Aguas del Cesar
S.A. E.S.P.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

AGUAS DEL CESAR S.A. E.S.P

VIGENCIA 2025

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

TABLA DE CONTENIDO

Contenido

INTRODUCCIÓN

La presente Política de Administración del Riesgo establece los lineamientos institucionales para la identificación, valoración, tratamiento, seguimiento y comunicación de los riesgos que puedan afectar el logro de los objetivos estratégicos, misionales y de apoyo de Aguas del Cesar S.A. E.S.P. La gestión del riesgo se concibe como un componente transversal del Sistema de Control Interno y del Modelo Integrado de Planeación y Gestión – MIPG, orientado a fortalecer la toma de decisiones, la eficiencia institucional y la integridad pública en la prestación de los servicios de acueducto y alcantarillado en el Departamento del Cesar.

Esta política aplica a todos los procesos, proyectos, productos y actividades desarrollados por las áreas y servidores de la entidad, quienes deben incorporar la administración del riesgo en el ejercicio de sus funciones y en la planeación de su gestión.

La Política de Administración del Riesgo recoge la estrategia definida por la Alta Dirección, enfocada en la identificación, análisis, tratamiento y monitoreo de los riesgos de gestión, corrupción, fraude, fiscales, regulatorios y de seguridad de la información, promoviendo el diseño e implementación de controles que mitiguen la probabilidad de ocurrencia y el impacto de eventos adversos. Así mismo, orienta la preparación y ejecución de acciones de contingencia ante la materialización de dichos riesgos, garantizando la continuidad institucional, la sostenibilidad operativa y la protección del interés público.

La administración del riesgo en Aguas del Cesar S.A. E.S.P. se desarrolla en coherencia con el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno – MECI, las disposiciones del Decreto 1499 de 2017, los principios de la Norma Internacional ISO 31000:2018, y los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) emitida por el Departamento Administrativo de la Función Pública – DAFP.

Para Aguas del Cesar S.A. E.S.P., la política para la gestión integral de riesgos se debe considerar que:

- para su formulación se requiere del compromiso y responsabilidad por parte de la Alta Dirección (Línea Estratégica);
- debe aportar como

propósito fundamental al logro de los objetivos estratégicos de la entidad;
- debe partir del análisis del contexto interno y externo, así como de la consideración de riesgos emergentes, para prever la asignación de recursos y medidas consecuentes;
- debe definir los niveles de autoridad y responsabilidad frente al manejo de los riesgos, con el fin de garantizar eficiencia en la implementación y efectividad para evitar afectaciones por materializaciones del riesgo que impidan el logro de los objetivos institucionales y el buen uso de los recursos públicos.
Así, en una gestión integral del riesgo, la aplicación y el desarrollo de estas políticas Implican:

Desde la perspectiva de Gobernanza y Cultura:

✓ Incorporar cultura de integridad y transparencia en la administración de recursos.
✓ Exigir al Comité institucional de gestión y desempeño la supervisión activa del riesgo de los riesgos inherentes a la gestión presupuestal.

Desde la perspectiva de la definición de la Estrategia y el Establecimiento de Objetivos:

✓ Considerar en la articulación de la planeación estratégica con los Planes de Desarrollo (nacionales o territoriales) y los Planes Operativos Anuales de Inversión, el análisis de los riesgos presupuestales que puedan limitar o afectar su ejecución.
✓ Establecer objetivos presupuestales y financieros que apoyen el logro de los objetivos estratégicos previstos.

Desde la perspectiva de identificación y Evaluación de Riesgos:

✓ Realizar mapas de riesgos considerando los riesgos propios de la gestión presupuestal y de contratación.
✓ Evaluar el impacto de los riesgos en eficiencia del gasto público y el cumplimiento de la regla fiscal.
✓ Considerar análisis prospectivos (riesgos macroeconómicos, caída de ingresos tributarios, retrasos en transferencias, entre otros).

Desde la perspectiva de la respuesta al riesgo y la selección de Estrategias:

✓ Definir controles internos presupuestales basados en riesgos, no solo en procedimientos normativos.
✓ Implementar alertas o indicadores claves sobre sobre los riegos presupuestales y de contratación identificados.

Desde la perspectiva de información, comunicación y reporte:

✓ Publicar la información presupuestal, conforme la normativa vigente.
✓ Elaborar y comunicar informes de gestión que den cuenta de la eficiencia y efectividad del gasto, más allá del cumplimiento de las apropiaciones.
✓ Promover la comunicación abierta y oportuna con los diferentes grupos de valor y otras partes interesadas, respecto a los resultados de la gestión presupuestal y contractual (rendición de cuentas).

Desde la perspectiva de revisión y Monitoreo:

✓ Facilitar las auditorías internas y externas y propiciar en estas la cobertura de los riesgos presupuestales críticos.
✓ Incorporar indicadores de desempeño y costo-eficiencia en el ciclo presupuestal.
✓ Promover el uso de herramientas analíticas para detectar alertas tempranas de corrupción o ineficiencia en la gestión presupuestal y de contratación.

De conformidad con el Anexo técnico del Decreto 1122 de 2024, los Programas de Transparencia y Ética Pública – PTEP, se constituyen en el conjunto de acciones que una entidad define e implementa para promover, al interior de la organización, una cultura de la legalidad e identificar, medir, controlar y monitorear los riesgos de corrupción que se presentan en el desarrollo de su misionalidad herramientas para que las entidades públicas implementen acciones para promover la cultura de la legalidad, identificar, medir, controlar y monitorear los riesgos de corrupción.

A su vez, el Programa de Transparencia y Ética Pública, en relación con el MIPG, vincula lineamientos de diferentes políticas de gestión y desempeño, con el fin de generar un esquema articulado para la prevención, detección y respuesta a situaciones que afecten la transparencia y la ética pública, que pueden configurarse en diferentes ámbitos de la gestión institucional, lo que exige un análisis integral de los procesos que se

desarrollan en las entidades. Se trata entonces de vincular en el PTEP herramientas e instrumentos de gestión de riesgos ya desarrollados por políticas institucionales, para una gestión integral de prevención, detección y respuesta frente a riesgos de corrupción, fraude o soborno; de los conflictos de interés, los incumplimientos al código de integridad, riesgos fiscales, de lavado de activos y otros que puedan afectar la imagen y confianza institucional de cara a la ciudadanía.

1. MARCO NORMATIVO

- **Ley 87 de 1993:** Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 Objetivos del Control Interno: Literal
  a) Proteger los recursos de la organización, buscando adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
- Ley 489 de 1998: Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno.
- Directiva presidencial 09 de 1999 Lineamientos para la implementación de la política de lucha contra la corrupción.
- Decreto 1537 de 2001 Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las empresas y organismos del Estado. El parágrafo del Artículo 4º señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (…) y en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su Artículo 4º la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…).
- **Ley 1474 de 2011:** Estatuto Anticorrupción Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las

entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.

- **Decreto 1649 de 2014 Funciones de la Secretaría de Transparencia:** 13) Señalar la metodología para diseñar y hacer seguimiento a las estrategias de lucha contra la corrupción y de atención al ciudadano que deberán elaborar anualmente las entidades del orden nacional y territorial.
- **ISO 9001:2015**: Norma Técnica Colombiana, elaborada por la Organización Internacional para la Estandarización (International Standarization Organization o ISO por sus siglas en inglés), determina los requisitos para un Sistema de Gestión de la Calidad.
- **Decreto 1081 de 2015:** Señala como metodología para elaborarla estrategia de lucha contra la corrupción la contenida en el documento “Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.
- **Decreto Nacional 1499 de 2017:** hace necesario adoptar para la Alcaldía municipal el MIPG, como el nuevo marco de referencia para el diseño e implementación del SIG, con el fin de fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades de la alcaldía municipal adecuar la institucionalidad del sistema y de las instancias correspondientes con el modelo nacional.
- **ISO 31000:2018:** Norma Técnica Internacional Administración del Riesgo-Principios y orientaciones.
- Guía para la Gestión Integral del Riesgo en Entidades PúblicasVersión 7 Agosto de 2025.

2. CONCEPTO BASICOS DE LA GESTION DEL RIESGO

Administración de riesgos: 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (INTOSAI, 2000).

Análisis de riesgo: Uso sistemático de la información disponible para valorar los riesgos en función

de las causas o agentes que los generan, las consecuencias generadas por un incidente y/o evento, su severidad y la posibilidad de ocurrencia del mismo, con el fin de estimar la zona de riesgo inicial (riesgo inherente).

Causa: Medios, circunstancias, situaciones o agentes generadores del riesgo. Algunas fuentes de riesgos son: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Consecuencia: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento

Control: Cualquier medida que adopte la entidad para gestionar los riesgos y proporcionar una seguridad razonable de alcanzar los objetivos y metas establecidos

Evaluación del riesgo: Determinación de las prioridades de gestión del riesgo, mediante la comparación del nivel de riesgo hallado (riesgo inherente) y la evaluación de las medidas de control existentes. Es una etapa que busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).

Gestión del riesgo: Es el conjunto de “Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Contempla las etapas de política de administración del riesgo, construcción del mapa de riesgos, comunicación y consulta, monitoreo y revisión y seguimiento.
Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- ✓ **Nota 1**: 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 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.

Probabilidad: se entiende 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: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

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

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Programa de Transparencia y Ética Pública (PTEP): es una estrategia obligatoria para entidades públicas en Colombia, creada por la Ley 2195 de 2022, que busca prevenir la corrupción, promover la cultura de la legalidad, gestionar riesgos, mejorar el acceso a la información y servicios, y fomentar la participación ciudadana y rendición de cuentas.

CICCI: Comité Institucional de Coordinación de Control Interno.

CGDI: Comité de Gestión y Desempeño Institucional. Fraude: Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Mapas de riesgo: Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.

MIPG: Modelo Integrado de Planeación y Gestión

MECI: Modelo Estándar de Control Interno Restablecimiento: Capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.

Riesgos Operativos: Posibilidad de incurrir en pérdidas por errores, fallas o deficiencias en el Talento Humano,

Procesos, Tecnología. Infraestructura y Eventos Externos.

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

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

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.

Tratamiento del riesgo: Proceso para modificar el riesgo.

Valoración del Riesgo: Establece la identificación y evaluación de los controles. En la etapa de valoración del riesgo se determina el riesgo residual.

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
Apetito de riesgo: es el nivel de riesgo que una entidad está dispuesta a asumir 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 gestionar.
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. (relacionado con la solvencia y liquidez).

3. METODOLOGÍA APLICADA

La presente Política de Administración del Riesgo desarrolla su gestión siguiendo los lineamientos fundamentales establecidos en la **Guía para la Gestión Integral del Riesgo en**

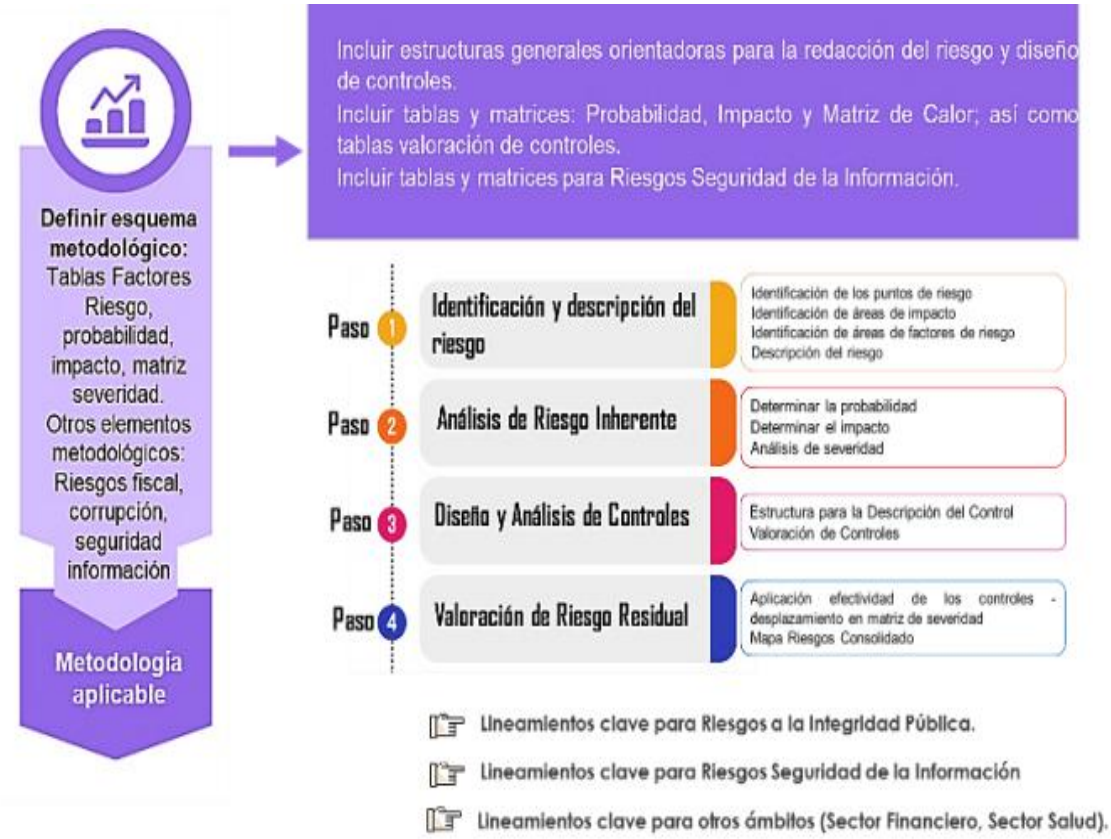
Entidades Públicas– Versión 7 (2025), emitida por el **Departamento Administrativo de la Función Pública – DAFP**, asegurando su coherencia con el **Modelo Integrado de Planeación y Gestión – MIPG**, el **Modelo Estándar de Control Interno – MECI**, y la **Norma ISO 31000:2018.**

La gestión integral de riesgos, es posible definirla como "*la cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo, de cara la creación, preservación y materialización de valor.*" (IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.10). Esta definición, adoptada, implica que la gestión del riesgo se consolida a través de: i) el reconocimiento de la cultura; ii) el desarrollo de capacidades; iii) el uso de las técnicas aplicadas; iv) la integración de la estrategia y el desempeño; v) la alineación con la estrategia y objetivos clave y vi) la relación con el valor.

La metodología aplicada se estructura en tres (3) pasos estratégicos fundamentales, que permiten la **identificación, análisis del riesgo inherente, diseño y análisis de controles de los riesgos y valoración del riesgo residual** de manera sistemática, garantizando la integración de la gestión de riesgos en todos los procesos, planes, proyectos y actividades de la Alcaldía Municipal**.**

Para su implementación efectiva la política será necesario desplegar una estructura metodológica tomando como referencia la dispuesta en la guía, considerando elementos básicos como i) tabla factores de riesgo; ii) tablas de probabilidad e impacto; iii) matriz de severidad; iv) tabla valoración controles. Así mismo, se incluye lineamientos clave para los riesgos a la Integridad Pública, riesgos fiscales y riesgos de seguridad de información, así como otros marcos y normatividad aplicable.

A continuación, se presenta la estructura operativa de la metodología, con sus desarrollos básicos, que sirven como guía para la aplicación coherente y sistemática de la política en toda la Administración Municipal.

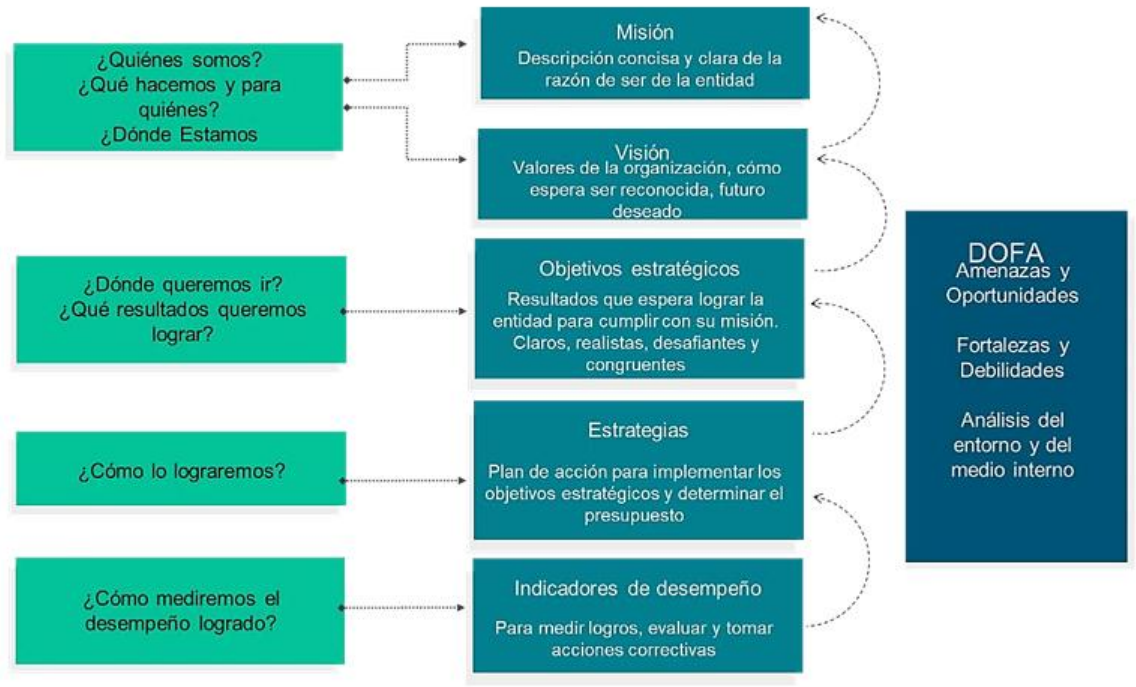


Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 de 2025

4. ANÁLISIS ESTRATÉGICO DE LA ENTIDAD Y SU MODELO DE OPERACIÓN BASADA EN PROCESOS:

Para el análisis estratégico de la entidad es necesario que el Modelo Integrado de Planeación y Gestión (MIPG) sea visto de manera integral, dado que las políticas y dimensiones que lo integran se articulan de manera directa con una adecuada gestión por procesos. En particular, la dimensión de Direccionamiento Estratégico contempla que una entidad debe realizar un análisis del entorno tanto específico como general, así como un análisis de capacidades internas. Se desarrolla un modelo básico de planeación estratégica, donde se precisan las preguntas que pueden orientar la construcción de cada uno de los componentes:

Figura 4 Modelo básico de planeación estratégica



Niveles de Madurez para la Gestión del Riesgo:

Teniendo en cuenta que la gestión estratégica del riesgo involucra una serie componentes y elementos que se deben fortalecer desde la cultura organizacional, se hace necesario evaluar su nivel de madurez. Para este efecto, atendiendo uno de los marcos que sustentan el desarrollo de la presente guía que corresponde al COSO-ERM-2017 se propone una estructura que, "consta de cinco componentes interrelacionados de la gestión del riesgo empresarial y su relación con la misión, visión y valores clave de la entidad". Los cinco componentes que integran una óptima gestión del riesgo a la luz de este marco de referencia, se describen a continuación:

Componente	Principios
Gobierno y Cultura	Supervisión de riesgos a través del consejo de administración.
	Establece estructuras operativas
	Define la cultura deseada
	Demuestra compromiso con valores clave
	Atrae, desarrolla y retiene a profesionales capacitados
Establecimiento de la estrategia y objetivos	Analiza el contexto (externo e interno)
	Define el apetito del riesgo
	Evalúa estrategias alternativas
	Formula objetivos estratégicos y operacionales
Desempeño	Identifica y describe el riesgo
	Evalúa el riesgo inherente
	Diseña controles efectivos
	Prioriza riesgos
	Desarrolla visión integral
Análisis y monitorización	Evalúa los cambios significativos
	Revisa el riesgo y el desempeño
	Persigue la mejora de la gestión del riesgo
Información, Comunicación y Reporte	Aprovecha la información y la tecnología
	Comunica información sobre riesgos
	Informa sobre el riesgo, la cultura y el desempeño

Fuente: Adaptado por Dirección de Gestión y Desempeño Institucional a partir de Auditoria Interna y gestión de riesgos, Instituto de Auditores de España. Octubre 2021

5. OBJETIVO GENERAL

Establecer el marco institucional y los elementos fundamentales para la gestión integral de los riesgos a los que se enfrenta Aguas del Cesar S.A. E.S.P., de cualquier naturaleza, asegurando la identificación, análisis, evaluación, tratamiento, control y seguimiento de los mismos.

La política orienta la respuesta oportuna a amenazas que puedan generar eventos con impacto en el logro de los objetivos estratégicos, misionales y de apoyo de la entidad, considerando los riesgos de gestión, corrupción, seguridad y privacidad de la información, fraude, fiscales y regulatorios, y definiendo niveles claros de responsabilidad en cada proceso.

6. OBJETIVOS ESPECIFICOS

- Establecer lineamientos y criterios técnicos que orienten a la Alcaldía Municipal en la gestión integral de riesgos, considerando los elementos de contexto estratégico, identificación, análisis, valoración, políticas de administración del riesgo, trazabilidad, registro y monitoreo, de conformidad con la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025), el MIPG y la Norma ISO 31000:2018.
- Orientar la toma de decisiones estratégicas y operativas, minimizando efectos adversos en los procesos institucionales, garantizando la continuidad de la gestión y el logro de los objetivos misionales y estratégicos.
- Fomentar la adopción de un enfoque de pensamiento basado en riesgos dentro de la Entidad, promoviendo la identificación temprana de riesgo y la cultura de prevención en todas las dependencias.
- Promover la mejora continua en los procesos institucionales mediante la implementación de controles, la evaluación periódica de riesgos y la retroalimentación de los resultados de gestión.
- Realizar seguimiento, evaluación y reporte de los riesgos asociados a los procesos y actividades de la entidad, asegurando la efectividad de los controles y la implementación de medidas correctivas oportuna.
- Garantizar una gestión integral de riesgos, mediante la identificación de acciones de control, la definición de respuestas oportunas y la implementación de estrategias institucionales que mitiguen la ocurrencia de eventos que afecten el cumplimiento de la misión y el logro de los objetivos institucionales

7. ALCANCE

La presente Política de Administración del Riesgo es de aplicación a todas las áreas, procesos y servidores en todos los niveles jerárquicos de Aguas del Cesar S.A. E.S.P., comprendiendo los objetivos estratégicos, planes, programas, proyectos, productos y actividades desarrollados en la entidad dentro del Departamento del Cesar.

Su implementación asegura que la gestión de riesgos sea transversal e integrada, promoviendo la identificación, análisis, tratamiento, monitoreo y control de los riesgos de gestión, corrupción, fraude, fiscales, regulatorios y de seguridad de la información

- ✓ **Riesgos de Gestión y Riesgos de Corrupción y Fraude:** Aplican a todos los procesos misionales, estratégicos y de apoyo de Aguas del Cesar S.A. E.S.P., incluyendo operación técnica de acueducto y alcantarillado, proyectos de infraestructura, planeación institucional, contratación y control interno.

- ✓ **Riesgos del Sistema de Gestión de Seguridad de la Información - Seguridad Digital:** Comprenden los procesos que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información (SGSI), tales como:
  Procesos misionales de operación técnica y control de calidad del agua.
  Procesos de planeación y gestión documental.
  Procesos de TIC y soporte tecnológico.

8. CONTEXTO INTERNO Y EXTERNO:

Para garantizar una gestión integral del riesgo alineada con los objetivos institucionales, Es necesario desplegar un análisis interno y externo específico para la entidad, donde se expliquen mediante información institucional formalizada y datos específicos relacionados, teniendo en cuenta los siguientes elementos:

✓ Contexto Interno: estructura organizacional, cultura institucional, capacidad tecnológica, talento humano, procesos internos, recursos financieros, políticas internas y marco normativo aplicable.

✓ Contexto Externo: entorno político, económico, social, ambiental y tecnológico; actores del sector, reguladores, organismos de control, ciudadanos y partes interesadas, así como riesgos asociados a cambios normativos y eventos externos. Sector donde opera la entidad y su relacionamiento con otras entidades e instancias necesarias para su gestión, así como entorno de desarrollo territorial**.**

El análisis del contexto permite identificar aquellos riesgos que podrían afectar el cumplimiento de los objetivos estratégicos, asegurando que la **gestión del riesgo** se

enfoque en los eventos con mayor impacto institucional.

Tabla 1 Contexto Estratégico

CONTEXTO ESTRATEGICO	
CONTEXTO EXTERNO	**Económicos**: Disponibilidad de Capital, Liquidez; mercados financieros, desempleo, competencia.
	Políticos: Cambio de Gobiernos, Legislación, Políticas Públicas, regulación.
	Sociales y Culturales: Demografía, responsabilidad social, Orden Público.
	T**ecnológico**: Avances en tecnologías, Accesos a sistema de información externo, Tecnología emergente, Gobierno en Línea.
	Medioambientales: Condiciones ambientales, emisiones, residuos, energía, agua, catástrofes naturales, desarrollo sostenible,
	Comunicación Externa: Mecanismos para estar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.
CONTEXTO INTERNO	**Financieros**: Presupuesto de funcionamiento, recurso de inversión, infraestructura, capacidad instalada.
	Personal: Evaluar la Competencia del personal, Identificar oportunidades de desarrollo profesional, disponibilidad.
	Proceso: 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
	Estructura Organizacional: 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
CONTEXTO DEL PROCESO	**Diseño de Procesos**: Claridad en la descripción, alcance, objetivos del proceso
	Interacción con otros Procesos: Relación precisa con otros procesos en cuanto al insumo, proveedores, producto, usuario cliente.
	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 Procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.

9.NIVELES DE AUTORIDAD Y RESPONSABILIDADES – ROLES

En el marco del Esquema de Líneas de Defensa, se establecen las periodicidades y responsables para el seguimiento a los riesgos estratégicos y operativos de la entidad, considerando con especial relevancia las responsabilidades de la Línea Estratégica y Alta Dirección en términos de la definición del apetito de riesgo, la aprobación de la política y la asignación de

recursos para su implementación.

La primera línea, conformada por los líderes de proceso, es responsable de identificar, evaluar y controlar riesgos en sus diferentes procesos, proyectos o iniciativas estratégicas. Todos los servidores de la entidad tienen la responsabilidad de reportar oportunamente los riesgos materializados, aplicar los controles establecidos y proponer mejoras cuando sean necesarias.

Este esquema de líneas de defensa, como componente del Modelo Integrado de Planeación y Gestión (MIPG), permite establecer con claridad los roles y responsabilidades tanto de los servidores como de los órganos de dirección involucrados, conforme se detalla a continuación:

Línea Estratégica. Alta dirección y Comité Institucional de Coordinación de Control Interno, a quienes corresponde**:**

Alta Dirección

- ✓ Revisar el Contexto, la plataforma estratégica, el modelo de Operación por proceso y la planeación Institucional, con el fin de identificar posibles cambios que puedan generar nuevos riesgos o modificar los ya existentes.
- ✓ Examinar la información relacionada con el cumplimiento de los Objetivos institucionales y de los diferentes procesos, en lo que respecta a la implementación de la gestión del riesgo con el propósito de evaluar su efectividad y continuidad.
- ✓ Analizar el informe de evaluación de la gestión del riesgo y en caso de ser necesario, formular propuestas o acciones de mejora para los planes para el tratamiento de los mismos.
- ✓ Asumir la responsabilidad primaria del Sistema de Control Interno y de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo.

Comité Institucional de Coordinación de Control Interno

- ✓ Someter a aprobación del representante legal de la entidad la política de administración del riesgo, garantizando su alineación con el direccionamiento estratégico institucional.

- ✓ Evaluar y emitir lineamientos técnicos en materia de administración del riesgo, con el fin de orientar su adecuada implementación en todos los niveles de Aguas del Cesar S.A. E.S.P.
- ✓ Proveer retroalimentación a la alta dirección respecto al monitoreo y la efectividad de la gestión del riesgo y de los controles establecidos. Asimismo, realizar seguimiento a su implementación, gestionar los riesgos estratégicos y asegurar la aplicación eficaz de los controles correspondiente**.**
- ✓ Evaluar los planes de tratamiento definidos para los riesgos materializados, con el objetivo de reducir la probabilidad de recurrencia de los eventos.

Primera Línea. En Aguas del Cesar S.A. E.S.P., la primera línea de defensa está conformada por los gerentes públicos y líderes de proceso, quienes tienen la responsabilidad directa sobre la administración y gestión integral de riesgos en sus áreas. Les corresponde:

- ✓ Evaluar los cambios en el direccionamiento estratégico o en el contexto estratégico, identificando cómo dichos cambios pueden generar nuevos riesgos o modificar los ya existentes.
- ✓ **Liderar la identificación de los riesgos asociados al proceso o procesos bajo su responsabilidad,** conforme a las directrices establecidas en el procedimiento vigente de administración de riesgo.
- ✓ **Gestionar los riesgos identificados con el apoyo del equipo de trabajo,** lo cual incluye su análisis, calificación, definición de controles, ejecución de acciones y seguimiento periódico, conforme a los lineamientos establecidos para su tratamiento y mejora continua.
- ✓ **Revisar, actualizar y hacer seguimiento periódico a los mapas de riesgos**, - de acuerdo con los lineamientos institucionales, informando cualquier ajuste a la Oficina de Planeación y Control Interno
- ✓ **Socializar los controles implementados**, garantizando su adecuada comprensión y oportuna aplicación por parte de los actores involucrados, así como la difusión de la información necesaria sobre la gestión del riesgo, en los espacios previamente definidos.
- ✓ **Evaluar de manera periódica la eficacia de los controles establecidos para el**

tratamiento de los riesgos identificados, y actualizar los riesgos cuando se presenten cambios en la operatividad del proceso fuente.

✓ **Reportar los planes de tratamiento correspondientes a los riesgos materializados,** incluyendo las acciones orientadas a prevenir su repetición, así como la identificación de las causas que originaron dichos eventos.

Servidores y contratistas de acuerdo con las funciones, obligaciones, roles y responsabilidades.

✓ **Participar activamente en la construcción y administración de los riesgos asociados al proceso en el cual desempeñan sus funciones o desarrollan sus actividades**, contribuyendo al fortalecimiento de la gestión del riesgo institucional.

✓ **Conocer los riesgos vinculados al proceso en el que ejercen sus funciones, así como los riesgos generales de la Entidad**, con el propósito de identificar aquellos no previstos por los líderes de otros procesos y aportar a su gestión integral.

✓ **identificar, registrar y reportar de manera oportuna los riesgos potenciales y/o la posible materialización de riesgos previamente identificados,** con el fin de facilitar su tratamiento adecuado y la implementación de acciones de mitigación eficaces.

Segunda Línea. La segunda línea de defensa en Aguas del Cesar S.A. E.S.P. está conformada por servidores que ocupan cargos del nivel directivo o asesor, quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.

Esta línea incluye a los líderes de áreas estratégicas y de apoyo, tales como:

- Oficina Asesora de Planeación
- Dirección Financiera
- Secretaría General
- Dirección Administrativa y de Gestión Humana
- Dirección Técnica
- Dirección de Aseguramiento de la Prestación del Servicio
- Servidores responsables de monitoreo y evaluación de controles internos

Jefe Asesor de la oficina de Planeación

- ✓ **Determinar la metodología para la identificación y gestión de riesgos,** en cumplimiento de la normatividad vigente y los lineamientos institucionales, para cada una de las tipologías de riesgo, con excepción de aquellas que, por su naturaleza específica, requieren un desarrollo metodológico particular, como los riesgos ambientales, los de seguridad y salud en el trabajo, y los de seguridad de la información.
- ✓ **Realizar el monitoreo continuo del mapa de riesgos,** evaluando la efectividad de los controles y sus respectivas acciones, e identificando aquellas situaciones que obstaculicen o impidan una adecuada gestión de riesgos, en concordancia con la promoción de la cultura del autocontrol dentro de la entidad.
- ✓ **Formular lineamientos técnicos que orienten a los procesos institucionales,** para garantizar una gestión de riesgos eficaz, eficiente y efectiva en todos los niveles organizacionales.
- ✓ **Coordinar y liderar la ejecución de las etapas definidas para el diseño e implementación del componente de administración de riesgos**, mediante el uso de la herramienta institucional dispuesta para tal propósito.
- ✓ **Consolidar y publicar el mapa de riesgos institucional,** asegurando su actualización, difusión y disponibilidad para todos los actores relevantes dentro de la entidad.
- ✓ **Brindar acompañamiento y asesoría metodológica a los diferentes procesos,** en el marco de la gestión integral de riesgos, en articulación con la tercera línea de defensa, con el fin de fortalecer la capacidad.

Dirección Financiera

Determinar e implementar la metodología específica para la identificación, análisis, tratamiento, seguimiento y monitoreo de los riesgos propios de su competencia, conforme a la normatividad vigente y a los lineamientos o parámetros institucionales establecidos, con especial énfasis en la gestión de esta tipología particular de riesgo**.**

Secretaria General - Gestión Contractual:

- ✓ **Revisar que en los estudios previos la tipificación, distribución y asignación**

de los riesgos previsibles se realice dentro del marco legal vigente, sin vulnerar los derechos de las partes involucradas ni de terceros interesados. Asimismo, verificar que la modalidad de contratación seleccionada sea la más adecuada, en cumplimiento de la Ley 1150 de 2007 y sus normas reglamentarias, considerando la justificación presentada por la dependencia solicitante para la adquisición del bien, servicio u obra.

- ✓ **Verificar el comportamiento de los riesgos asociados a cada contrato bajo su supervisión y/o interventoría,** prestando especial atención al seguimiento y reporte de los eventos relacionados con las partes responsables de asumir dichos riesgos. En caso de presentarse eventos que puedan impactar el valor del contrato, se deberá informar de forma inmediata al Ordenador del Gasto, para la adopción de las medidas correctivas pertinentes**.**
- ✓ **Revisar y proponer ajustes a los procedimientos y al Manual de Contratación y del Comité de Contratación,** con el fin de asegurar la correcta aplicación de la Política Integral de Administración de Riesgos en todos los procesos de selección y contratación de la entidad**.**
- ✓ **Adoptar, para la gestión de los riesgos relacionados con la contratación estatal, lo dispuesto en el Manual de contratación en los Procesos de Contratación,** así como en cualquier otro instrumento que sea emitido en la materia. Igualmente, incorporar las disposiciones establecidas en los documentos CONPES 3186 de 2002 y 3714 de 2011, u otros que sean emitidos por el Gobierno Nacional sobre riesgos contractual.

Tercera Línea – Oficina de Control Interno

Esta línea está bajo la responsabilidad de la (el) profesional asesor de control interno; desarrollaran su labor a través de los siguientes roles a saber: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento.

El funcionario responsable y líder del proceso de Control Interno evalúa manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la 2ª línea de defensa**.**

- ✓ Hacer seguimiento a la evolución de los riesgos y al cumplimiento de las acciones propuestas, con el fin de

verificar su ejecución, y si es necesario proponer mejoras.

- ✓ Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la Entidad**.**

- ✓ Adelantar el registro de no conformidades, en el marco de las auditorías internas, cuando se constituya un incumplimiento en la aplicación de la política de riesgo, las cuales permiten eliminar la causa que originó dicha situación; de ser reiterativa, se presentará a consideración del Comité Institucional de Coordinación de Control Interno, para que adopte las decisiones pertinentes.

- ✓ Comunicar al Comité de Coordinación de Control Interno posibles cambios evidenciados en la evaluación del riesgo, detectados durante las auditorias**.**

- ✓ **Adelantar el seguimiento a los mapas de riesgos, verificando y evaluando que los líderes de los procesos desarrollen adecuadamente las etapas de identificación, valoración, seguimiento y control de los riesgos identificados, y que adelanten acciones que permitan su administración.**

Tabla No. 2 Roles y responsabilidades para la administración del Riesgo

LINEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Línea Estratégica	Alta Dirección Comité Institucional de Coordinación de Control Interno	Esta línea al ser una instancia decisoria dentro del sistema de Control Interno, su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad. Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la Línea Estratégica: • Fortalecimiento del Comité Institucional de Coordinación de Control Interno incrementando su periodicidad para las reuniones. • Evaluación de la forma como funciona el Esquema de Líneas de Defensa, incluyendo la línea estratégica. • Definición de líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• Definición y evaluación de la Política de Administración del

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		entidad, cambios en el entorno que puedan definir ajustes,

		dificultades para su desarrollo, riesgos emergentes.

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		Humano (forma de provisión de los cargos, capacitación,

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

- Define el marco general para la gestión del riesgo y el

		control; y supervisar su cumplimiento.

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		niveles, quienes aplican las medidas de control interno en las operaciones

		del día a día de la entidad. su rol principal es el mantenimiento efectivo de

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		protocolos y otras herramientas que permitan tomar acciones

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		así como su seguimiento, acorde con el diseño de dichos

		controles, evitando la materialización de los riesgos.

		• El seguimiento a los indicadores de gestión de los procesos e

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

- La formulación de planes de mejoramiento, su aplicación y

		seguimiento para resolver los hallazgos presentados.

		• La coordinación con sus equipos de trabajo, de las acciones

		establecidas en la planeación institucional a fin de contar con

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		aplicada por parte de la 2ª línea de defensa.

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		cuentas ante la Alta Dirección**.**

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		o quienes hagan sus veces; coordinadores de equipos de trabajo,

		coordinadores de sistemas de gestión, gerentes de riesgos, líder de

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		con la complejidad y misionalidad de la entidad.

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		de la 1ª línea de defensa sean apropiados y funcionen correctamente,

		además, se encarga de supervisar la eficacia e implementación de las

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• Consolidación y análisis de información sobre temas claves

		para la entidad, base para la toma de decisiones y de las

		acciones preventivas necesarias para evitar materializaciones

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• Realizar el seguimiento al mapa de riesgos de su proceso.

		• Proponer las acciones de mejora a que haya lugar posterior al

		análisis, valoración, evaluación o tratamiento del riesgo.

		• Actualizar, según se requiera, los escenarios de riesgo y la

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• Supervisar la implementación de las acciones de mejora o la

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• La (El) Jefe de Oficina Jurídica tendrá el compromiso de

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• Trabajo coordinado con las oficinas de control interno o quien

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		requerida (auditoría interna a sistemas de gestión,

		seguimientos a través de herramientas objetivas, informes con

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• Acompañar, orientar y entrenar a los líderes de procesos en la

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• Supervisar en coordinación con los demás responsables de

		esta segunda línea de defensa, que la primera línea identifique,

		analice, valore, evalúe y realice el tratamiento de los riesgos,

		que se adopten los controles para la mitigación de los riesgos

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		la probabilidad o impacto de los riesgos.

		• Monitorear los controles establecidos por la primera línea de

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

Calle 28 No. 6ª – 15 Barrio Santa Rosa.
PBX: + (57) 5901166 Teléfono: 5901167
Correo: adcsaesp@aguasdelcesar.com.co
Valledupar - Cesar – Colombia

		• Evaluar que la gestión de los riesgos este acorde con la

		presente política de la entidad y que sean monitoreados por la

		primera línea de defensa. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.
Tercera Línea	Oficina de Control Interno quien haga sus veces	Esta línea está bajo la responsabilidad de la (el) profesional asesor de control interno; desarrollaran su labor a través de los siguientes roles a saber: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento. El funcionario Responsable y líder del proceso de Control Interno evalúa de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la 2ª línea de defensa. Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 3ª Línea**:** • A través de su rol de asesoría orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Secretaria de Planeación o quien haga sus veces se garantiza el cumplimento efectivo de los objetivos. • Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. • Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. • Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. • Informar los hallazgos y proporcionar recomendaciones de forma independiente. • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa • Recomendar mejoras a la política de operación para la administración del riesgo.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicad Versión 7 de 2025

9. DESARROLLO DEL ESQUEMA METODOLOGICO

9.1. RIESGO INTEGRAL DEL RIESGO

La metodología para la Administración del Riesgo en **Aguas del Cesar S.A. E.S.P.** se define a partir de los lineamientos establecidos por el **Departamento Administrativo de la Función Pública (DAFP)** en la **Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025)**, considerando las etapas de **identificación, valoración, tratamiento, seguimiento y comunicación**.

El análisis integral de los riesgos contempla aquellos eventos que puedan afectar el cumplimiento de las funciones y objetivos institucionales, incluyendo:

- La afectación al patrimonio público y la sostenibilidad financiera.
- La vulneración de activos de información y sistemas tecnológicos.
- La pérdida de confianza por parte de usuarios, comunidades, entes de control y demás partes interesadas.
- Conductas asociadas a corrupción, fraude o incumplimiento ético que comprometan la integridad del servicio público.

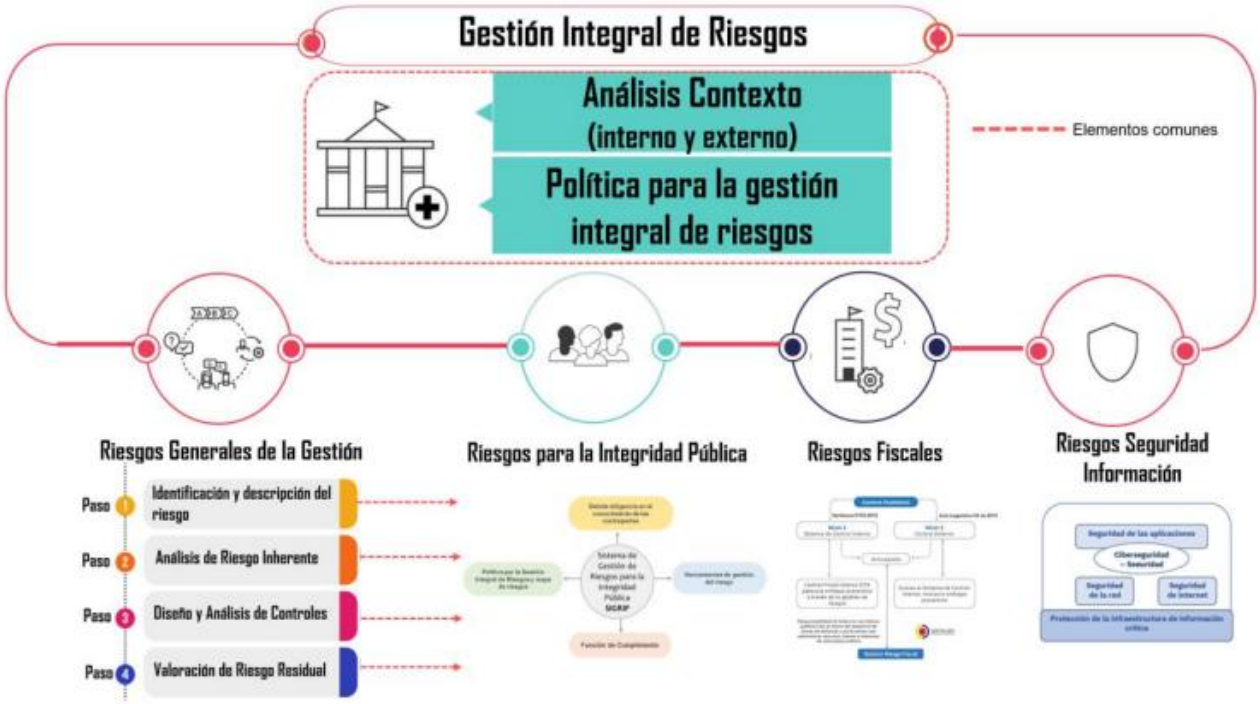
La política adopta un enfoque transversal, aplicable a todas las tipologías de riesgo que afectan a la entidad, y se desarrolla mediante los siguientes pasos metodológicos:

1. **Identificación y descripción del riesgo:**
   - Reconocimiento de eventos potenciales que puedan afectar los procesos misionales, estratégicos o de apoyo.
   - Definición clara del riesgo, sus causas, consecuencias y factores asociados.
2. **Análisis del riesgo inherente:**
   - Evaluación de la probabilidad y el impacto del riesgo en ausencia de controles.
   - Determinación del nivel de severidad inicial.
3. **Diseño y análisis de controles:**
   - Identificación de medidas existentes o propuestas para mitigar el riesgo.
   - Evaluación de su eficacia, cobertura, oportunidad y trazabilidad.
4. **Valoración del riesgo residual:**

- Recalificación del riesgo considerando la efectividad de los controles aplicados.
- Determinación del nivel final de exposición y definición de acciones de tratamiento.

Este enfoque permite a **Aguas del Cesar S.A. E.S.P.** integrar la gestión del riesgo en todos sus procesos, fortalecer la toma de decisiones, garantizar la continuidad operativa y proteger el interés público en la prestación de los servicios de acueducto y alcantarillado en el Departamento del Cesar.

Figura 13 Articulación ámbitos gestión del riesgo



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

9.1.1. Identificación y descripción del Riesgo.

Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente

identificados:

El objetivo de la identificación del riesgo es reconocer los riesgos a los que está expuesta la entidad, ya sea que se encuentren bajo el control directo de la entidad o no, considerando el contexto estratégico, los objetivos institucionales y la caracterización detallada de cada proceso, incluyendo su propósito, alcance y factores internos y externos que puedan impactar su desempeño.

En esta etapa se identifican los riesgos asociados a los objetivos estratégicos y a todos los procesos de la entidad, asegurando como mínimo un riesgo por proceso u objetivo, con su respectivo análisis.

Para una identificación asertiva y precisa de los riesgos claves de cada proceso, deberán considerarse aquellos eventos que podrían afectar de forma previsible el logro de los objetivos de proceso, considerados y ya descritos con los atributos SMART, incluidos en el Análisis Estratégico de la entidad y su modelo de Operación basada en procesos

La identificación de riesgos se realiza bajo un enfoque sistemático, transversal a toda la entidad, asegurando una base sólida para el análisis, tratamiento y seguimiento efectivo de los riesgos institucionales.

Fuentes generadoras del Riesgo: Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

Tabla 3 Fuentes Generadoras de Riesgo

Factor	Definición		Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional		Falta de aplicación de los procedimientos
			Falta segregación de funciones
			Errores de grabación, autorización
			Falta de supervisión o interventoría

Factor	Definición		Descriptores
			Errores en cálculos para pagos internos y externos
			Alta rotación o insuficiencia de personal
			Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
			Acciones contrarias a las leyes o acuerdos contractuales
			Falta de capacitación y otros temas relacionados con el personal

Transacción u Operación (aplica para LA/FT/FP	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.		Contrapartes de la entidad (naturales o jurídicas)
			Productos (bienes o servicios) que oferta/requiere
			Canales utilizados para la operación
			Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.		Fraude Interno
			Soborno
			Gestión inadecuada de conflicto de Intereses
			Corrupción

Factor	Definición		Descriptores
			Hurto activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de sistemas de información y aplicaciones
			Caída de redes
			Errores en hardware o software
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.		Fraude Externo

Factor	Definición		Descriptores
			Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

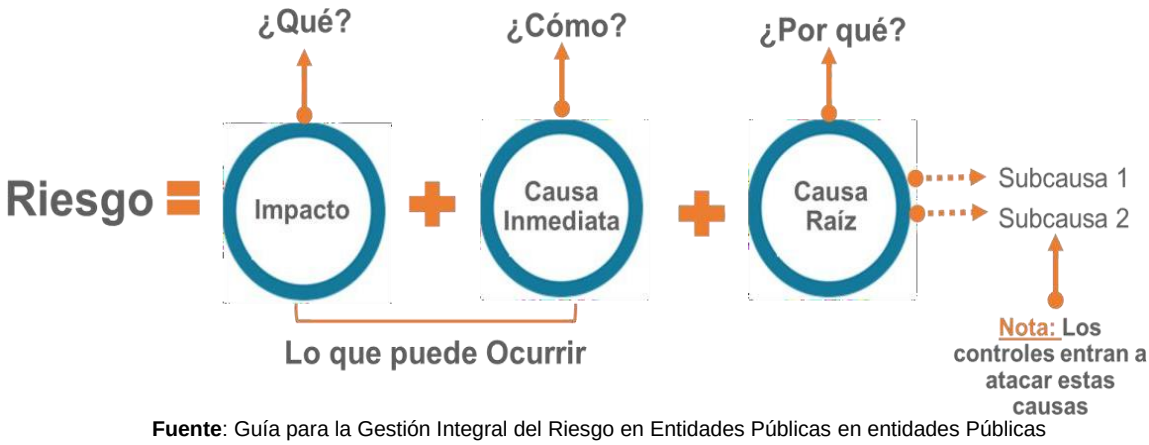
Fuente: Guía para la

9.1.2. Descripción del Riesgo

La descripción del riesgo se realiza a partir de los documentos que establecen el direccionamiento estratégico de la entidad Aguas del Cesar S.A. E.S.P, identificando aquellos eventos o situaciones que puedan afectar el normal desarrollo de los objetivos estratégicos o de los procesos institucionales.

Cada riesgo debe ser descrito de manera completa, clara y comprensible, de tal forma que permita su entendimiento tanto por los líderes de proceso como por personas ajenas al mismo, garantizando la consistencia en su análisis y gestión. La redacción debe iniciar con la frase: “POSIBILIDAD DE”, seguida de la situación o evento que podría impactar la entidad, permitiendo estandarizar la información y facilitar su priorización y seguimiento.

Figura 2 Estructura para redacción del Riesgo



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Públicas Versión 7 de 2025

- ✓ **Impacto:** las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) 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:** Se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles en el paso 3 de diseño y análisis de controles. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

9.1.3. Valoración del Riesgo

9.1.3.1. Análisis del Riesgo inherente

Esta etapa tiene como objetivo establecer la probabilidad de ocurrencia del riesgo, es decir la exposición que tiene la entidad frente al riesgo y el impacto o consecuencias que se pueden generar, con el fin de determinar la zona de severidad del riesgo inherente, así mismo se diseñarán y analizarán la efectividad de los controles.

9.1.3.1.1. Determinar la Probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, 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.

Se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo? Está asociada a la exposición al riesgo del proceso o actividad que se está analizando. Lo anterior, permite determinar con total claridad la frecuencia con la cual se lleva a cabo una actividad y no 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 la entidad.

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	Muy 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

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

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 figura 3 se establecen los criterios y rangos para definir el nivel de probabilidad, los cuales son adoptados de la tabla sugerida por el Departamento Administrativo de la Función Pública.

Figura 3 Criterios para definir el nivel de probabilidad

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

Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicas Versión 7 de 2025

9.1.3.1.2. Determinación del Impacto

Son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en versiones anteriores de la guía 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 hace necesario agruparlos en impacto económico y reputacional, con el fin de facilitar el análisis y evitar la subjetividad en los análisis por parte de los líderes internos.

Figura 4 Criterio para definir Nivel de Impacto

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicas Versión 7 de 2025

Cuando se presenten ambos impactos para un riesgo, tanto económico como

reputacional, los cuales tienen diferentes niveles, se debe tomar el más alto

9.1.4. Análisis de severidad

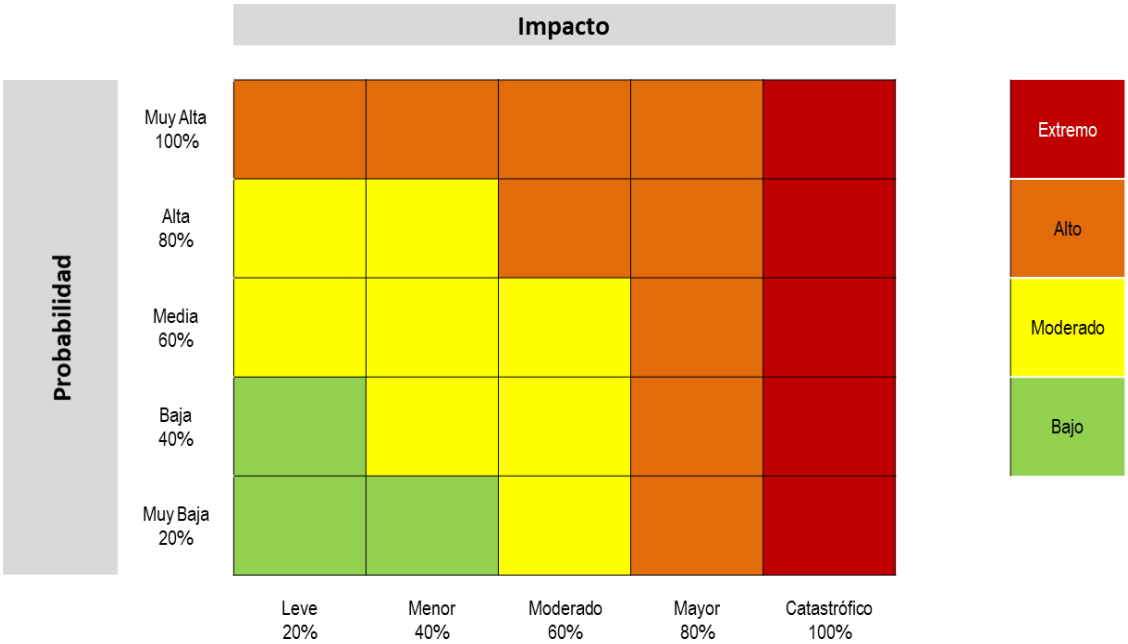
Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor

9.1.4.1. Análisis Preliminar (Riesgo Inherente)

En esta fase, una vez que el riesgo ha sido identificado y descrito, se procede a evaluar sus características mediante el análisis de dos variables fundamentales: la probabilidad de ocurrencia y el impacto potencial. A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar el nivel de RIESGO INHERENTE.

Para la determinación del nivel de severidad del riesgo inherente, se definen cuatro (4) zonas de severidad como se observa en la matriz de calor que se presenta a continuación

Figura 5 Matriz de Calor (Niveles de severidad del Riesgo)



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicas Versión 7 de 2025

9.1.4.2. Diseño y análisis de los Controles

Las actividades de control son acciones concretas y con unos atributos específicos que son establecidas a través de políticas, procedimientos u otras directrices o documentos institucionales e implementados con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos. Para la identificación o bien el diseño de controles se debe tener en cuenta que:

Estas se pueden diseñar y establecer para cada riesgo a través de diferentes mecanismos, bien sea a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos que el líder del proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo.

Se requiere considerar los diferentes atributos de las actividades de control para asegurar aspectos tales como: los responsables de su ejecución, la segregación de funciones y niveles de autoridad apropiados.

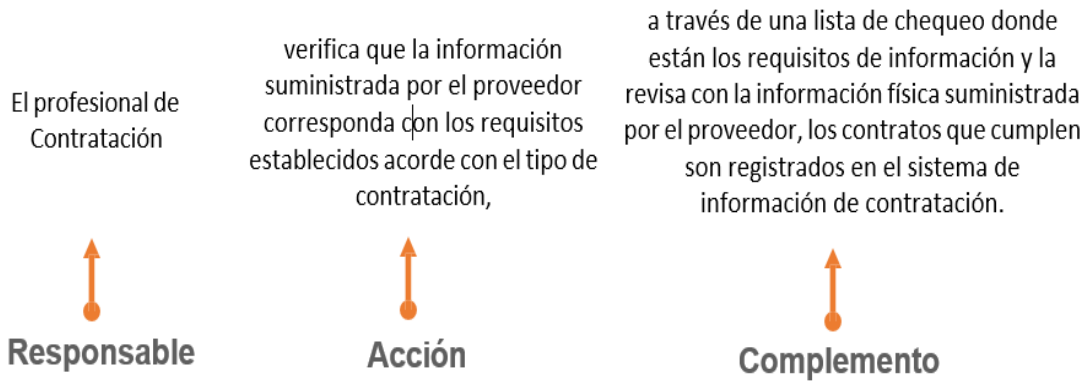
9.1.4.2.1. Estructura para la descripción del control

Para una adecuada redacción del control se propone una estructura que facilitara 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 se ser 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 al responsable implementar el control, tal como ha sido establecido o diseñado.

Figura 6 Ejemplo aplicado bajo la estructura propuesta para la redacción del control



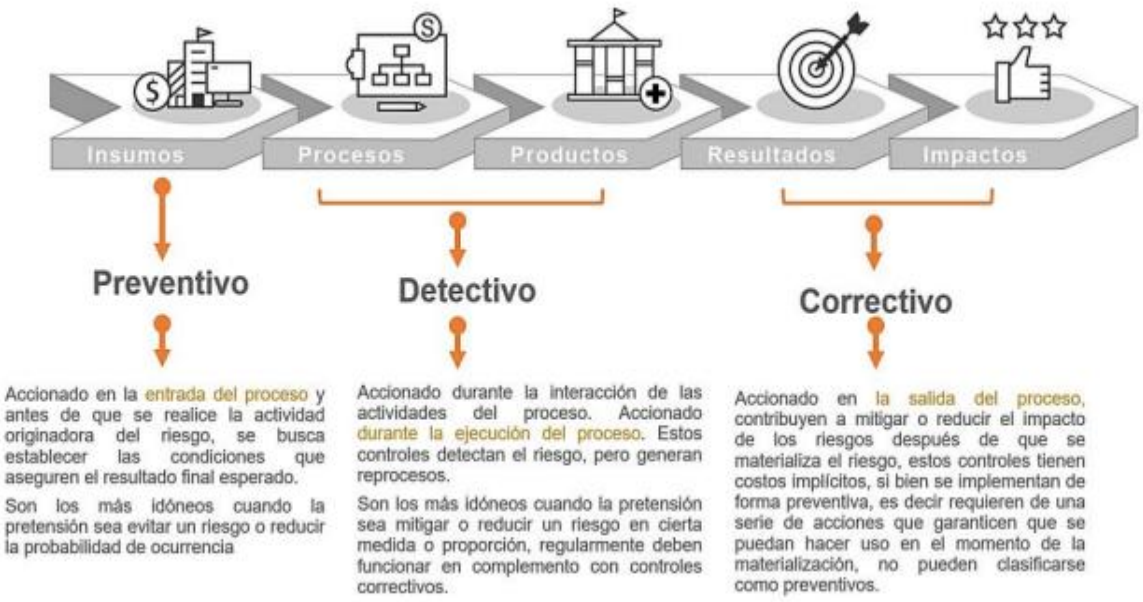
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Públicas Versión 7 de 2025

9.1.4.2.2. Tipología de controles y los procesos:

Se tendrá una tipología de controles a través del ciclo de procesos que permitirá saber cuándo se debe activar el control. Los controles pueden ser preventivos, detectivos o correctivos.

Figura 7 Ciclo del proceso y Tipologías de controles

Figura 20 Cadena de valor del proceso y las tipologías de controles



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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicas Versión 7 de 2025

De acuerdo con estos tenemos las siguientes tipologías de Controles:

Control preventivo: 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: accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control correctivo: accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Se debe tener en cuenta que los controles que se contemplan en esta tipología usualmente tienen que ver con pólizas de seguro, copias de seguridad (backup), bancos de datos u otros mecanismos que permiten

enfrentar el riesgo una vez materializado, los cuales se implementan de forma preventiva, es decir requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización pero no pueden clasificarse como preventivos, ya que sería una sobrevaloración de control que podría generar análisis errados en los niveles de severidad.

En consecuencia, si bien estos controles requieren en su diseño que se apliquen actividades con un enfoque preventivo, al ser activados al momento de materialización del riesgo deben ser considerados como controles correctivos no preventivos. Así mismo, de acuerdo con la forma como se ejecutan tenemos:

Control manual: ejecutados por personas.
Control automático: ejecutados por un sistema o software previamente programado o diseñado

9.1.4.2.3. Valoración de los controles

La Alcaldía Municipal de Dibulla establece los controles considerando tres aspectos clave: la estructura para su descripción, la tipología del control y la forma en que este es implementado.

Es fundamental tener en cuenta que los controles **preventivos** y **detectivos** contribuyen principalmente a la reducción de la **probabilidad de ocurrencia** del riesgo, mientras que los **correctivos** suelen estar orientados a la mitigación del **impacto** una vez materializado el evento

Por tal razón, es indispensable evaluar qué tipo de controles deben ser definidos o fortalecidos para mitigar adecuadamente los riesgos identificados dentro de los procesos de la entidad**.**

Adicionalmente, debe aclararse que, según su **tipología** (preventivo, detectivo o correctivo) y su **modo de implementación** (manual o automático), a cada control se le asigna un **peso porcentual**. Este peso es un insumo fundamental para realizar la **valoración del riesgo inherente.**

A continuación, se establecen los criterios para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización es de aclarar que mínimo se deben garantizar la tipología y la implementación del control para conocer la eficiencia de este y

los otros atributos se determinan bajo el criterio del líder del proceso de manera informativa.

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:

Tabla 4. Atributos 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 intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano	15%

Características de eficiencia	Descripción

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 Siempre que se ejecuta la actividad	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.
		Periódicamente (diario, mensual, bimestral, trimestral, semestral).	El control se aplica aleatoriamente a la actividad que conlleva el riesgo
	Evidencia (Trazabilidad de la ejecución)	Con registro manual	El control deja un registro permite evidencia la ejecución del control.
		Con registro electrónico	Se deja evidencia o rastro de la ejecución del control.
	Ejecución (Fuentes de información internas o externas)	Interna	formatos o registros internos formales.
		Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
		Mixta	Combinación de datos de fuentes internas y externas formales

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicas

9.1.4.3. Valoración del 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 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.

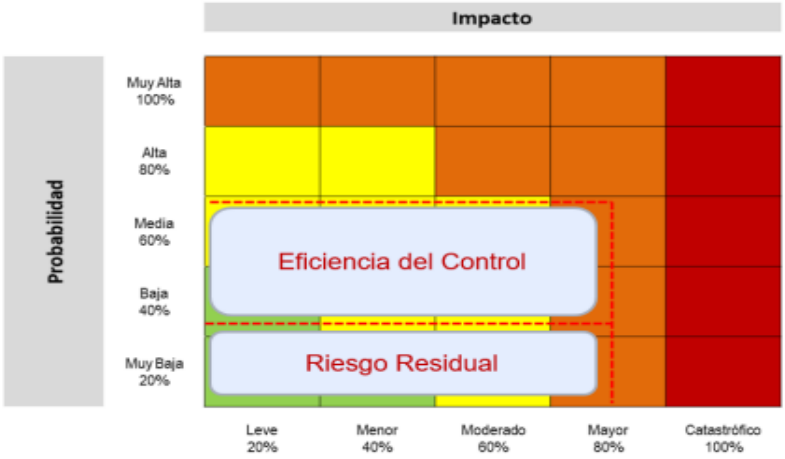
En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

Tabla 8 Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
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 2º control				36%
	Valoración control 2 detectivo			30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual				**25,2%**
	Valoración de Impacto				
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual				**80%**

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

Figura 22 Movimiento en la matriz de calor con el ejemplo propuesto



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

9.1.5. Consolidación Mapa de Riesgos Integral:

Una vez aplicada la totalidad de la metodología explicada se procede con la elaboración de los mapas de riesgo por proceso, cuya estructura puede corresponder a una matriz en formato Excel o bien para aquellas entidades con mayor nivel de complejidad y capacidad institucional puede tener un desarrollo a través de software especializados, los cuales en todo caso deben mantener la misma línea del esquema metodológico propuesto.

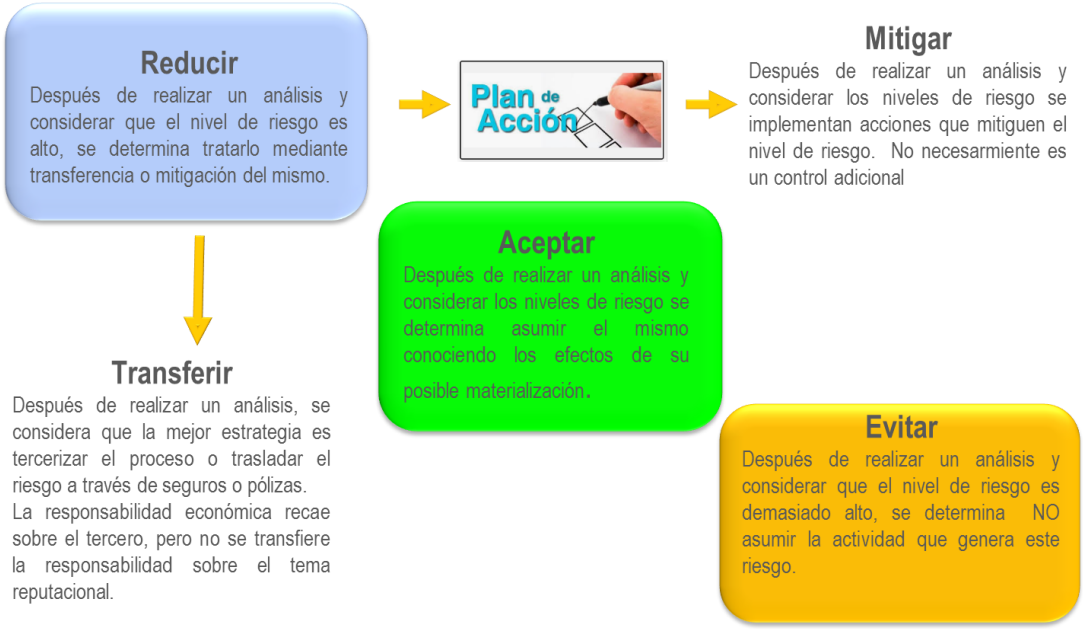
9.2. ESTRATEGIAS PARA COMBATIR EL RIESGO

Las estrategias para enfrentar un riesgo identificado se basan en tres posibles decisiones: **aceptarlo**, **reducirlo** o **evitarlo**. La elección de una de estas alternativas depende del nivel de riesgo evaluado. Para los procesos en funcionamiento, dicha evaluación se realiza sobre el riesgo residual; en el caso de procesos nuevos, se analiza a partir del riesgo inherente.

Cada estrategia seleccionada debe estar respaldada por un **plan de acción específico**, el cual debe ser incorporado en el **mapa de riesgos** correspondiente. Este plan de acción permite gestionar adecuadamente el riesgo, garantizando su seguimiento

y control, y asegurando la trazabilidad de las decisiones tomadas:

Figura 8 Estrategia para combatir el Riesgo



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

9.3. HERRAMIENTAS PARA LA GESTION DEL RIESGO

La entidad Aguas del Cesar S.A. E.S.P. Adopta el mapa de riesgos como herramienta principal para la identificación, valoración, tratamiento y seguimiento de los riesgos.

Toda la información necesaria para el análisis y seguimiento de los riesgos es suministrada a través de esta herramienta. En este marco, la Oficina de Planeación cumple un rol fundamental al asesorar y socializar la metodología adoptada, además de realizar el seguimiento **al cumplimiento de los lineamientos establecidos en esta política.**

Asimismo, la Oficina de Planeación revisa periódicamente el estado de los riesgos y las acciones definidas para su tratamiento, de acuerdo con la severidad del riesgo y la periodicidad establecida para su monitoreo.

9.4. MONITOREO Y REVISION

El monitoreo y la revisión del riesgo se fundamentan en el Modelo Integrado de Planeación y Gestión (MIPG), específicamente en su dimensión 7, la cual incorpora el Modelo Estándar de Control Interno (MECI). Este modelo, junto con el enfoque de las líneas de defensa, actúa como eje articulador para definir y distribuir las responsabilidades relacionadas con la gestión del riesgo y el control interno.

Estas responsabilidades no recaen en una única dependencia, sino que están **distribuidas entre diferentes servidores de la entidad**, según su rol dentro de la estructura organizacional, garantizando así un enfoque integral y coordinado para la administración del riesgo.

Los monitoreos le corresponden a: la línea estratégica, primera y segunda línea de defensa y se desarrollarán de la siguiente manera**:**

Línea estratégica: el comité de Coordinación de Control Interno realizará monitoreo cada semestre, para verificar el cumplimiento de la política de administración de riesgos. Estos se reportarán a través de los (formatos, herramientas y/o instrumentos que los responsables determinen).

Primera línea de defensa: Realiza monitoreo cuatrimestral a las acciones tendientes a controlar y gestionar los riesgos y enviará a la Oficina de Planeación los resultados de esos monitoreo los 5 primeros días hábiles siguientes al cierre del periodo antes descrito. Estos se reportarán a través de los (formatos, herramientas y/o instrumentos que los responsables determinen).

Para los riesgos del proceso de contratación, la primera línea de defensa debe realizar un monitoreo constante dado que las circunstancias cambian rápidamente y los riesgos no son estáticos. La matriz y el plan de tratamiento deben ser revisadas constantemente y, si es necesario, hacer ajustes al plan de tratamiento de acuerdo con las circunstancias.

Sumado a lo anterior, la primera línea de defensa debe monitorear los riesgos y revisar la efectividad y el desempeño de las herramientas implementadas para su gestión. Para lo cual, debe:

- ✓ Asignar responsables
- ✓ Fijar fechas de inicio y terminación de las actividades requeridas
- ✓ Señalar la forma de seguimiento (encuestas, muestreos aleatorios de calidad, u otros)
- ✓ Definir la periodicidad de revisión
- ✓ Documentar las actividades de monitoreo

Segunda línea de defensa: Realizará monitoreo cuatrimestral a través de los informes que los líderes de procesos remitan, asegurando que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados, se ejerzan por el responsable apropiadamente y funcionen como se pretende. Estos se reportarán a través de los (formatos, herramientas y/o instrumentos que los responsables determinen).

10. GESTION PREVENTIVA DEL RIESGO FISCAL

10.1. Control Fiscal Interno y Prevención del Riesgo Fiscal.

Tiene como finalidad orientar el análisis de la operación de las entidades públicas para identificar y gestionar los riesgos que puedan provocar un daño patrimonial al Estado, el cual en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado. Para ello, es necesario partir del concepto de gestión fiscal.

Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000. Para tener claro el ámbito normativo y jurídico, es necesario precisar que sus bases están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, los cuales fueron modificados por el Acto Legislativo 04 de 2019 que se fundamentó en la necesidad de un ejercicio preventivo del control fiscal, que detuviera el daño fiscal e identificara riesgos fiscales; de esta manera, la administración y el gestor fiscal podrían adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública.

¿Qué es?	¿Quién la realiza?	¿Qué comprende?	¿Para qué?
El conjunto de actividades económicas, jurídicas y tecnológicas	Los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos	La adecuada y correcta • adquisición • planeación • conservación • administración • custodia • explotación • enajenación • consumo • adjudicación • gasto • inversión • disposición (de los bienes públicos) • recaudación • manejo • inversión (de sus rentas)	En orden a cumplir los fines esenciales del Estado, con sujeción a los principios establecidos en artículo 3 de la Ley 610 de 2000

Fuente: Elaboración Dirección de Gestión y Desempeño. 2025. Con base en Ley 610/2000 art. 3.

A partir de lo anterior el control fiscal además de posterior y selectivo a través de las auditorias, es preventivo y concomitante, buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, con lo cual surgen conceptos clave como:

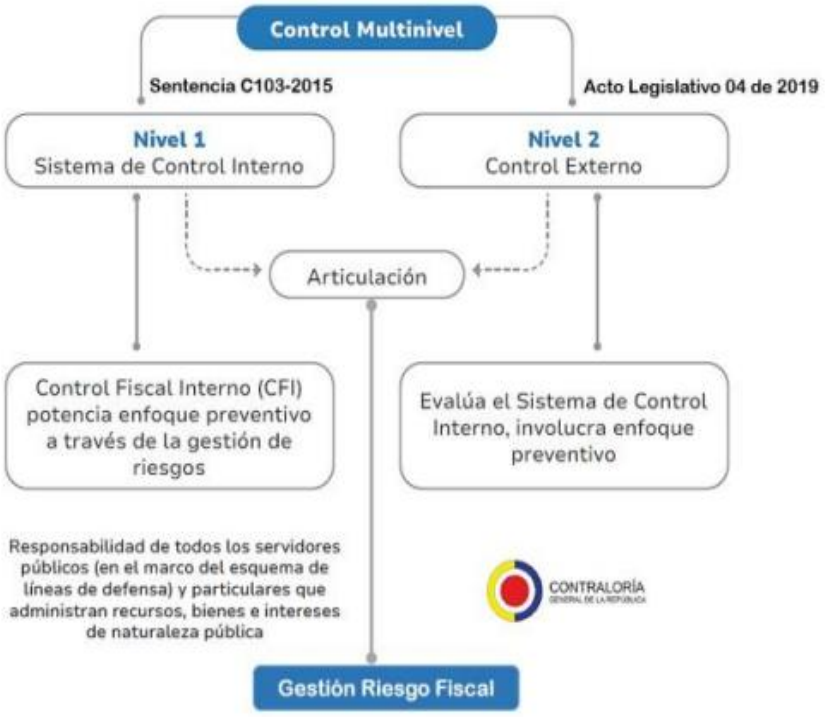
Control fiscal Multinivel: Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

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.

La figura 7 muestra este despliegue y sus elementos de articulación que sustentan el desarrollo del presente capítulo.

Figura 9 Articulación modelo constitucional control fiscal y sistema de control interno



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

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.

La metodología que se propone es de gran utilidad para 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.

10.2. Definición y Elementos del Riesgo Fiscal.

Teniendo en cuenta la estructura y los elementos que conforman la definición de riesgos en la presente política —en armonía con lo establecido en la norma ISO 31000, se define el riesgo fiscal de la siguiente manera:

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:

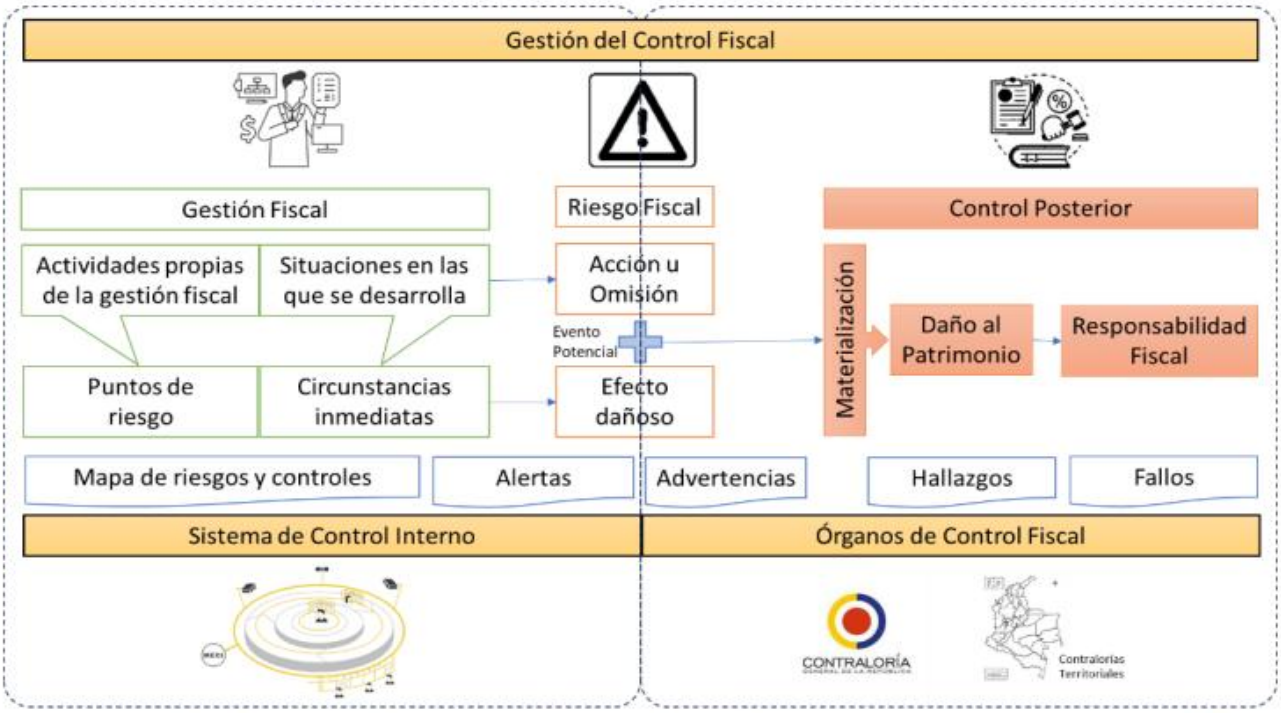
Efecto. es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

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 intereses patrimoniales de naturaleza pública. En esta guía, 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.



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

10.3. Metodología y paso a paso para el levantamiento del mapa de Riesgos Fiscales

A continuación, se describe el procedimiento para llevar a cabo de manera adecuada la identificación, clasificación, valoración y control del riesgo fiscal. Este proceso es fundamental tanto para el logro de los objetivos de gestión de cada entidad como para garantizar la seguridad y prevenir responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre

otros).

Paso 1 identificación de riesgos fiscales

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: actividades que representen gestión fiscal.

Figura 25 Pasos para la identificación del riesgo fiscal

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

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

Para identificar los puntos de riesgo y las circunstancias inmediatas, se realizará un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor**.** Para este taller, puede usar las siguientes preguntas orientadoras:

Tabla 5 Preguntas orientadoras para puntos riesgo f iscal y causas inmediatas

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza 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 Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno-SACI-
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los último 3 años?
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas"

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

Identificación de áreas de impacto

En el contexto del riesgo fiscal, el área de impacto se refiere siempre a una consecuencia de carácter económico que afecta al patrimonio público.

Esto implica que, en caso de materializarse el riesgo, la Alcaldía Municipal de Dibulla estaría expuesta a una pérdida o afectación directa sobre sus recursos financieros o bienes, comprometiendo así su sostenibilidad, eficiencia y responsabilidad en el uso de los recursos público.

Es importante tener en cuenta que no todos los efectos económicos constituyen riesgos fiscales; sin embargo, todo riesgo fiscal implica necesariamente un efecto económico.
Esto se debe a que el riesgo fiscal se define como aquel que conlleva un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Por lo tanto, mientras pueden existir efectos económicos derivados de riesgos operativos,

reputacionales u otros que no comprometan directamente el patrimonio público, **todo riesgo fiscal representa una amenaza directa al patrimonio económico de la entidad.**

Son ejemplos de efectos económicos que no constituyen 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).

Identificación de la Causa Raíz o Potencia 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.

La Causa raíz o potencial hecho generador y el efecto dañoso (daño) mantienen entre sí una relación directa de causa y efecto**.** En este sentido, la identificación de la **causa raíz** o del **potencial hecho generador** del riesgo fiscal se logra a través del análisis de la **acción, omisión o acto que pueda lesionar el patrimonio estatal.**

Una adecuada gestión de riesgos fiscales exige que la identificación de las causas sea objetiva, rigurosa y fundamentada**.** Esto se debe a que los **controles que se diseñen e implementen deben estar orientados a mitigar o eliminar dichas causas,** ya que son el origen del riesgo fiscal. Solo mediante un análisis preciso de las acciones, omisiones o condiciones que pueden generar un daño patrimonial, es posible estructurar controles efectivos que permitan **prevenir la materialización de daños fiscales** y proteger los recursos públicos.

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).

Descripción del Riesgo Fiscal.

A continuación, se presenta la estructura de redacción de riesgos fiscales, la cual integra los elementos clave previamente descrito. 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.

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

Figura 9 Estructura para la redacción del Riesgo

Figura 26 Descripción riesgo fiscal

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicas Versión 7 de 2025

Ejemplo: Gestión de Recursos.

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

Figura 10 Ejemplo de Para la Reducción del Riesgo

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Públicas - Versión 7 de 2025

Paso 2 Valoración del Riesgo Fiscal

Evaluación del Riesgo.

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 la siguiente tabla definida en el numeral 9.1.3.1.1 de la presente política.

Impacto

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá 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 9.1.3.1.2 de la presente política.

Determinación del Nivel del 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 9.1.4.1 de la presente política

Paso 3 Valoración de los 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 9.1.4.2.2. y tabla definida en el numeral 9.1.4.2.3. de la presente política**.**

Nivel del 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.

11. RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCION

La Alcaldía Municipal de Dibulla, adopta como marco de referencia para la gestión del riesgo de corrupción los lineamientos establecidos en la **versión 4 de la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*(2018)**, expedida por el Departamento Administrativo de la Función Pública. Esta guía continúa vigente y constituye un instrumento técnico clave para la identificación, análisis, evaluación, tratamiento, monitoreo y seguimiento del riesgo de corrupción en las entidades del Estado.

En consecuencia, la formulación del mapa de riesgos de corrupción deberá remitirse a los parámetros establecidos en dicho documento. Con el fin de facilitar su aplicación, a continuación, se transcriben algunas de las pautas más relevantes contenidas en la Guía, las cuales deben ser tenidas en cuenta durante todo el proceso de gestión del riesgo**.**

Adicionalmente, se informa que, de acuerdo con información disponible, la Secretaría de Transparencia se encuentra actualmente analizando la posibilidad de actualizar la metodología para la gestión de riesgos de corrupción. No obstante, hasta tanto se expidan nuevos lineamientos oficiales, se mantiene la aplicación obligatoria de la Guía de 2018**.**

11.1. RIESGO DE CORRUPCION

11.1.1 Definición

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

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

ACCION U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO

El riesgo de la Corrupción Se establece 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 evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, La Administración utilizara de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada

casilla quiere decir que se trata de un riesgo de corrupción

Figura 11 Matriz Definición del Riesgo de Corrupción

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 dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas**Versión 7 de 2025**

Generalidades acerca de los riesgos de corrupción

- ✓ Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal.
- ✓ Se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.
- ✓ Consolidación: la oficina de planeación, quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.
- ✓ Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.
- ✓ Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación.

- ✓ Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.
- ✓ Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- ✓ Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

11.1.2. Valoración del Riesgo

11.2.2.1. Cálculo de la probabilidad e impacto

11.2.2.1.1. Análisis de la probabilidad

Se deberá analizar qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones. o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Criterios para Calificar la Probabilidad:

Figura 11 Criterios para Calificar

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicas

11.2.2.1.2. Análisis del Impacto

Para la Determinación del Impacto La Alcaldía de Dibulla el Impacto lo analizara y calificara a partir de las consecuencias identificadas en la fase de descripción del riesgo-

Criterios para calificar el impacto en riesgos de corrupción

Figura 11 Criterios de Calificación

Fuente**: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 de 2025**

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	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, servicios o 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 UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		**10**	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Nivel de impacto MAYOR

Análisis del riesgo del Impacto de Corrupción.

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

11.2.2.1.3. Valoración de los Controles

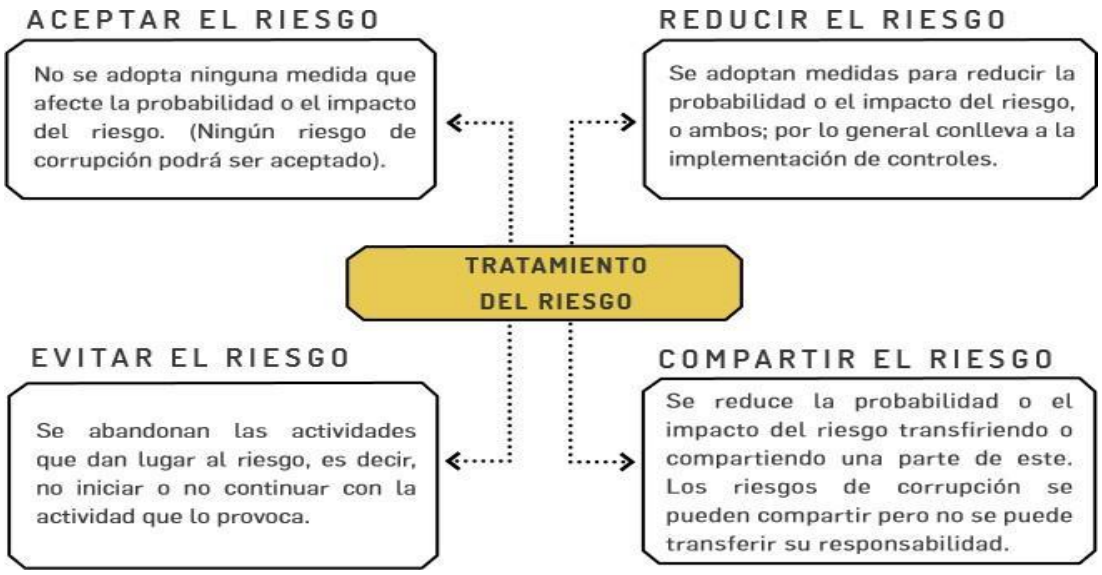
La entidad Aguas del Cesar S.A. E.S.P. tendrá en cuenta para el diseño de controles,

los parámetros señalados en la versión 4 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades públicas, de 2018, continúan vigentes.

Tratamiento del Riesgo.

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

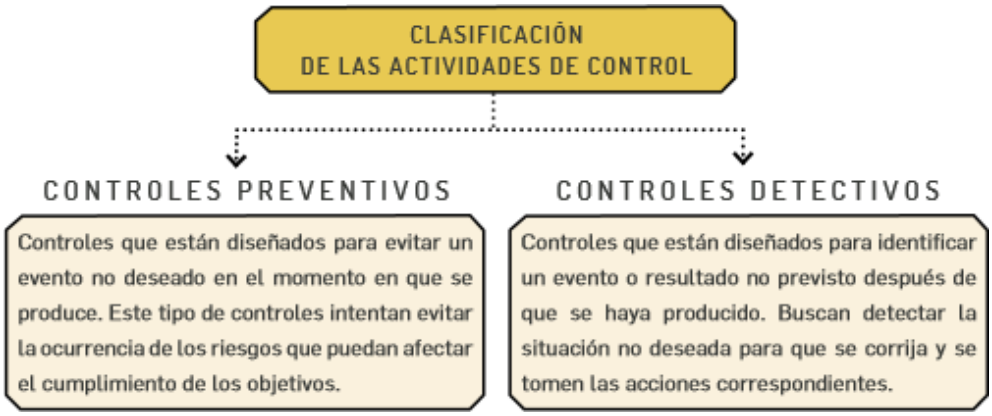
Figura 12 Categorías para tratamiento del Riesgo



Fuente**: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 de 2025**

El tratamiento de control es rol de la primera línea 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.

Figura 13 Clasificación de las Actividades de Control



Fuente**: Guía para la Gestión Integral del Riesgo en Entidades PúblicasVersión 7 de 2025**

Monitorio de Riesgo de Corrupción.

Los gerentes públicos y líderes de proceso, en conjunto con sus equipos de trabajo deben monitorear y revisar periódicamente revisar periódicamente la gestión de riesgos de corrupción y si es el 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. Dicho monitoreo será en los tiempos que determine la entidad.

Reporte de la gestión del riesgo de corrupción

La Alcaldía Municipal de Dibulla deberá reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

Seguimiento de Riesgo de Corrupción

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.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la Página web de la entidad.

Acciones a seguir en caso de materialización del Riesgo de Corrupción

En el evento de materializarse el 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.
- ✓ Llevar a cabo un monitoreo permanente.

La oficina de Control Interno deberá asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- ✓ Determinar la efectividad de los controles
- ✓ Mejorar los controles
- ✓ Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- ✓ Determinar si se adelantaron acciones de monitoreo.

12. RIESGO DE SEGURIDAD DE LA INFORMACION

12.1. Identificación de los Activos de Seguridad de la Información

En primer lugar, se deben identificar los activos de Información7 mediante las actividades descritas en los “Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional” del MSPI, en esta se presenta los lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación y clasificación de activos de información de cada entidad.

Figura 14 Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano,** aumentando así su confianza en el uso del entorno digital.

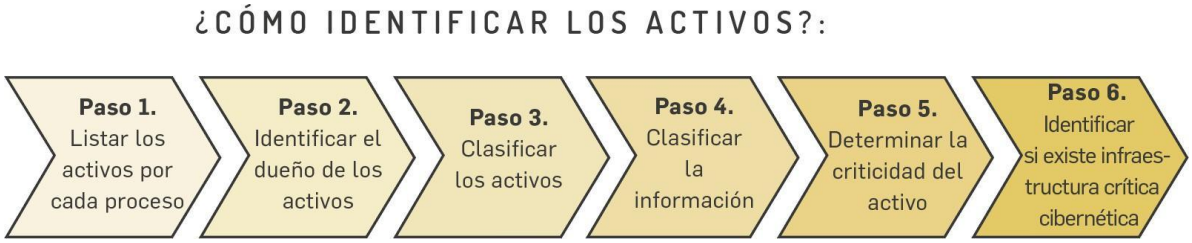
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 de 2025

Pasos para la identificación de los activos:

Como base para la identificación de los riesgos de seguridad de la información se debe tomar el índice de activos de información del proceso.

Para llevar a cabo la identificación de activos, se deberá consultar la sección 3.1.6 del 'Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.

Figura 15 Identificación de Activos de Información



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 de 2025

12.2. Identificación del Riesgo

Posteriormente a la identificación de los activos de la información se deberá o se podrá identificar los riesgos inherentes de seguridad de la información.

Para cada riesgo 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:

- ✓ Pérdida de la confidencialidad
- ✓ Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

Figura 15 Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D

Tabla 22 Tabla de Vulnerabilidades Comunes

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 de 2025

Descripción del Riesgo:
En este campo se describe la situación específica que da como resultado el correspondiente riesgo. “Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.” Si requiere información adicional remitirse al punto 3.4 de esta misma guía.
Clasificación del Riesgo: Este campo corresponde al nombre que identifica a la situación

que podría presentarse, es decir, el posible incidente de seguridad.

12.3. Análisis del Riesgo INHERENTE

La determinación de la probabilidad se debe llevar a cabo de acuerdo con lo establecido en el aparte 9.1.3.1.1. de la presente política, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

Las variables confiabilidad, integridad, y disponibilidad se definirán de acuerdo al modelo de seguridad y privacidad de la información de la estrategia de gobierno digital (GD) del Ministerio de Tecnología de la Información y las Comunicaciones.

A partir de este paso metodológico se incorporan las tablas y matrices establecidas en el numeral 3.5 del capítulo IV que desarrolla los lineamientos para los riesgos generales de la gestión. 5.5 Determinar la probabilidad En esta actividad se debe realizar el análisis de probabilidad de la materialización de estos riesgos.

Frecuencia: Este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.
% Probabilidad Inherente: Este campo corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa.

Probabilidad inherente: Este campo corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa.

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

Determinar el impacto

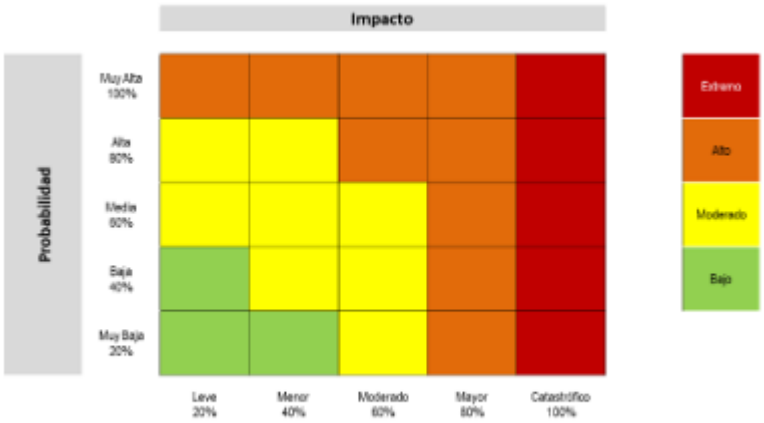
En esta actividad se debe realizar el análisis del impacto de la materialización de estos riesgos

% Impacto Inherente: Este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa

Impacto Inherente: Este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa.

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

Análisis de severidad
Zona de riesgo inherente: En este campo se determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto



12.4. Controles Asociados a la seguridad de la Información

La Administración municipal adoptara para mitigar o tratar los riesgos de seguridad de la información utilizando, como mínimo, los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013. Estos controles están incluidos en el 'Modelo Nacional de

Gestión de Riesgo de Seguridad de la Información en Entidades Públicas', siempre que sean coherentes con los resultados del análisis de riesgo.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información:

Figura 16. Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas -Versión 7 de 2025

"La implementación efectiva de esta política no depende solo de los líderes institucionales, sino del compromiso de cada servidor público y contratista. Trabajar bajo un enfoque basado en riesgos significa anticiparse, actuar con responsabilidad y tomar decisiones informadas que protejan los recursos públicos y fortalezcan la confianza ciudadana."

12.4. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA - SIGRIP

Teniendo en cuenta la expedición de la Ley 2195 de 2022, que hace obligatorio para las entidades públicas la "prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional" (artículo 31), la Secretaría de Transparencia de la Presidencia de la República sugiere a las entidades obligadas a implementar un Programa de Transparencia y Ética Pública contar con un sistema de gestión que le permita prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), de manera integral. Para eso, ha diseñado el Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP.

Integridad pública: Las organizaciones se exponen frecuentemente a que sus objetivos no se cumplan como consecuencia de los diferentes intereses que pueden confluir en la toma de decisiones, en la medida que se privilegian intereses propios sobre el interés general de la organización. En el caso del sector público, el interés general, que no es otra cosa que el interés por la consecución de los fines del Estado, también se puede ver afectado por intereses particulares, lo que termina afectando la capacidad de las entidades públicas para cumplir con las funciones que se le han encomendado.

Amenazas para la integridad pública

La Organización para la Cooperación y el Desarrollo Económico, ODCE, ha planteado la necesidad de aplicar un enfoque basado en riesgos cuando se habla de integridad pública8. Hay varias amenazas que pueden incidir en diferentes puntos de los procesos organizacionales que terminan afectando la capacidad de una entidad para alcanzar sus objetivos, en

particular, asegurar el cumplimiento de la ley. Para el propósito de esta guía, nos centraremos en cinco amenazas para la integridad, que constituyen una lista enunciativa, en la medida que una entidad pública podría identificar adicionales:

Soborno

El Soborno puede ser entendido como "ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]"9. Y opera en dos niveles: Soborno Entrante y Saliente. Se entiende como Entrante el soborno al servidor de la Entidad, y como Saliente el soborno por parte de servidores a otros en nombre de la Entidad.

Fraude

El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.
Este puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima. El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.

Inadecuada gestión del conflicto de intereses:

Un conflicto de intereses surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.

Corrupción

La Corrupción *es "todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero.*

Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral".

Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP

La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la capacidad del Estado para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento.

El SIGRIP busca articular la Política para la Gestión Integral de Riesgos que formule cada entidad, mediante la cual se gestionan los Riesgos Generales de la Gestión, la Gestión Preventiva de Riesgos Fiscales y los Riesgos de Seguridad de la Información, con los demás elementos que son necesarios para gestionar los riesgos para la integridad pública, que se describen a continuación. Al final, un riesgo de gestión, un riesgo fiscal o un riesgo de seguridad de la información puede tener como causa el soborno, el fraude, un conflicto de intereses gestionado inadecuadamente o la corrupción. Además, puede también favorecer el lavado de activos, la financiación del terrorismo o la financiación de la proliferación de armas de destrucción masiva. Por esta razón, es necesario abordar los riesgos para la integridad pública de forma integral y en estrecha articulación con la gestión institucional del riesgo.

El SIGRIP, además, permite a las entidades dar cumplimiento a los lineamientos establecidos para la gestión de riesgos en los Programas de Transparencia y Ética Pública, según lo dispuesto por la Secretaría de Transparencia de la Presidencia de la República. En la medida que se implemente plenamente el Sistema, la entidad estará acreditando la gestión de riesgos para la integridad pública, de riesgos LA/FT/FP, canales de denuncia y debida

diligencia.

Contexto de la organización

Según lo establecido en esta Guía, las entidades en el marco de la formulación de la Política para la Gestión Integral de Riesgos deberán realizar un análisis del contexto interno y externo.

Para efectos del SIGRIP, ese contexto debe complementarse con los siguientes análisis:

- La planta y estructura de la entidad, así como la delegación de autoridad o poder decisorio discrecional dentro de la organización.
- Los grupos de valor o partes interesadas, incluidos los clientes internos y externos.
- Si la entidad está desconcentrada en el país, identificar los lugares en qué opera
- La naturaleza, escala y complejidad de los procesos, servicios, trámites u otras operaciones administrativas de la organización.
- Información general sobre los contratos y principales proveedores de la entidad.
- Las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización.
- La naturaleza y alcance de las interacciones con entidades de otras Ramas del Poder Público, órganos de control o independientes.
- Las obligaciones generales de la entidad, con independencia de la fuente: legal, reglamentaria, contractual, extracontractual u obligaciones profesionales.

Liderazgo del Sistema

Según lo establecido en esta Guía, las entidades en el marco de la formulación de la Política para la Gestión Integral de Riesgos deberán asignar unos niveles de responsabilidad

Tabla 31 Roles y responsabilidades SIGRIP

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	Auditor del Programa	Administrador del Programa	Ejecutores del Programa
Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno	Oficina de Control Interno, Auditoría Interno o quien haga sus veces	Dependencia o persona designada por la Alta Dirección	Directivos, líderes de proceso, servidores y colaboradores
Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.	En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP asume la función de cumplimiento que se desarrolla en el numeral 6.3.7.3	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Planificación

Según lo establecido en esta Guía, las entidades en el marco de la formulación de la Política para la Gestión Integral de Riesgos deberán definir un objetivo y un alcance, así como establecer marco de apetito del riesgo, y el esquema metodológico que aplicarán para lo cual deberán contemplar los siguientes aspectos relevantes del SIGRIP:

Se debe asegurar que dentro del objetivo se contemple la protección de la integridad pública, el alcance de la Política debe contemplar los aspectos relevantes de la organización que se hayan identificado del análisis del contexto interno y externo.

Para el diseño del esquema metodológico, tener en cuenta los lineamientos desplegados a detalle:

Apoyo

Para que el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP pueda operar adecuadamente, la entidad debe disponer de los recursos necesarios, señalar claramente los atributos comportamentales que se requieren, disponer de una estrategia de formación y de comunicación, y documentar cada una de las actividades que se ejecuten; para lo cual:

La entidad debe identificar los recursos financieros y humanos, soluciones de TI, habilidades especializadas, infraestructura organizacional, material de referencia y experiencia que dispone.

Establecer en la Política para la Gestión Integral de Riesgos las características que debe cumplir las personas que realicen un trabajo que afecte el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, su desempeño y operaciones.

La entidad debe asegurar la toma de conciencia del personal, los líderes, el administrador, la Alta Dirección y, en general, de toda la organización, sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.
La toma de conciencia sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, también implica comunicar interna y externamente los resultados de su operación, así como cualquier actualización del Sistema o de algunos de sus elementos. Cada uno de los elementos del Sistema debe estar correctamente documentado.

Operación

Como se indició previamente, el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP es un conjunto de elementos que operan e interactúan entre sí. El principal elemento del Sistema es la Política para la Gestión Integral de Riesgos, que cada entidad debe formular, junto con su respectivo mapa de riesgos.

Figura 28 Sistema de Gestión de Riesgos para la Integridad Pública

Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos

En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, las entidades deberán identificar y valorar los riesgos que pueden impactar el ejercicio íntegro de la función pública, incluidos los riesgos de LA/FT/FP. La Corrupción es la principal amenaza para la integridad, sin embargo, hay manifestaciones muy específicas de esta práctica que requieren ser identificadas y valoradas individualmente, como lo es el soborno, el fraude y la inadecuada gestión del conflicto de intereses. También, los riesgos por conductas que permiten o favorecen el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva, deben ser gestionados.

Paso 1: Identificación y descripción del riesgo

1. Respecto de la “Identificación de los puntos de riesgo” En el marco de la gestión del riesgo de LA/FT/FP, debe tenerse en cuenta que los puntos de riesgo se refieren a operaciones que lleva a cabo la entidad. Estas operaciones son los puntos de riesgo relevantes, que deben tenerse en cuenta para la identificación del riesgo de lavado de activos, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.

Respecto del riesgo de Corrupción y sus manifestaciones específicas como soborno, fraude e inadecuada gestión del conflicto de intereses, los puntos de riesgos pueden ser cualquier actividad dentro del flujo de proceso y no solo las operaciones.

Respecto de la “Identificación de áreas de impacto” En el marco de la gestión de los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

Respecto de la “Identificación de factores de riesgo” Como factores del riesgo LA/FT/FP se tiene a las contrapartes, los productos, los canales y las jurisdicciones, aspectos mínimos a contemplar en cualquier análisis, los cuales en conjunto conforman el concepto de “transacción” u “operación”, en el entendido que una transacción, en todos los casos, será realizada por un cliente o usuario, que accedió o entregó un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica. Estos factores deben permitirle a la entidad mayor efectividad en el conocimiento de las contrapartes, el diseño y aplicación de señales de alerta, la identificación de operaciones inusuales y la determinación y el reporte de operaciones sospechosas.

Respecto de la “Descripción del riesgo” La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en el numeral 3.4 de esta Guía. Todos iniciarán con la formula “Posibilidad de”, y deben señalar el impacto, la causa inmediata y la causa raíz.

En el caso particular del riesgo LA/FT/FP, debe hacerse referencia particularmente a las actividades del flujo de procesos en que existe la vulnerabilidad o exposición al riesgo.

Tabla 33 Análisis riesgos LA/FT/FP

Impacto	Causa Inmediata	Causa Raíz
Económico, Reputacional, Legal, Operativo o de Contagio	Usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva	Descripción de la Operación o Transacción

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Impacto	Causa inmediata		Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar [...]".	
	Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una	

Impacto	Causa inmediata		Causa raíz
		persona actúe o se abstenga de actuar […]".	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Paso 2: Análisis de Riesgo Inherente

Respecto del "Análisis de Riesgo Inherente" Por la naturaleza de los riesgos para la integridad pública, el objetivo fundamental es prevenirlos, detectarlos y reportarlos en términos de oportunidad y eficacia. Esta perspectiva debe ser transversal al análisis del riesgo y al diseño de controles.

Paso 3: Diseño y Análisis de Controles

Respecto del "Diseño y análisis de controles" Para el diseño de controles deberá tenerse en cuenta que, además de la Política para la Gestión Integral de Riesgos y su respectivo Mapa de Riesgos, las entidades deberán desarrollar, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, un Manual para el desarrollo del principio de debida diligencia, contar con una función de cumplimiento y formular una serie de herramientas de gestión.

Paso 4: Valoración de Riesgo Residual
Respecto de la "Valoración del riesgo residual" Sobre este punto referirse completamente

Debida diligencia en el conocimiento de las contrapartes Las entidades deben contar con lineamientos y procedimientos internos sobre la debida diligencia con que deben llevar a cabo el conocimiento de sus contrapartes.

De acuerdo con lo anterior, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, cada entidad deberá contar con un Manual que incorpore mecanismos que desarrollen el principio de debida diligencia en todas las interacciones con contrapartes, en las que exista una exposición a riesgos para la integridad pública, es decir, en aquellas interacciones en que se haya identificado un riesgo de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.

Herramientas de gestión del riesgo

Además de contar con una Política para la Gestión Integral de Riesgos, un Mapa de Riesgos, un Manual de Debida Diligencia en el Conocimiento de las Contrapartes y una función de cumplimiento distribuida dentro de la organización, la gestión de riesgos para la integridad pública requiere que la organización implemente una serie de políticas, procedimientos y códigos de conducta, que contribuyen a la integralidad del sistema.

Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP).

La entidad deberá formular una política institucional que, expresamente: manifieste el compromiso de la Alta Dirección con una cultura de prevención y mitigación del LA/FT/FP; prohíba y rechace cualquier practica asociada al LA/FT/FP; obligue a la entidad a cumplir con la normativa ALA/CFT/CFP; obligue a actuar con debida diligencia en el conocimiento de las contrapartes; promocione la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias; informe las consecuencias del incumplimiento de la política.

Política Antisoborno.

La entidad deberá formular una política institucional que, expresamente: manifieste el compromiso de la Alta Dirección con una cultura de prevención y mitigación del soborno; tipifique las prácticas

de soborno; prohíba y rechace cualquier practica asociada al soborno; obligue a la entidad a cumplir con la normativa antisoborno; obligue a actuar con debida diligencia en el conocimiento de las contrapartes; promocione la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias; informe las consecuencias del incumplimiento de la política.

Política Antifraude.

La entidad deberá formular una política institucional que, expresamente: manifieste el compromiso de la Alta Dirección con una cultura de prevención y mitigación del fraude; tipifique las prácticas de fraude; prohíba y rechace cualquier practica asociada al fraude; obligue a la entidad a cumplir con la normativa antifraude; promocione la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias; informe las consecuencias del incumplimiento de la política.

Procedimiento para la gestión de los conflictos de intereses.

La entidad deberá formular un procedimiento interno que, expresamente: contenga un catálogo de situaciones que se podrían presentar dentro de la organización, con ejemplos reales, que generen un conflicto de intereses; el paso a paso que debe seguir cualquier persona para declarar un conflicto de intereses al interior de la organización; el paso a paso que seguirá la entidad para tramitar un conflicto de intereses; el margen de acción de la entidad para gestionar los conflictos de intereses; el paso a paso para realizar las declaraciones periódicas que la ley establezca; el paso a paso para controlar que se hayan realizado las declaraciones periódicas que la ley establece.

Procedimiento para el reporte de operaciones sospechosas.

La entidad deberá formular un procedimiento interno que, expresamente: establezca los criterios y señales de alerta para determinar que una operación es inusual; el paso a paso para que los líderes de proceso reporten a quien ostente la función de cumplimiento las operaciones inusuales; el paso a paso para que quien ostenta la función de cumplimiento evalúe la operación inusual y determine si es sospechosa; el paso a paso para reportar a las autoridades competentes la operación sospechosa, incluso cuando fue intentada.

Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético.

La entidad deberá formular un procedimiento interno que, expresamente: identifique los medios de recepción de denuncias e inquietudes; el paso a paso para evaluar las denuncias e inquietudes que se presenten por el canal; el paso a paso para tratar las denuncias e inquietudes que correspondan a todas las herramientas de gestión deben desarrollarse en los Programas de Transparencia y Ética Pública de las entidades. La Política para la Gestión Integral de Riesgos, el Mapa de Riesgos, y el Manual de Debida Diligencia en el Conocimiento de las Contrapartes, también, hacen parte integral del Programa de Transparencia.

Monitoreo, evaluación, auditoría y mejora

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto permanente de monitoreo, evaluación, auditoría y mejora. Para este propósito, deben tenerse en cuenta las siguientes consideraciones:

- En la Política para la Gestión Integral de Riesgos debe quedar establecido la periodicidad y el contenido del monitoreo a los riesgos que gestiona el SIGRIP.
- Corresponde al Administrador del Programa, desde su rol como segunda línea de defensa, la evaluación de la gestión del riesgo.
- El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto de auditoría, la cual estará a cargo de la unidad de control interno o quien ejerza la tercera línea de defensa.
- Finalmente, la mejora del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP corresponde a la Alta Dirección o línea estratégica, quien lleva a cabo la revisión integral del Sistema

13. Bibliografía

Guía para la Gestión Integral del Riesgo en Entidades Públicas en Entidades Públicas, DAFP, Versión 7, de agosto de 2025 y anexos.

	NOMBRE	CARGO	Versión
Elaboró	JANOS CONSULTORES	Profesionales Asesores	**1**
Revisó y Aprobó	Comité Institucional de Gestión y desempeño		