupción y de evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la **Matriz de definición de riesgo de corrupción**, que incorpora cada uno de los componentes de su definición. Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

Matriz definición del riesgo de corrupción				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato	X	X	X	X

Fuente: Secretaria de Transparencia de la Presidencia de la Republica

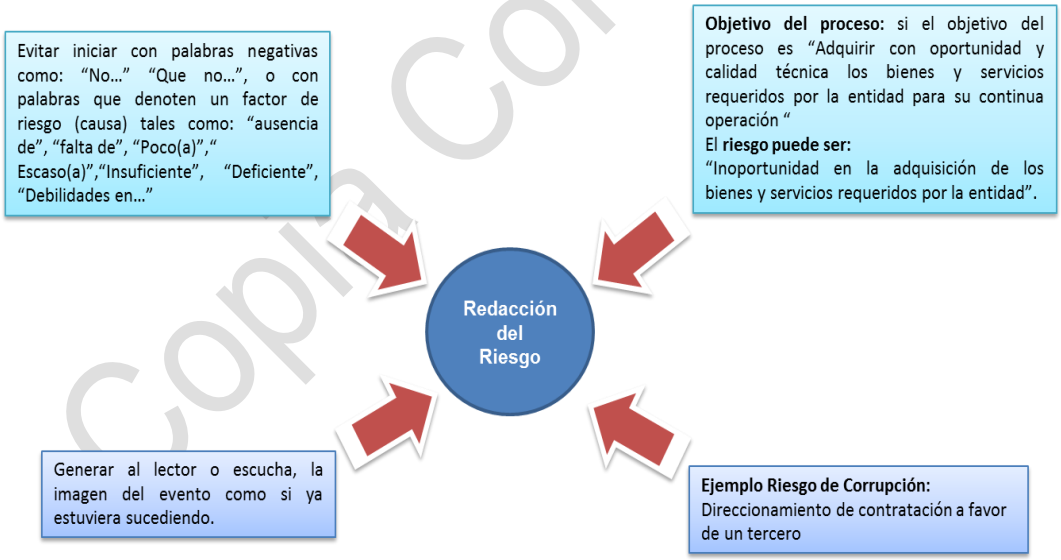
Ejemplo:

N°	Riesgo	Clasificación	Causa	Probabilidad	Impacto	Riesgo Residual	Opción Manejo	Actividad de Control
1	Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o para terceros...	Corrupción	Falta de...	Probable	Catastrófico	Catastrófico	Evi	INFORMACION ANONIMIZADA

Importante: Tenga en cuenta que la Información clasificada o reservada la señala la ley, un decreto con fuerza de ley o convenio internacional ratificado por el Congreso o en la Constitución.

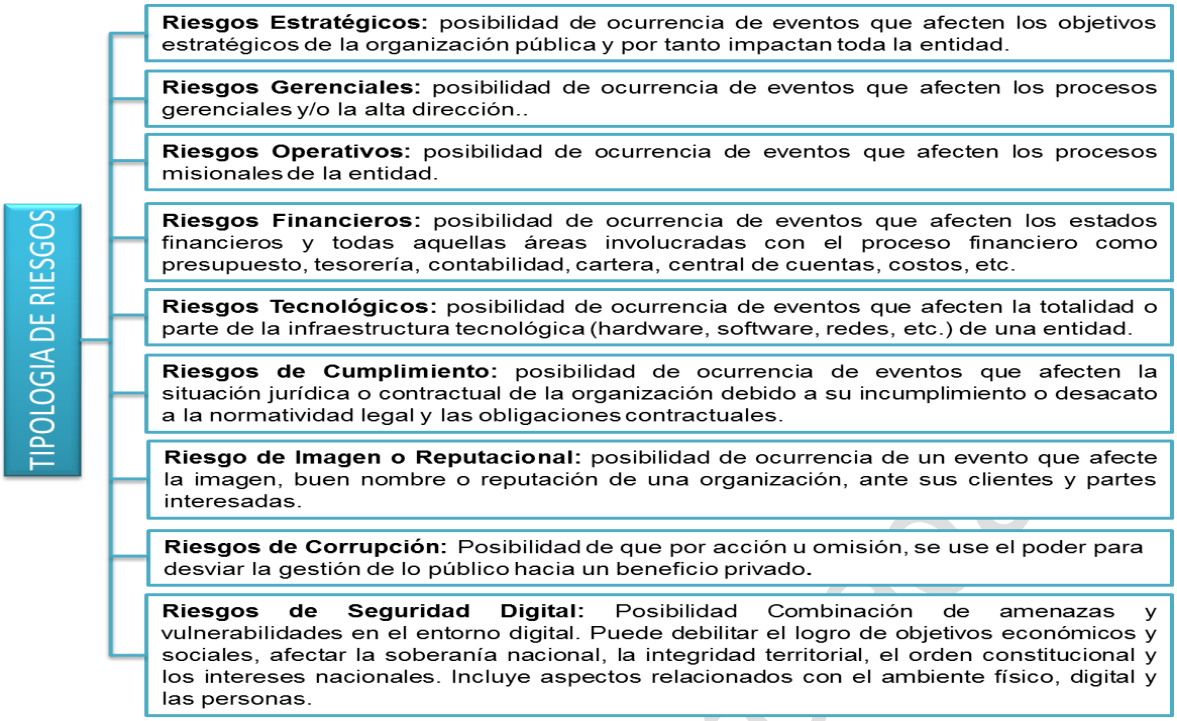
Una resolución no puede calificar la información como clasificada o reservada.

Esquema 5. Redacción del riesgo



Fuente: Departamento Administrativo de la Función Pública.

Importante: Pregúntese si el riesgo identificado está relacionado directamente con las características del objetivo. Si la respuesta es "no" este puede ser la causa o la consecuencia.



Fuente: Departamento Administrativo de la Función Pública

Importante: La tipología de riesgos depende de la misión de la Contraloría General de Santiago de Cali, de las normas que regulan su operación, de los sistemas de gestión que implemente, entre otros aspectos. Los riesgos de corrupción, siempre deben gestionarse.

Ejemplos descripción del riesgo

Formato de descripción del riesgo de gestión.

Riesgo	Descripción	Tipo	Causas	Consecuencias
Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	La combinación de factores como, insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación, pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad, repercutiendo en la continuidad de su operación.	Operativo	Carencia de controles en el procedimiento de contratación. Insuficiente capacitación del personal de contratos. Desconocimiento de los cambios en la regulación contractual. Inadecuadas políticas de operación.	1. Parálisis en los procesos 2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor. 3. Demandas y demás acciones jurídicas. 4. Detrimento de la imagen de la entidad ante sus grupos de valor. 5. Investigaciones disciplinarias

Fuente: Departamento Administrativo de la Función Pública.

Importante: La descripción del riesgo consolida lo pasos vistos en la metodología de gestión y facilita su análisis.

Formato de descripción del riesgo de corrupción

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin celebrar un contrato.	Situaciones como: debilidades en la etapa de la planeación del contrato, la excesiva discrecionalidad, las presiones indebidas, la carencia de controles, la falta de conocimiento y/o experiencia, sumados a la falta de integridad pueden generar un riesgo de corrupción en la contratación, como por ejemplo "Exigencias de condiciones en los procesos de selección que solo cumple un determinado proponente".	Corrupción	Debilidades en la etapa de planeación, que faciliten la inclusión en los estudios previos, y/o en los pliegos de condiciones de requisitos orientados a favorecer a un proponente. Presiones indebidas Carencia de controles en el procedimiento de contratación Falta de conocimiento y/o experiencia del personal que maneja la contratación Excesiva discrecionalidad Adendas que modifican las condiciones generales del proceso de contratación para favorecer a un proponente	1. Pérdida de la imagen institucional 2. Demandas contra el estado 3. Pérdida de confianza en lo público 4. Investigaciones penales, disciplinarias y fiscales 5. Detrimento patrimonial 6. Obras inconclusas 7. Mala calidad de las obras 8. Enriquecimiento ilícito de contratistas y/o servidores públicos

Fuente: Secretaria de transparencia de la Presidencia de la Republica

Importante: En la descripción de los riesgos de corrupción deben concurrir **TODOS** los componentes de su definición: Acción **u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado**.

Formato de descripción del riesgo de seguridad digital

Los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo: **"Pérdida de la integridad, confidencialidad o la disponibilidad"**.

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización

Formato de descripción del riesgo de seguridad digital

ACTIVO	RIESGO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/Vulnerabilidades	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada causando la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad Digital	Falta de políticas de seguridad digital. Ausencia de políticas de control de acceso. Contraseñas sin protección Autenticación débil	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo. (Legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ejm. Posible retraso en el pago de nómina

Fuente: Ministerio de las TIC´S

Seleccionar las Vulnerabilidades asociadas a la amenaza identificada

Importante:

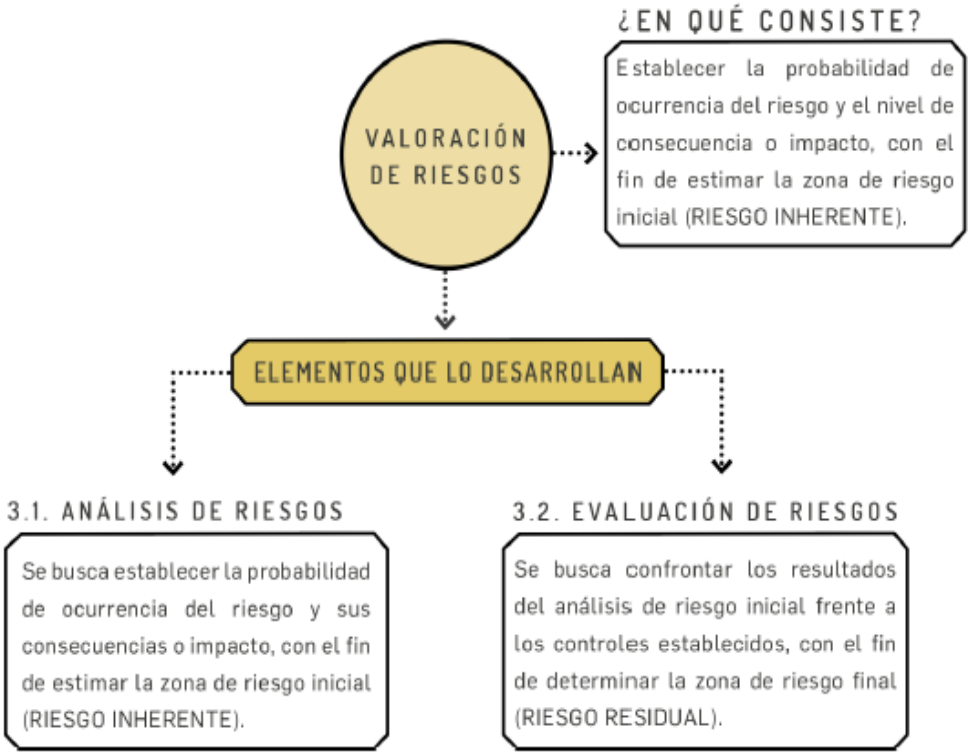
- Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

- Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección en los “Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas”, como anexo a la presente metodología.

- NOTA: Tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

PASO 3. VALORACIÓN DE RIESGOS

Esquema 6. Valoración de Riegos



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

3.1 Análisis de riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

3.1.1 Determinar la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo.

la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas en Colombia.

Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Tabla 3 Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la **exposición al riesgo** estará asociada al proceso o actividad que se esté analizando, es decir, al **número de veces que se pasa por el punto de riesgo en el periodo de 1 año,** en la tabla 4 se establecen los criterios para definir el nivel de probabilidad.

Tabla 4 Criterios para definir el nivel de probabilidad

PROBABILIDAD		
Nivel	**Frecuencia de la Actividad**	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 4 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 5 a 12 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 13 a 365 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 366 veces al año y máximo 1.500 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 1.501 veces por año	100%

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, v. 5 de diciembre de 2020.

Nota: Dependiendo del tamaño y complejidad de los procesos de la entidad, la tabla 4 podrá ser ajustada o adaptada a las necesidades de cada entidad.

3.1.2 Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en la versión 2018 de la Guía de administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

En las tablas 5 y 6 se establecen los criterios para definir el nivel de impacto, como los criterios para riesgos de seguridad digital.

Tabla 5. Criterios para definir el nivel de impacto

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

Fuente: Guía de Auditoría de riesgos y el diseño de controles - DAFP

Tabla 6. Criterios de impacto para riesgos de seguridad digital

NIVEL	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
Insignificante	Afectación ≥X% de la **población**	Sin afectación de la integridad
	Afectación ≥X% del **presupuesto** anual de la entidad	Sin afectación de la disponibilidad
	No hay **Afectación medioambiental**	Sin afectación de la confidencialidad
Menor	Afectación ≥X% de la población	Afectación leve de la integridad
	Afectación ≥X% del presupuesto anual de la entidad	Afectación leve de la disponibilidad
	Afectación leve del Medio Ambiente requiere de ≥X días de recuperación	Afectación leve de la confidencialidad
Moderado	Afectación ≥X% de la población	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros
	Afectación ≥X% del presupuesto anual de la entidad	Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros
	Afectación leve del Medio Ambiente requiere de ≥X semanas de recuperación	Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros
Mayor	Afectación ≥X% de la población	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros

NIVEL	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
	Afectación ≥X% del presupuesto anual de la entidad	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros
	Afectación importante del Medio Ambiente que requiere de ≥X meses de recuperación	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros
Catastrófico	Afectación ≥X% de la población	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros
	Afectación ≥X% del presupuesto anual de la entidad	Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros
	Afectación muy grave del Medio Ambiente que requiere de ≥X años de recuperación	Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros

Fuente: Guía de Auditoría de riesgos y el diseño de controles - DAFP

Importante: Frente al análisis de probabilidad e impacto **no se utiliza criterio experto**, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

Ejemplo (continuación):

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

Número (Nº) de veces que se ejecuta la actividad: la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.

Cálculo afectación económica: de llegar a materializarse, tendría una afectación económica de 1.500 SMLMV.

Aplicando las tablas de probabilidad e impacto tenemos:

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

La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

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

La afectación económica se calcula en 500SMLMV, el impacto del riesgo es **mayor**.

Probabilidad inherente = media 60%, **Impacto inherente =** mayor 80%

3.1.3 Análisis del impacto (riesgos de gestión y corrupción)

Tabla 7. Criterios de impacto riesgo de corrupción

Nro	PREGUNTA: Si el riesgo de corrupción se materializa podría…	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la Entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		X
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		X
9	¿Generar pérdida de información de la Entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNO a CINCO pregunta(s) genera un impacto Moderado.		10	
Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor.			
Catastrófico.			

Nivel de Impacto MAYOR

MODERADO	Genera medianas consecuencias sobre la entidad
MAYOR	Genera altas consecuencias sobre la entidad.
CATASTROFICO	Genera consecuencias desastrosas para la entidad

Fuente: Guía de Auditoría de riesgos y el diseño de controles - DAFP

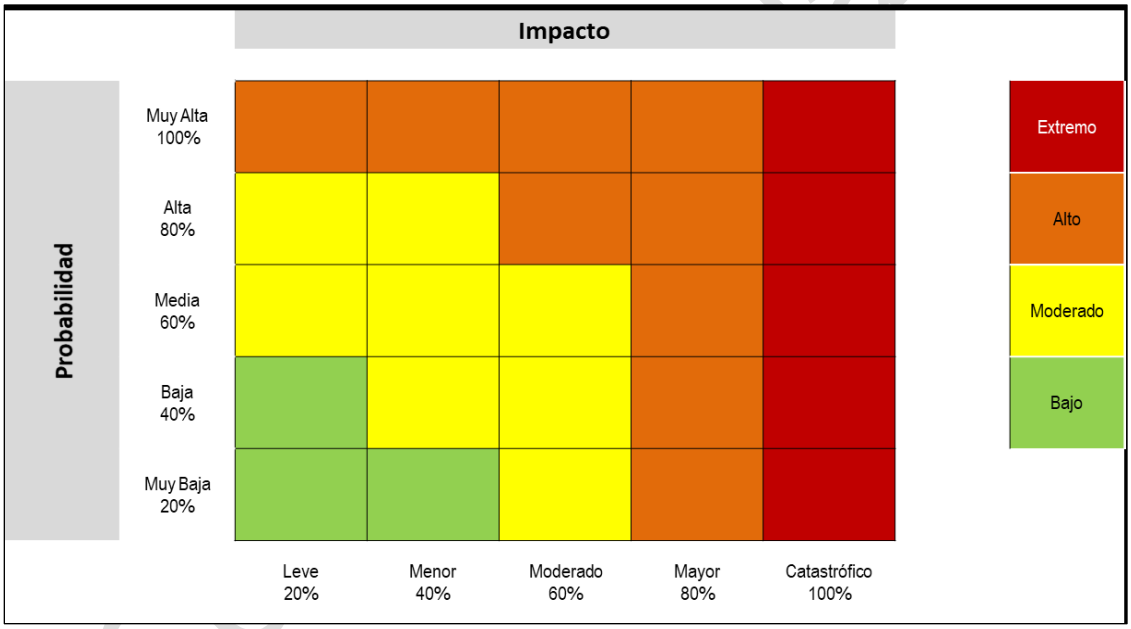
3.2 Evaluación del riesgo

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

3.2.1 Análisis preliminar (riesgo inherente)

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

Matriz de Calor (Niveles de severidad de calor)



Ejemplo (continuación):

Proceso: gestión de recursos

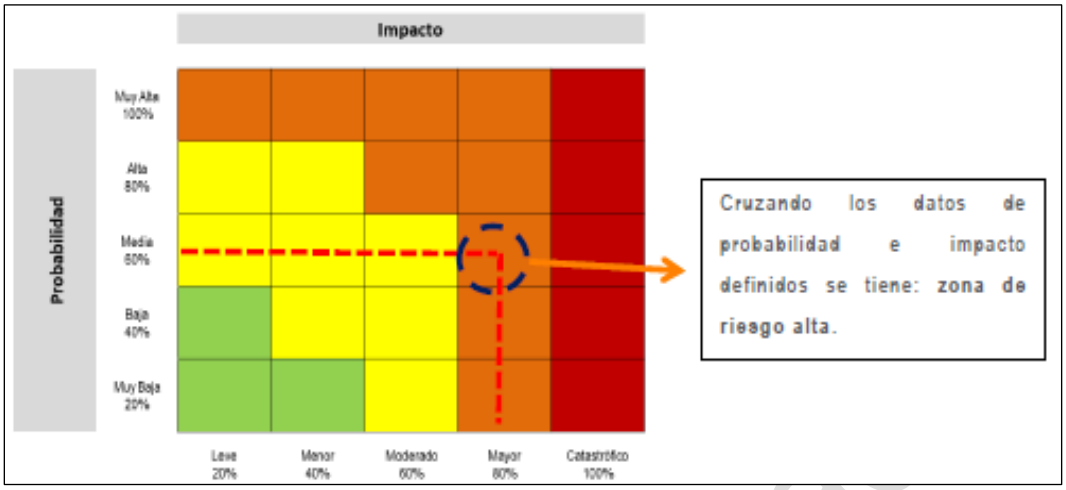
Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos

Probabilidad Inherente = moderada 60%

Impacto Inherente = mayor 80%

Aplicando la matriz de calor tenemos:



3.2.2 Valoración de controles

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

3.2.2.1 Estructura para la descripción del control

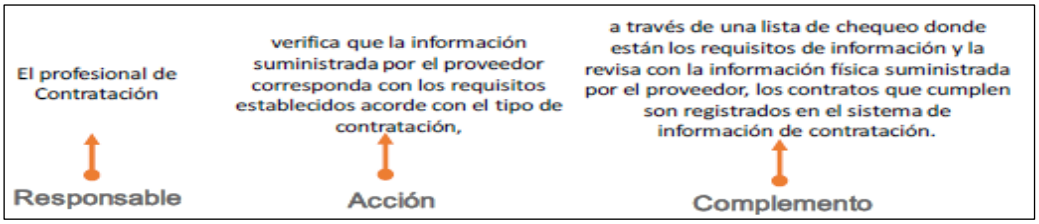
Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.

- **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo: aplicado bajo la estructura propuesta para la redacción del control



3.2.2.2 Tipología de controles y los procesos

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas

- **Control automático:** son ejecutados por un sistema.

3.2.2.3 Análisis y evaluación de los controles - Atributos

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

Atributos de para el diseño del control

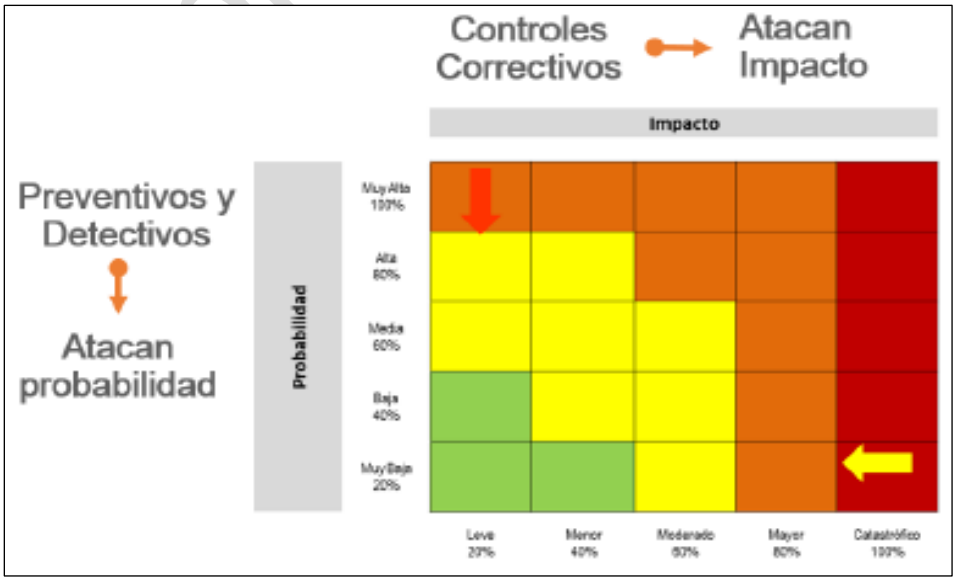
Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la	25%

Características			Descripción	Peso
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Nota: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Movimiento en la matriz de calor acorde con el tipo de control



Ejemplo:

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos

Probabilidad Inherente = moderada 60%

Impacto Inherente = mayor 80%

Zona de riesgo = alta

Controles identificados

Control 1: el profesional del área de contratos 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 revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

Control 2: el jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Aplicación tabla atributos a ejemplo propuesto

Controles y sus características				Peso
Control 1 El profesional del área de contratos 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 revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con registro	X	-
		Sin registro		-
Total valoración control 1				40%

3.2.3 Nivel de riesgo (riesgo residual)

Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

Ejemplo:

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

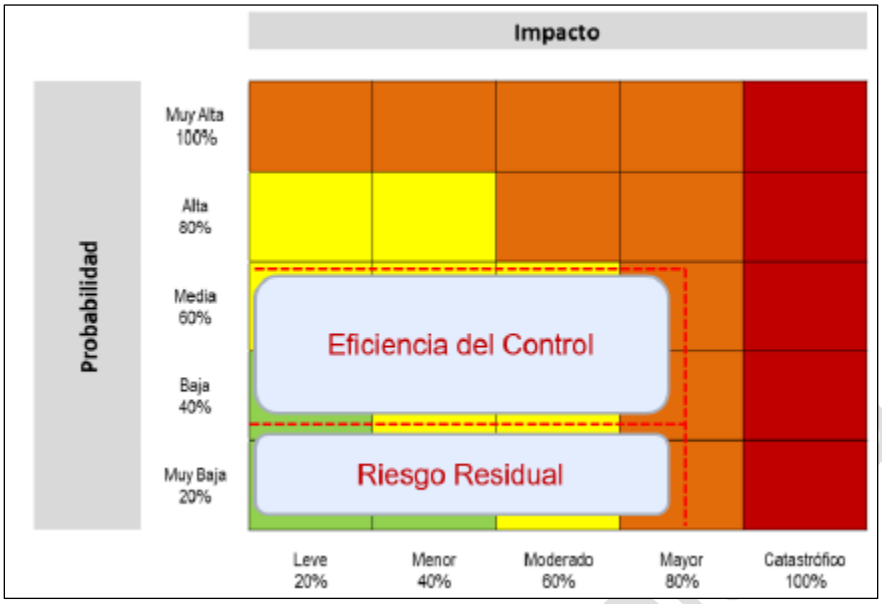
Probabilidad residual = baja 26.8%

Impacto Residual = mayor 80%

Zona de riesgo residual = alta

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

Movimiento en la matriz de calor con el ejemplo propuesto



Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

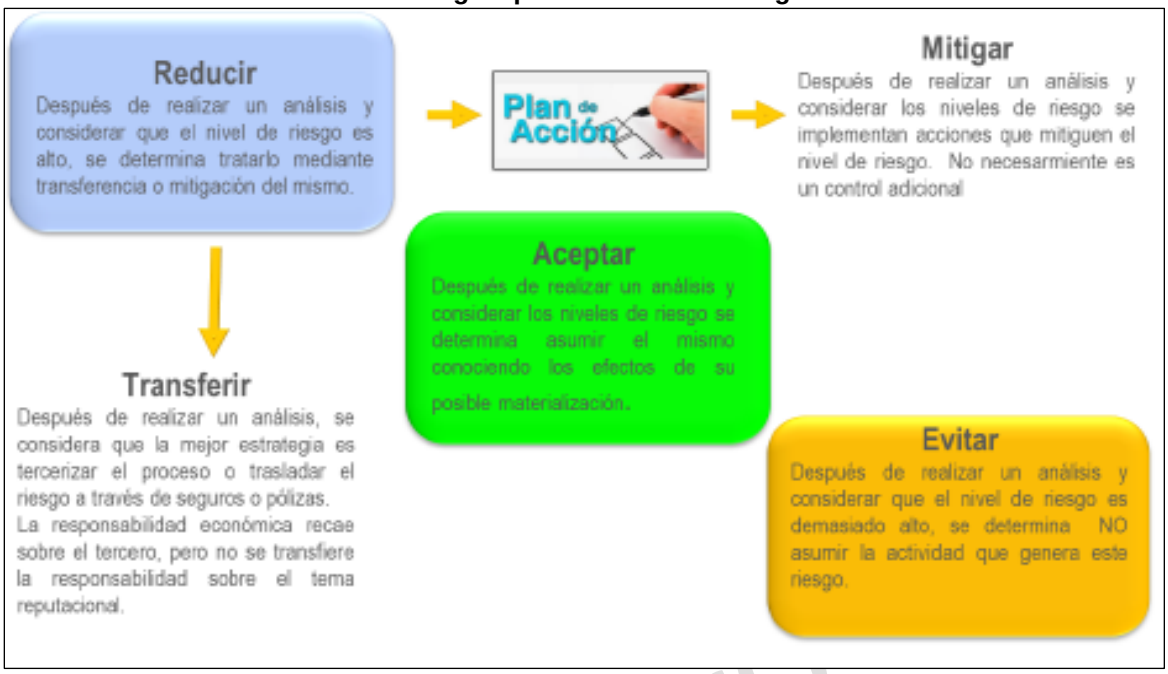
Importante: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.
Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

3.3 Estrategias para combatir el riesgo

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

En la siguiente figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Estrategias para combatir el riesgo



Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

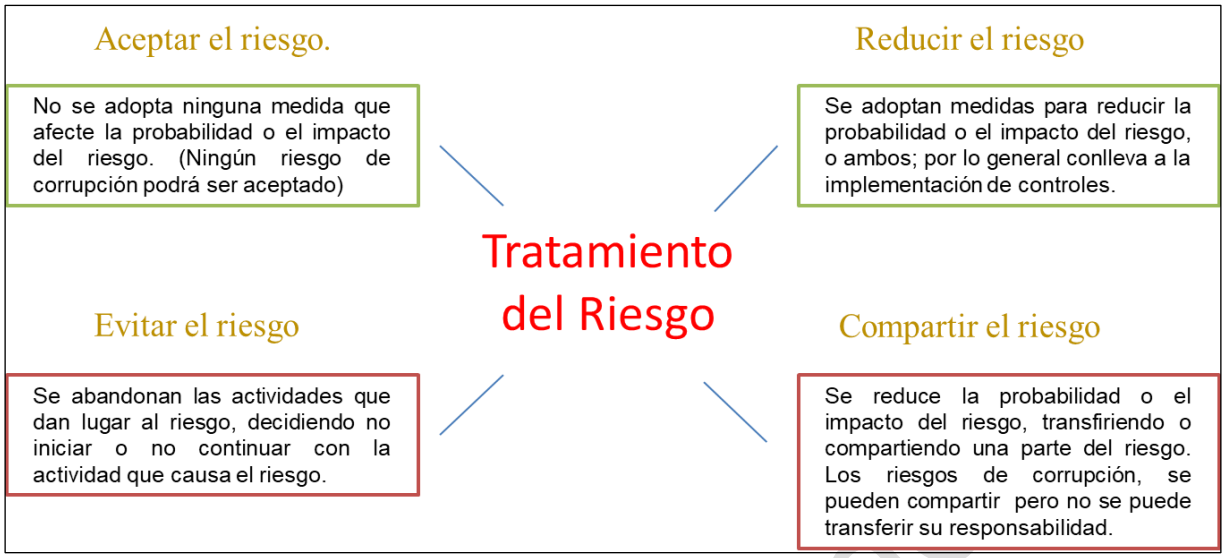
Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca dentro del Plan de Continuidad de Negocio2 y se consideraría un control correctivo.

Tratamiento del riego

¿Qué es Tratamiento del riesgo?

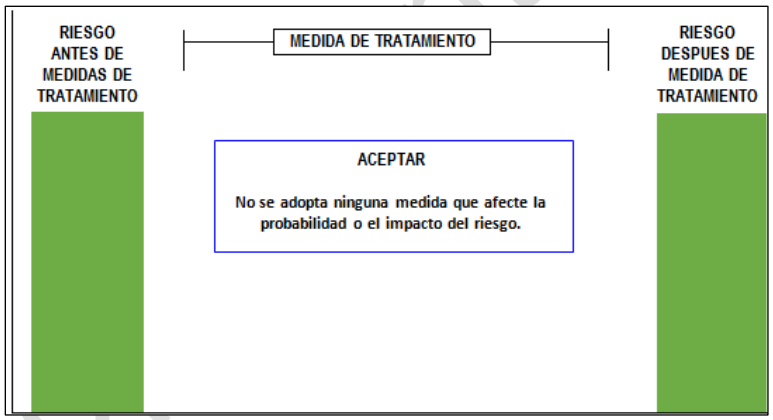
Es la respuesta establecida por la **Primer Línea de Defensa** para la mitigación de los diferentes riesgos, incluyendo los riesgos de Corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento.

Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo. Ningún riesgo de corrupción podrá ser aceptado. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:



Aceptar el riesgo

Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.

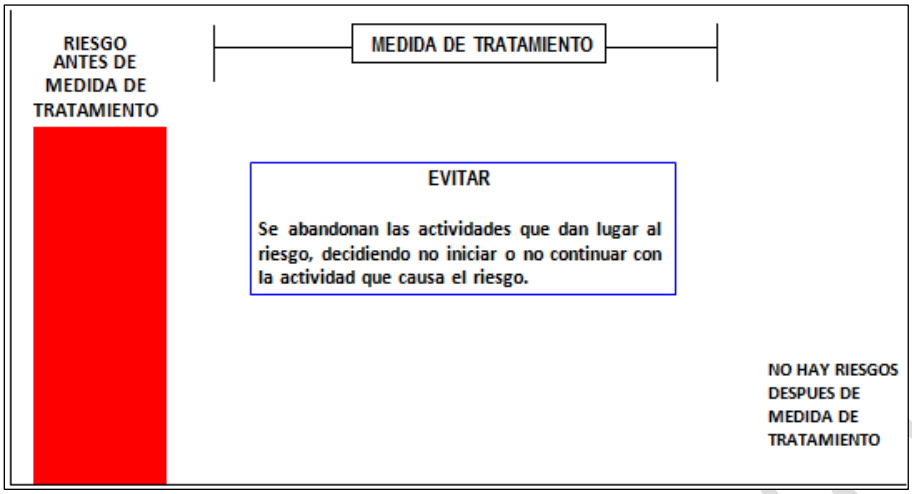


Importante: En el caso de riesgos de corrupción, estos no pueden ser aceptados.

La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Evitar el riesgo

Cuando los escenarios de riesgo identificado se consideran demasiados extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.

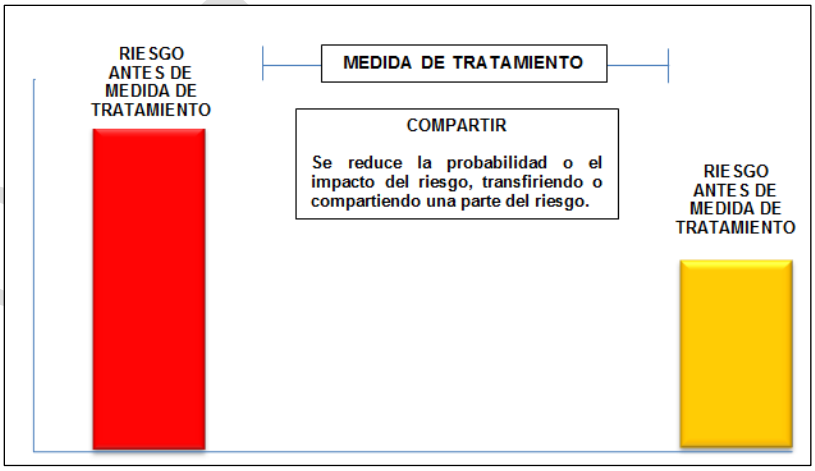


Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y por lo tanto hay situaciones donde no es una opción.

Compartir el riesgo

Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia.

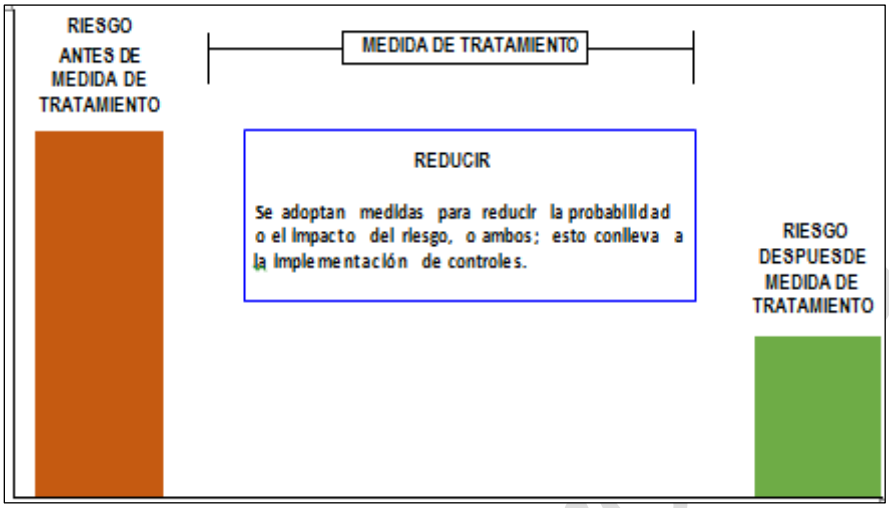
Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.



Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

Reducir el riesgo

El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.



Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, permitiendo que el tratamiento al riesgo adoptado, logre la reducción prevista sobre el riesgo.

Para mitigar/tratar los riesgos de seguridad digital, se deben emplear como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, los cuales igualmente se encuentran en. “Lineamientos para la gestión del riesgo de seguridad digital de la presente Metodología”

Tratamiento del Riesgo - Rol de la Primera Línea de Defensa.

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.

¿**Qué son actividades de control?:** Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Actividades de control documentadas en:

- **POLITICAS:** Las políticas establecen las líneas generales del control interno.
- **PROCEDIMIENTOS:** Los procedimientos son los que llevan dichas políticas a la práctica.

Importante:

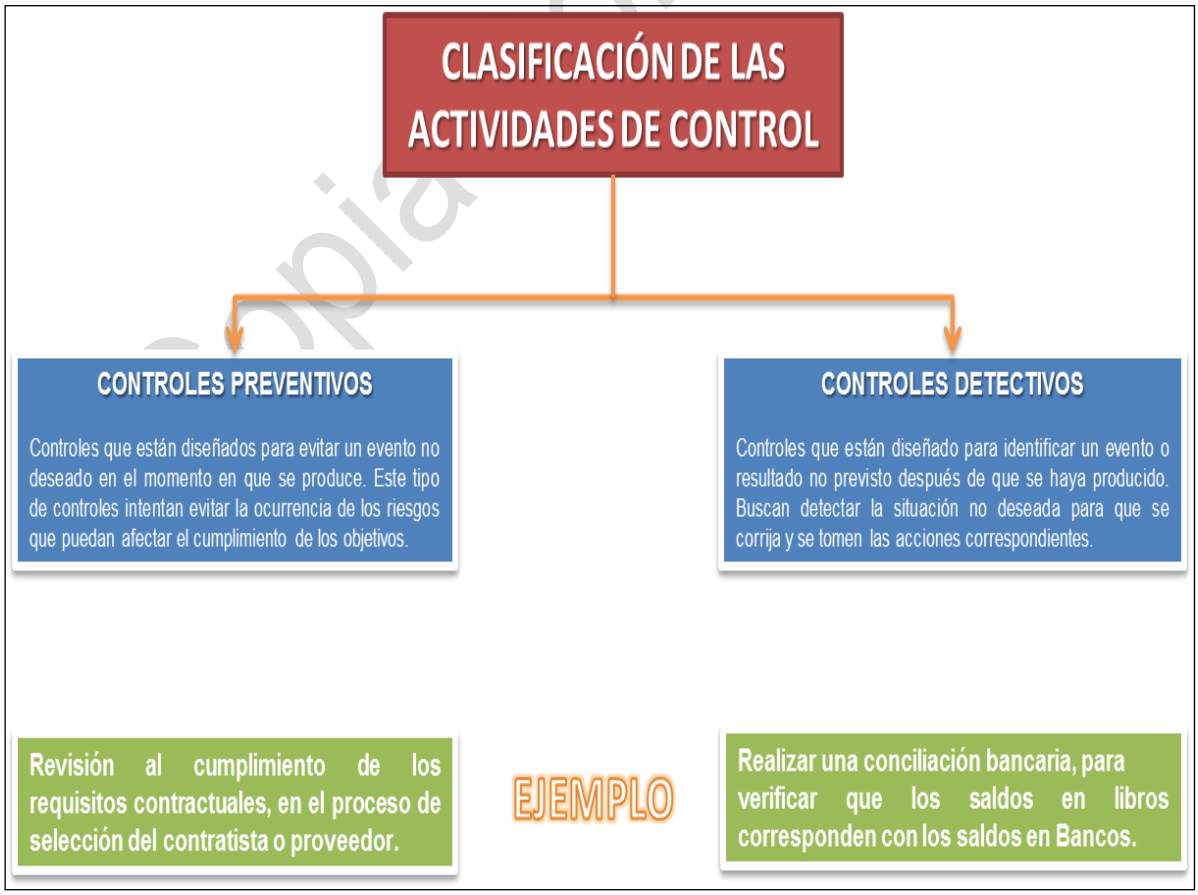
- Una política por sí sola no es un control.
- Los controles se despliegan a través de los procedimientos documentados.
- La actividad de control debe por si sola mitigar o tratar la causa del riesgo y ejecutarse como parte del día a día de las operaciones.
- Para mitigar/tratar los riesgos de seguridad digital, se deben emplear como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, los cuales igualmente se encuentran en los "Lineamientos para la gestión del riesgo de seguridad digital" de la presente metodología.

Ejemplo:

La política establece que para los contratos de bienes y servicios se debe tener tres cotizaciones. El procedimiento será la revisión que valide que la política se está cumpliendo, dejando claras las actividades y responsabilidades que asume el personal que lleva a cabo la actividad de control y asegura que existan las tres cotizaciones.

Tanto la política como el procedimiento deben estar documentados. Esto contribuye a que las actividades de control, sean parte del día a día de las operaciones de la entidad.

Las actividades de control, independiente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine, o en caso de que la situación de riesgos se presente, esta sea detectada de manera oportuna.

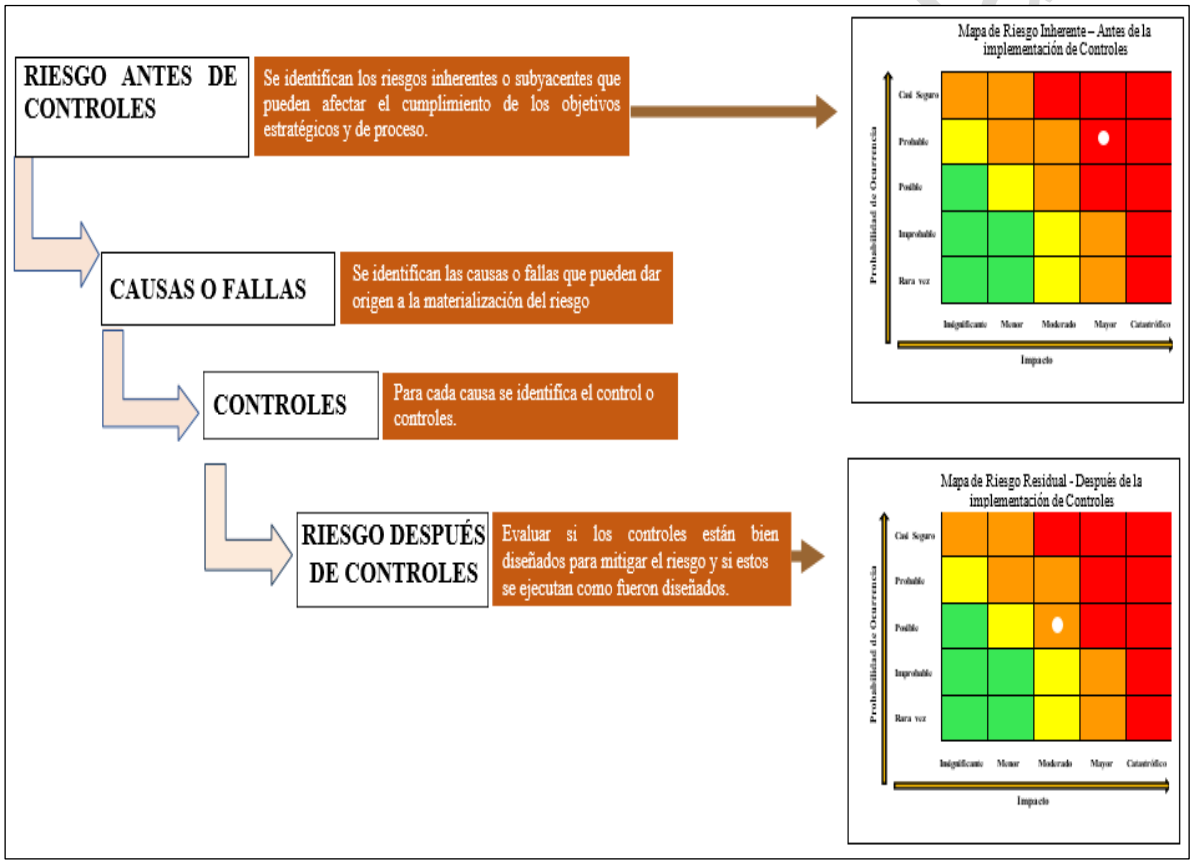


Importante: Se deben seleccionar actividades de control preventivas y detectivas que por sí solas ayuden a la mitigación de las causas que originan los riesgos.

3.3.1 Análisis preliminar (riesgo inherente)

Al momento de definir las actividades de control por parte de la Primera Línea de Defensa, es importante considerar que los controles estén bien diseñados, es decir, que estos mitigan las causas que hacen que el riesgo se materialice.

Esquema 7. Riesgo antes y después de controles



Importante:

- Para cada causa debe existir un control.
- Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).
- Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa especifica.

Resultados del mapa de riesgo residual.

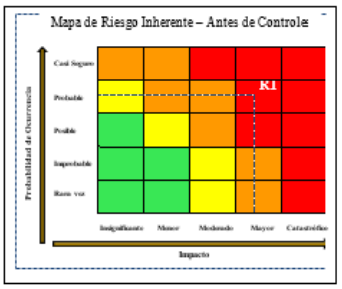
Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

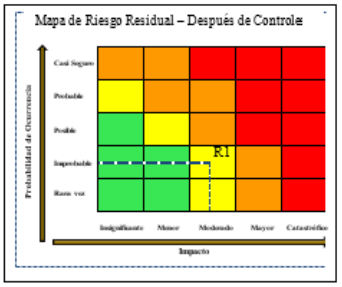
EJEMPLO

Tenemos el Riesgo 1 - Con una calificación de riesgo inherente de probabilidad e impacto como se muestra en la siguiente gráfica:

Como podemos observar es probable que el riesgo suceda y tiene un impacto en caso de materializarse mayor para la entidad, ahora supongamos que existen controles bien diseñados y que siempre se ejecutan, y que estos controles disminuyen de manera directa la probabilidad.

En nuestro ejemplo disminuiría dos cuadrantes de probabilidad, pasa de probable a improbable y un cuadrante de impacto, pasa de mayor a moderado.





3.4 Monitoreo y revisión

¿Por qué debo monitorear y revisar la gestión de riesgos?
Porque la entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Planeación y Gestión- (MIPG) en la dimensión 7 “Control Interno” desarrolla a través de las Líneas de Defensa la responsabilidad de la gestión del riesgo y control.

¿Cómo se define el modelo de las líneas de defensa?
Es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos

¿Quiénes son los asignados para monitorear y revisar la gestión de riesgos y cuáles son sus roles?

El monitoreo y revisión de la gestión de riesgos, está alineado con la dimensión del MIPG de “Control Interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue:

LÍNEA ESTRATÉGICA

Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

1ª. Línea de defensa	2ª. Línea de defensa	3ª. Línea de defensa
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende	Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa
A cargo de los líderes de procesos de la entidad. Rol principal: diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.	A cargo de la oficina de Planeación. Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.	A cargo de la oficina de control interno. El rol principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I. El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

Rol de la línea estratégica en el monitoreo y revisión de los riesgos y actividades de control

LÍNEA ESTRATÉGICA	
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.	
Actividades de Monitoreo y Revisión a Realizar	La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente: ✓ Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. ✓ Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. ✓ Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno. ✓ Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ✓ Hacer seguimiento y pronunciarse por lo menos cada cuatrimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas. ✓ Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

Rol de la primera línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

1ª. LÍNEA DE DEFENSA	
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los líderes de los procesos.	
Actividades de Monitoreo y Revisión a Realizar	Los líderes de procesos deben monitorear y revisar el cumplimiento de los objetivos instituciones y de sus procesos a través de una adecuada gestiónde riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente: ✓ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso. ✓ Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. ✓ Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. ✓ Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ✓ Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. ✓ Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

Rol de la segunda línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

2ª. LÍNEA DE DEFENSA	
Asiste y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los Riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)	
Actividades de monitoreo y revisión a realizar	Los jefes de planeación, supervisores e interventores de contratos, deben monitorear y revisar el cumplimiento de los objetivos institucionales y de procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción, con relación a lo siguiente: ✓ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos. ✓ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. ✓ Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. ✓ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad. ✓ Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

Rol de la tercera línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

3ª. LÍNEA DE DEFENSA	
Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Está conformada por la Oficina de Control Interno.	
Actividades de monitoreo y revisión a realizar	La oficina de control interno monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente: ✓ Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. ✓ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. ✓ Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción. ✓ Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. ✓ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. ✓ Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.

Monitoreo riesgos de corrupción

Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es del caso ajustarlo, (primera línea de defensa). Le corresponde, igualmente a la oficina de planeación adelantar el monitoreo, (segunda línea de defensa) para este propósito se sugiere elaborar una matriz para el monitoreo periódico. Este monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es - por sus propias características una actividad difícil de detectar.

Para el efecto deben atender las actividades descritas en la primera y segunda línea de defensa de este documento.

Reporte Plan de Tratamiento de Riesgos

Consolidar información para la gestión del riesgo

- Una vez analizado el nivel de riesgo residual y definido el tratamiento a implementar con el establecimiento de controles preventivos y detectivos, es necesario generar un reporte que consolide la información clave del proceso de gestión del riesgo.

- En el formato de Mapa y Plan de Tratamiento de Riesgos, se inicia con el registro del riesgo identificado, luego se especifica la clase de riesgo, se transcriben las causas raíz o causas priorizadas, así como la probabilidad e impacto que quedaron después de valorar los controles para determinar el riesgo residual.

- A partir de allí se deben analizar las estrategias DO y FA o estrategias de supervivencia formuladas en la etapa de establecimiento del contexto, que contrarresten las causas raíz, para colocarlas en las actividades de control del formato y con base en su contenido se establezca la opción de tratamiento a la que corresponden.

- Luego se relaciona el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

- Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice, para ello se deben analizar las estrategias DA o estrategias de fuga provenientes de la Matriz DOFA, seleccionando la(s) más apropiada(s) para el riesgo identificado.

- No olvidar colocar el soporte, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso o la estrategia.

- Por último se formulan los indicadores clave de riesgo (KRI por sus siglas en ingles) que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (Por riesgo identificado en los procesos).

Reporte de la gestión del riesgo

La primera línea de defensa reporta a la segunda línea de defensa, el estado de avance del tratamiento del riesgo en la operación, y la consolidación de los riesgos en todos los niveles será reportada por la segunda línea de defensa (encargado de la gestión del riesgo) hacia la alta dirección.

Formato mapa y plan de tratamiento de riesgos

Proceso:	Gestión de recursos
Objetivo:	Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
Alcance:	Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas

* Referencia	Impacto	Causa inmediata	Causa raíz	Descripción del riesgo	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente
1	Afectación económica	Multa y sanción del organismo de control	Incumplimiento de los requisitos para contratación	Posibilidad de afectación económica por multa y sanciones del organismo de control debido la adquisición de bienes y servicios fuera de los requerimientos normativos.	Ejecución y administración de procesos	120	Moderada	60%	Mayor	80%	Alta

Parte 2 Valoración del riesgo:

No. control	Descripción del control	Afectación		Atributos						Probabilidad residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
1	El profesional del área de contratos 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 revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	X		Preventivo	Manual	40%	Documentado	Continua	Registro material	36%	Baja	25,2%	Mayor	80%	Alta	Reducir

No. control	Descripción del control	Afectación		Atributos						Probabilidad residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
2	El jefe de del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	X		Detectivo	Manual	30%	Documentado	Continua	Con registro	25,2%						

Parte 3 Planes de acción (para la opción de tratamiento reducir):

Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso.	Oficina de TIC	30/11/2020	30/06/2020	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo.	En curso

Reporte de la gestión del riesgo de corrupción: De igual forma se debe reportar en el mapa y plan de tratamiento de riesgos, los riesgos de corrupción, de tal forma que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

Nro.	Riesgo	Clasificación	Causas	Probabilidad	Impacto	Riesgo Residual	Opción Manejo	Actividad de Control	Soporte	Responsable	Tiempo	Indicador
2	Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros para celebrar un contrato	Corrupción	Debilidades en la etapa de planeación	Probable	Catastrófico	Catastrófico	Reducir	Manual de contratación Implementado con parámetros técnicos y financieros para cada tipo de contratación, formalizado en procedimiento.	Manual de contratación	Jefe de Contratos	Primer trimestre de…	**EFICACIA: Indice de cumplimiento actividades=** (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD: Efectividad del plan de manejo de riesgos=** ((# de casos de favorecimiento a proponentes presentados periodo actual - # de casos de favorecimiento a proponentes presentados periodo anterior) / # de casos de favorecimiento a proponentes presentados periodo anterior) x 100
			Presiones indebidas				Reducir	Comité de Contratación	Acto administrativo conformando comité	Jefe de Contratos	Trimestralmente	
			Carencia de controles en el procedimiento de contratación				Reducir	Difusión y capacitación a todos los funcionarios del proceso.	Actas de capacitación	Director Talento Humano	Del (dia /mes/año) al (dia /mes/año)	
			Excesiva discrecionalidad				Acción de Contingencia	Iniciar la investigación disciplinaria, fiscal o remitir a las instancias correspondientes para el proceso penal.	Comunicación iniciando o remitiendo investigación	Jefe Control Disciplinario Interno	1 semana una vez el riesgo de iliquidez se materialice	

Reporte de la gestión del riesgo de seguridad digital

Igualmente en el caso de los riesgos de seguridad digital, se debe reportar en el mapa y planes de tratamiento. El responsable de seguridad digital apoyará y acompañará a las diferentes líneas de defensa tanto para el reporte, como para la gestión y el tratamiento de estos riesgos.

Formato mapa y plan de tratamiento de riesgos de seguridad digital

Nro.	Riesgo	Activo	Tipo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo residual	Opción tratamiento	Actividad de Control	Soporte	Responsable	Tiempo	Indicador
1	Pérdida de la integridad	Base de Datos de Nómina	Seguridad Digital	Modificación no autorizada	Ausencia de políticas de control de acceso.	Probable	Menor	Moderado	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA: Índice de cumplimiento actividades=** (# de actividades cumplidas / # de actividades programadas) x 100
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Cuarto trimestre de 2018	**EFECTIVIDAD: Efectividad del plan de manejo de riesgos=** (# de modificaciones no autorizadas)
					Ausencia de bloqueo de sesión				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Cuarto Trimestre de 2018	

Nota. En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada Oficina en particular, el análisis de riesgos determinará los controles y los responsables en cada caso.

Indicadores - gestión del riesgo de seguridad digital

Igualmente, en el caso de los riesgos de seguridad digital, se deben generar indicadores, para medir la gestión realizada, en esencia la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad debería definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

- 1 indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.

- 1 indicador de efectividad, para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

Importante: No se definirán indicadores por activo, teniendo en cuenta que pueden generarse un sinnúmero de indicadores lo que haría la gestión y seguimiento demasiado complejo para la entidad.

Ejemplos:

Eficacia: Porcentaje de controles implementados = (#controles implementados / #controles definidos) x 100

Efectividad: # Riesgos materializados de confidencialidad = (# de incidentes que afectaron la confidencialidad de algún activo del proceso)

Variación de incidentes de confidencialidad (para entidades con mediciones anteriores) = ((# de Incidentes de Confidencialidad Periodo Actual - # de Incidentes de Confidencialidad Periodo Previo) / Incidentes de Confidencialidad Periodo Previo) * 100%

3.5 Seguimiento riesgos de corrupción

GESTIÓN RIESGOS DE CORRUPCIÓN

- **Seguimiento:** El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- **Primer seguimiento**: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

- **Segundo seguimiento:** Con corte al 31 de agosto La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

- **Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la Entidad o en lugar de fácil acceso al ciudadano.

En especial 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.

- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.

- Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles.

- Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción.

- Realizar un monitoreo permanente.

Teniendo en cuenta que la Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riego y están funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Acciones encaminadas a determinar la efectividad de los controles.
- Acciones encaminadas a mejorar la valoración de los riesgos.
- Acciones encaminadas a mejorar los controles.
- Analizar el diseño e idoneidad de los controles, si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

Comunicación y consulta

La comunicación y consulta con las partes involucradas tanto internas como externas debería tener lugar durante todas las etapas del proceso para la gestión del riesgo[3].

Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

La comunicación y consulta: Se constituye en un elemento transversal a todo el proceso al involucrar a todos los funcionarios para el levantamiento de los mapas de riesgos.

La comunicación y consulta tiene un enfoque de equipos de trabajo que puede:

- Ayudar a establecer correctamente el contexto para los procesos.
- Garantizar que se toman en consideración las necesidades de los usuarios.
- Ayudar a garantizar que los riesgos estén correctamente identificados.
- Reunir diferentes áreas de experticia para el análisis de los riesgos.
- Garantizar que los diferentes puntos de vista se toman en consideración adecuadamente durante todo el proceso.

[3] Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC. Norma Técnica Colombiana NTC-ISO31000. 2011. p. 132.

- Fomentar la administración del riesgo como una actividad inherente al proceso de planeación estratégica.

Información, comunicación y reporte

Línea estratégica

Corresponde al Comité de Auditoría de las Empresas Industriales y Comerciales del Estado y/o a los Comités Institucionales de Coordinación de Control Interno, establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

Primera línea de defensa

Corresponde a los jefes de área y/o grupo (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.

Segunda línea de defensa

Corresponde al área encargada de la gestión del riesgo (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

Tercera línea de defensa

Le corresponde a la Oficina de Auditoría y Control Interno de la CGSC, realizar evaluación (aseguramiento) independiente al informe sobre la gestión de los riesgos elaborado por la OAPNC y sobre el Plan Anticorrupción y de Atención al Ciudadano, en particular los riesgos de corrupción y de fraude en la CGSC, catalogándola como una unidad auditable más dentro de su universo de auditoría, y por tanto debe dar a conocer a toda la entidad el Plan Anual de Auditorias basado en riesgos, y los resultados de la evaluación de la gestión del riesgo.

Orientar y asesorar, sin comprometer su independencia sobre el diseño y efectividad de los controles a los procesos, a través de la realización de la auditoría interna basada en riesgos. [4]

La comunicación de la información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

Por tanto, se debe hacer especial énfasis en la difusión, socialización, capacitación y/o entrenamiento de todos y cada uno de los pasos que componen la metodología de la

[4] Guía Rol de las Oficinas de Control Interno o quienes hacen sus veces. Versión 3 de noviembre 2022 de la Dirección de gestión y Desempeño Institucional de la Función Pública.

administración del riesgo, asegurando que permee a la totalidad de la organización pública.

Importante: Se debe conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas.

Adicionalmente, los riesgos de seguridad digital deberán ser reportados a las autoridades o instancias respectivas que el gobierno disponga.

PASO 4. LINEAMIENTOS PARA EL ANÁLISIS DE RIESGO FISCAL

4.1 Control fiscal interno y prevención del riesgo fiscal

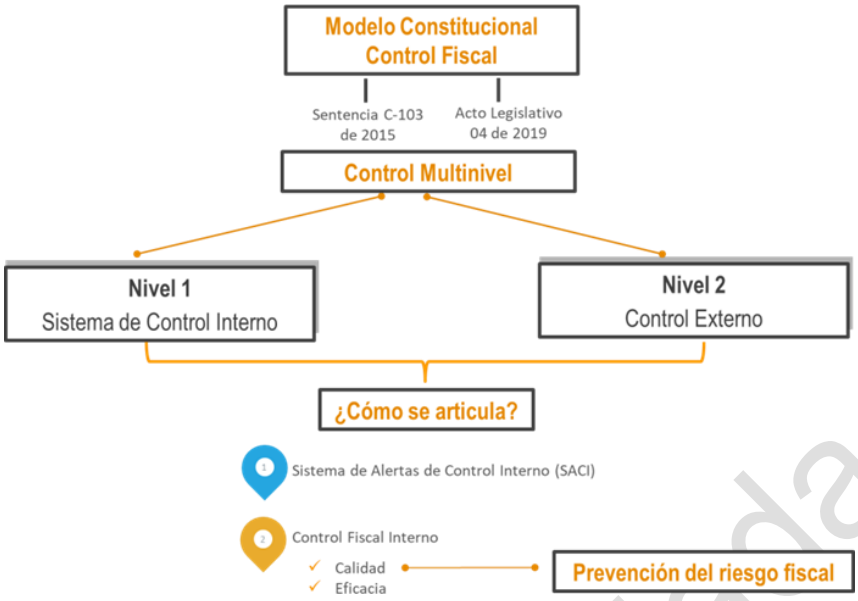
El control fiscal que ejerce la Auditoría General de la República, es posterior y selectivo a través de las auditorías (control micro), buscando con ello el control al recurso público administrado por CGSC, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno con el control externo aplicado a la Entidad por la AGR con lo cual surgen conceptos clave como:

- **Control fiscal Multinivel:** Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

- **Control fiscal Interno (CFI):** Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

En el nuevo modelo constitucional el control externo adquiere un enfoque preventivo y a su vez el control interno potencia el enfoque preventivo, partiendo de la premisa de que el Sistema de Control Interno es fundamental para conjugar el logro de resultados, con la prevención de riesgos de gestión, corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labor es de cobro, entre otros), a través de la prevención de responsabilidades fiscales.

La siguiente se muestra este despliegue y sus elementos de articulación que sustentan el desarrollo del presente capítulo.



A continuación se presenta el paso a paso de la gestión del riesgo fiscal (Identificación, análisis y valoración), que debe vincularse al análisis general de los riesgos institucionales, a fin de contar con un esquema integral que facilite su seguimiento por parte de los líderes del proceso de la CGSC.

Se pretende gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez permite, mitigar la posibilidad de configuración de responsabilidades fiscales para los diferentes gestores públicos.

Por tanto, a continuación se pone a disposición, como insumo de referencia, el Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas formulado por la Dirección de Gestión y Desempeño Institucional del DAFP, el cual ha sido construido como resultado del análisis de precedentes; aproximadamente 130 fallos con responsabilidad fiscal de contralorías territoriales y de la Contraloría General de la República, a través de los cuales se identifican 50 puntos de riesgo fiscal e igual número de circunstancias inmediatas.

CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS		
Referencia	***Puntos de Riesgo Fiscal**	****Circunstancia Inmediata**
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio dela entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes	Pérdida, extravío, hurto, robo o

CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS		
Referencia	***Puntos de Riesgo Fiscal**	****Circunstancia Inmediata**
	muebles de la entidad	declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron
19	Suscripción de contratos	No incluir en el contrato de seguros - amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a	Bienes, servicios u obras inconclusos,

CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS		
Referencia	***Puntos de Riesgo Fiscal**	****Circunstancia Inmediata**
	satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratistas
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento

CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS		
Referencia	***Puntos de Riesgo Fiscal**	****Circunstancia Inmediata**
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2022[5]

* Actividad en la que potencialmente se origina el riesgo fiscal
** Situación por la que se presenta el riesgo

Este marco de referencia debe ser utilizado por los procesos de la CGSC, para la identificación y valoración de riesgos fiscales, siempre atendiendo las particularidades, naturaleza, complejidad, recursos, usuarios o grupos de valor, portafolio de productos y servicios, contexto, así como otras condiciones específicas del proceso acorde con la misión de la CGSC.

Además, en los procesos de la CGSC se deberá analizar si existen, de acuerdo con su contexto y particularidades, puntos de riesgos y circunstancias inmediatas diferentes a los identificados en el catálogo y tenerlas en cuenta en la identificación de sus riesgos fiscales.

4.2 Definición y elementos del riesgo fiscal

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

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente metodología, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

Efecto. Es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial. Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar **daño sobre** los recursos públicos y/o los bienes y/o interés patrimonial de naturaleza pública. En esta metodología, el evento potencial es equivalente a la causa raíz.

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso

Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

4.3 Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales

A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, que es fundamental para el resultado de la gestión de cada entidad y para la seguridad y prevención de responsabilidades fiscales de los gestores públicos en la CGSC.

4.3.1 identificación de riesgos fiscales

Identificación de puntos de riesgo

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.[6]

[6] Ley 610 de 1993, Artículo 3.

Es así, que los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

De otra parte, para identificar los puntos de riesgo y las circunstancias inmediatas, la Oficina de Planeación, Normalización y Calidad, debe convocar al personal del nivel directivo y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, para realizar un taller para que basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal y circunstancias Inmediatas.

Para este taller, se pueden usar las siguientes preguntas orientadoras:

SIRVE PARA IDENTIFICAR	PREGUNTAS Y RESPUESTAS PARA LA IDENTIFICACIÓN
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme, relacionados con hechos de la entidad o del sector y/o las advertencias de la CGR.
	Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.
	Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.
	Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado
	Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la CGR es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.

Identificación de áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.

- Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el capítulo uno de conceptos básicos).

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública.

Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal.

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño -efecto- (Contraloría General de la República, 2021).[7]

[7] Concepto CGR- OJ- 115 - 2021 de la Contraloría General de la República, pág. 13

Ejemplo:

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

¿Cuál es el daño? El daño fiscal corresponde al monto pagado por concepto de intereses moratorios

¿Cuál es el hecho generador? La omisión de pagó oportuno del canon de arrendamiento.

Conclusión: El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

Descripción del Riesgo Fiscal

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

Para redactar un riesgo fiscal se debe tener en cuenta:

- **Iniciar con la oración.** Posibilidad de, debido a que nos estamos refiriendo al evento potencial.

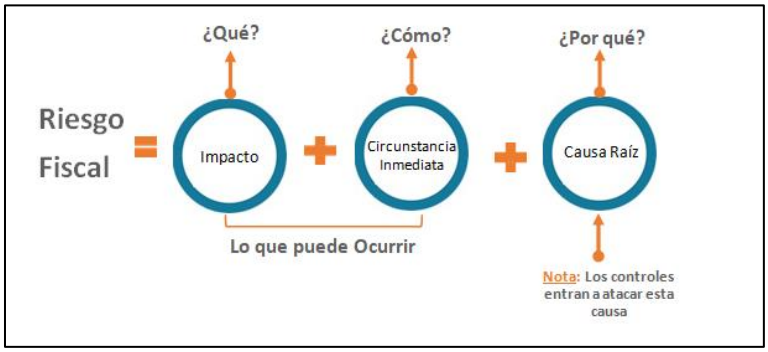
- **Impacto.** Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

- **Circunstancia inmediata.** Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

- **Causa Raíz.** Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es 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.[8]

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:

[8] El control f iscal y la responsabilidad f iscal en Colombia. Luz Jimena Duque Botero y Fredy Céspedes Villa. Ibáñez 2018



Ejemplo:

Proceso: Gestión de Recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

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

Como complemento a continuación se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso, es decir efecto dañoso sobre bienes públicos, recursos públicos o sobre intereses patrimoniales de naturaleza pública.

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista

4.3.2 Valoración del riesgo fiscal evaluación de riesgos

Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

Probabilidad

La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

Teniendo esto de presente, para definir el nivel de probabilidad, se ha de tener en cuenta en la siguiente tabla definida en el numeral 3.1.1 (Tabla 4) de la presente metodología:

PROBABILIDAD		
Nivel	**Frecuencia de la Actividad**	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 4 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 5 a 12 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 13 a 365 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 366 veces al año y máximo 1.500 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 1.501 veces por año	100%

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles v. 6

Nota: Es necesario mencionar, que las frecuencias pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que las frecuencias en cada nivel pueden ser adaptadas a las necesidades y complejidad de cada entidad.

Impacto

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tend rá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

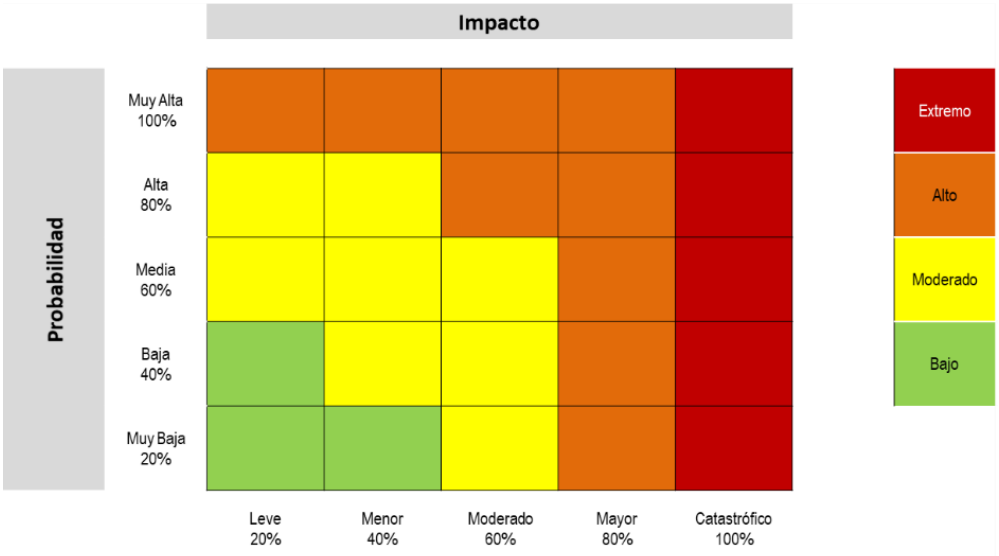
Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos, es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales, sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal, se aplicará la siguiente tabla definida en el numeral 3.1.2 (Tabla 5) de la presente metodología:

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

Nota: Es necesario mencionar, que los niveles en la afectación económica pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que los rangos en cada nivel pueden ser adaptados a las necesidades y complejidad de cada entidad.

Determinación del nivel de riesgo inherente

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (Riesgo inherente), se trata de determinar los niveles de severidad, para lo cual se aplica la matriz definida en el numeral 3.2 de la presente guía:



Nota: Es necesario mencionar, que esta matriz de severidad está diseñada de acuerdo a estándares internacionales que permiten tener trazabilidad en los desplazamientos en cada zona, por lo que se recomienda no modificarla.

Ejemplo (continuación):

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad: Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta que los bienes muebles en cada entidad varía en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.

Aplicando las tablas de probabilidad e impacto tenemos:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año ymáximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año ymáximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 365 veces al año ymáximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al	100%

La actividad se realiza 365 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

Para determinar el impacto es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública.

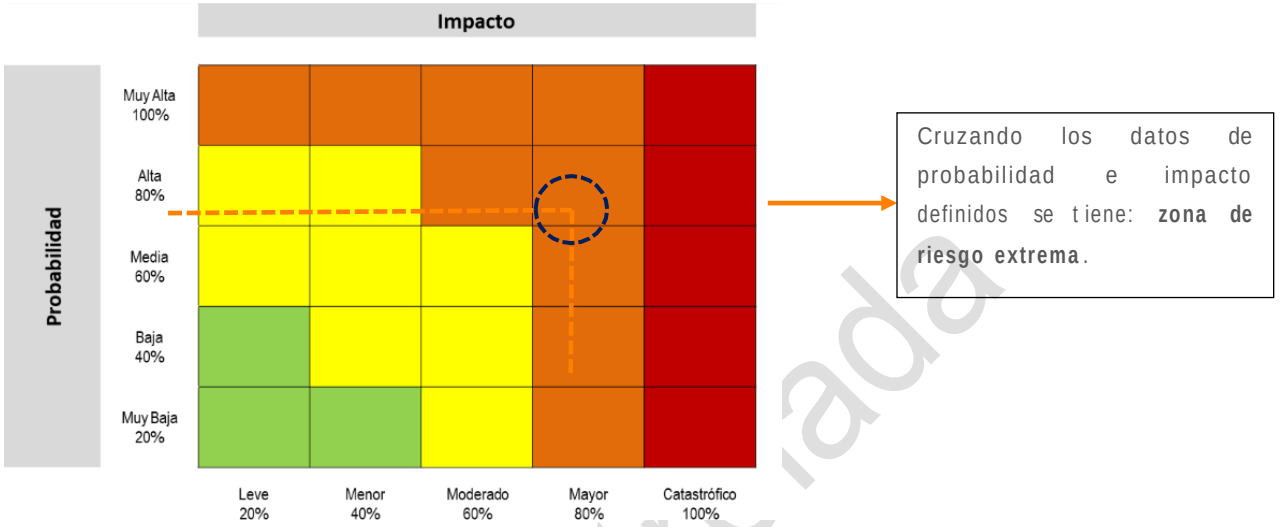
En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que para el ejemplo se determina que es de $2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico

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

La afectación económica se calcula en más de 500SMLMV, el impacto del riesgo es **catastrófico**.

Probabilidad inherente = media 60%, **Impacto inherente =** catastrófico 100%

Zona de severidad o nivel de riesgo: De acuerdo con la tabla para la definición de zona severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un nivel de riesgo extremo.



4.3.3 Valoración de controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Tipologías de controles:

Control Preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.

Control Detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.

Control Correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos.

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Se aplican los lineamientos para la redacción del control establecidos en el numeral 3.2.2.1 y tabla definida en el numeral 3.2.2.3 de la presente guía.

Ejemplo (continuación):

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimien to de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad Inherente: Media 60%

Impacto Inherente: Catastrófico 100%

Zona de riesgo: Extrema

Controles Identificados:

Control 1 Preventivo: El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.

Control 2 Detectivo: El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.

Control 3 Correctivo: El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.

Aplicando la tabla de valoración de controles tenemos:

Control 1	Criterios de efectividad			Peso
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 1 =40%			

Control 2	Criterios de efectividad			Peso
El coordinador administrativo verifica	Tipo	Preventivo		
		Detectivo	X	15%

Control 2	Criterios de efectividad			Peso
mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 2 = 30%			
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	X	10%
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 3 = 25%			

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a continuación se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y su respectiva valoración, a fin de determinar el riesgo residual.
Nivel de riesgo (riesgo residual):

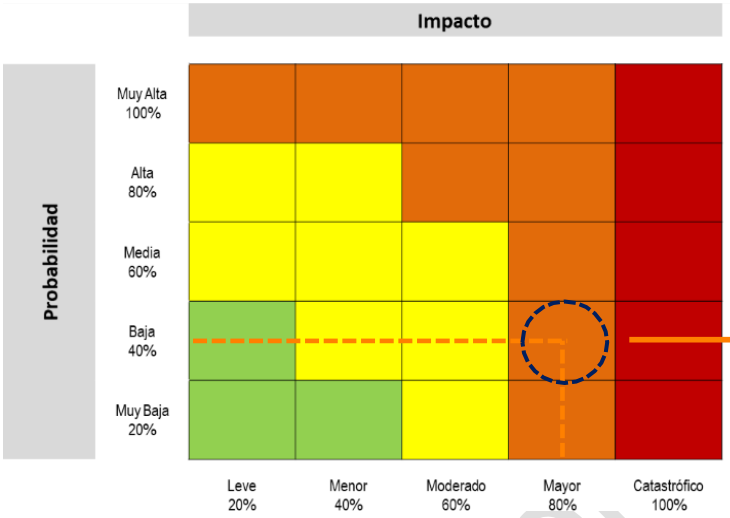
Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Para mayor claridad a continuación, siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de efectos dañoso sobre bienes públicos	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60%* 40% =24% 60% - 24% = 36%
(área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión de cumplimiento	Valor probabilidad para aplicar 2o control	36%	Valoración control 2 Detectivo	30%	36%* 30% =10.8% 36% - 10,8% = 25,2%
Del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona	Probabilidad Residual	25,2%	Valoración control correctivo	25%	100%* 25% =25% 100% - 25% = 75%
	Impacto Inherente	100%			

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
las pólizas cuando haya lugar (causa raíz).	Impacto Residua	75%			

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor, a continuación se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y cálculo final:



Cruzando los datos de probabilidad e impacto después de controles se tiene: **zona de riesgo alto.**

La anterior información puede trasladarse al mapa de riesgo que hace parte de la presente metodología.

REFERENCIAS BIBLIOGRÁFICAS

Celis, Ó. B. (2012). Gestión Integral de Riesgos. Bogotá D.C.: Consorcio Gráfico Ltda.

COSO Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise Risk Management. Integrating with Strategy and Performance. Durham: Association of International Certified Professional Accountants.

COSO Committee of Sponsoring Organizations of the Treadway Commission. PwC. Instituto de Auditores Internos de España. (2013). Control Interno - Marco Integrado. Marco y Apéndices. Instituto de Auditores Internos de España.

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA GTC 137. GESTIÓN DEL RIESGO. VOCABULARIO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2013). NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31010. GESTION DE RIESGOS. TÉCNICAS DE VALORACIÓN DEL RIESGO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Instituto de Auditores Internos de Colombia. (2017). MARCO INTERNACIONAL PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORÍA INTERNA. Bogotá D.C.

Núñez, A. C. (9 de 11 de 2016). Inboundlead Blog. Obtenido de Los 7 Mejores Ejemplos de Objetivos SMART: https://blog.inboundlead.com/los-7-mejores-ejemplos-de-objetivos-smart-o-inteligentes-para-empresas

INDICE DE TABLAS ILUSTRATIVAS

PÁGINA

ÍNDICE DE ESQUEMAS

PÁGINA

REVISADO POR: JEFE OFICINA ASESORA DE PLANEACIÓN, NORMALIZACIÓN Y CALIDAD (P2)	**APROBADO POR:** JEFE OFICINA ASESORA DE PLANEACIÓN, NORMALIZACIÓN Y CALIDAD (P2)	**FECHA DE IMPLEMENTACIÓN:** ABRIL 28 DE 2023