SOCIEDAD DE ACTIVOS ESPECIALES

Política de Riesgos

Versión No. 04 – 28 de noviembre del 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN 2

2. OBJETIVO 2

3. ÁMBITO DE APLICACIÓN 2

4. GLOSARIO 2

5. CONTEXTO INTERNO Y EXTERNO 5

6. POLÍTICA 5

7. PRINCIPIOS ORIENTADORES DE LA GESTIÓN INTEGRAL DEL RIESGO 6

8. LÍNEAS DE DEFENSA Y NIVELES DE RESPONSABILIDAD FRENTE A LA GESTIÓN DE RIESGOS 7

9. VALORACIÓN DEL RIESGO 9

9.1 Criterios para definir el nivel de probabilidad 9

9.2 Criterios para definir el nivel de impacto 10

9.3 Lineamientos para los riesgos fiscales 10

9.3.1 Definición y elementos del riesgo fiscal 10

9.3.2 Valoración del riesgo fiscal 11

9.4 Lineamientos para los riesgos para la integridad pública 11

9.4.1 Valoración de los riesgos para la integridad pública 12

9.5 Lineamientos para los riesgos de seguridad de la información 12

9.5.1 Elementos riesgos seguridad de la información 12

9.5.2 Valoración riesgos seguridad de la información 13

10. NIVELES DE SEVERIDAD DEL RIESGO 14

11. CAPACIDAD, TOLERANCIA Y APETITO DEL RIESGO 14

12. TIPOS DE TRATAMIENTO DE LOS RIESGOS 15

13. ESTRATEGIA DE TRATAMIENTO Y MONITOREO DE LOS RIESGOS 16

14. INDICADORES CLAVE DE RIESGO (KRI) 17

15. EVALUACIÓN ANUAL DEL NIVEL DE MADUREZ DEL SISTEMA INTEGRADO DE GESTIÓN 17

16. AUDITORIA DEL SIGRIP 17

17. ACCIONES POR SEGUIR EN CASO DE MATERIALIZACIÓN DE RIESGOS 18

18. DIVULGACIÓN DE LA POLÍTICA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS 19

19. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA 19

20. CONTROL DE CAMBIOS 20

21. CONTROL DE ÚLTIMA APROBACIÓN 20

1. INTRODUCCIÓN

En cumplimiento con lo establecido por el Departamento Administrativo de la Función Pública (DAFP) en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V7 y el Modelo Integrado de Planeación y Gestión (MIPG), a continuación, se dan a conocer los elementos de la Política Integral para la Administración de Riesgos, como compromiso de la presidencia y del equipo directivo de la Sociedad de Activos Especiales - SAE.

Es importante destacar que esta política utiliza como guía los lineamientos emitidos por el Departamento Administrativo de la Función Pública, (DAFP), Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) y la Secretaría de Transparencia de la Presidencia de la República correspondientes a los riesgos de gestión, seguridad de la información y corrupción respectivamente.

La Política Integral para la Gestión de Riesgos se encuentra alineada con la planificación estratégica de la SAE y se adopta a través de Comité Institucional de Coordinación de Control Interno, para garantizar razonablemente el cumplimiento de la misión y los objetivos institucionales, mediante la gestión eficaz de los riesgos.

Esta política responde al Modelo Integrado de Planeación y Gestión (MIPG) según Decreto 1499 de 2017, dentro de sus políticas de Política de Planeación Institucional, Política de Seguimiento del Desempeño Institucional y la Política de Control Interno, siendo el eje fundamental de análisis el contexto organizacional interno y externo, la planeación institucional, los objetivos institucionales y las políticas sectoriales y específicas que define el Gobierno Nacional y el modelo de operación por procesos.

Por lo anterior, la entidad busca implementar la gestión del riesgo, fomentando una cultura organizacional dirigida a la prevención de eventos potenciales que impidan el cumplimiento y logro de los objetivos institucionales, así como de los procesos, con el propósito de tomar decisiones oportunamente, en pro de la mejora continua.

2. OBJETIVO

Establecer los lineamientos estratégicos y operativos que orienten la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos en la Sociedad de Activos Especiales – SAE que puedan afectar el logro de los objetivos de la entidad, en articulación con el Modelo Integrado de Planeación y Gestión – MIPG y las mejores prácticas internacionales de gestión de riesgos basadas en el marco de Gestión de Riesgos Empresariales (Enterprise Risk Management) desarrollado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO).

3. ÁMBITO DE APLICACIÓN

La presente Política aplica para todos los procesos de la Entidad y/o o actividades tercerizadas que puedan afectar su misionalidad, así como a los servidores y servidoras de la SAE, en todos los niveles jerárquicos y áreas misionales, estratégicas, de apoyo y de seguimiento y evaluación. Incluye la gestión de riesgos en la planeación, ejecución presupuestal, prestación de servicios, adopción de tecnologías, fortalecimiento organizacional, así como en la implementación de proyectos y programas institucionales.

4. GLOSARIO

- **Activo:** Cualquier elemento que tiene valor para la organización, tales como: aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización en ejecución de sus funciones.

- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos,

el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Beneficio:** Impacto positivo generado por el aprovechamiento de una oportunidad y que puede afectar el logro de los resultados previstos.
- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales.

- **Bien de uso público:** aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.

- **Bienes fiscales:** aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

- **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.

- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un 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:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o sub-causas que pueden ser analizadas.

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

- **Control:** Medida que permite reducir o mitigar un riesgo.

- **Evaluación del riesgo:** proceso de comparación de los resultados del análisis del riesgo con los criterios definidos, para determinar si el riesgo, su magnitud o ambos, son aceptables o tolerables al interior de la SAE S.A.S. (adaptado de NTC ISO 31000).

- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.

- **Financiación del terrorismo:** proveer, recolectar, entregar, recibir, administrar, aportar, custodiar o guardar fondos, bienes o recursos, o realizar cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas (Ley 599 de 2000).

- **Gestión de riesgo fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

- **Gestor fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas,

en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)" . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales". A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

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

- **LA/FT/FPADM:** Lavado de activos, Financiación del Terrorismo, Financiación de la Proliferación de Armas de Destrucción Masiva.

- **Matriz de riesgos LA/FT/FPADM:** instrumento que permite a la entidad identificar, individualizar, segmentar, evaluar y controlar los riesgos LA/FT/FPADM a los que se podría ver expuesta la compañía, conforme a los factores de riesgo identificados.

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

- **Patrimonio público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

- **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.

- **Programa de Transparencia y Ética Pública:** es un conjunto de acciones que busca promover la legalidad y la transparencia en la gestión pública, que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

- **Punto de riesgo:** Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.

- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.
  Nota: Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.

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

- **Riesgo fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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

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

- **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).

- **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.

5. CONTEXTO INTERNO Y EXTERNO

La Sociedad de Activos Especiales – SAE realiza de manera anual un análisis de contexto, el cual atiende las orientaciones dadas por el Modelo Integrado de Planeación y Gestión – MIPG, dando relevancia a la identificación de factores de contexto interno y externo que puedan afectar tanto positiva como negativamente a la Entidad.

La construcción de este análisis de contexto toma como insumo el desarrollo de matrices DOFA para la identificación de los aspectos internos y externos que se realizan a través de talleres prácticos de análisis de contexto realizados a nivel nacional, que permiten generar insumos para el establecimiento de los focos e iniciativas estratégicos que se requieren. Es importante resaltar que este ejercicio se sustenta en una construcción colectiva, en la cual las direcciones territoriales y las áreas en la Dirección General desempeñaron un rol relevante.

6. POLÍTICA

La Sociedad de Activos Especiales - SAE conforme a su misión se compromete con sus grupos de valor e interés a identificar a través del análisis de contexto interno y externo los riesgos que impacten el cumplimiento de su misión, visión, objetivos estratégicos, prestación de sus servicios, logro de los objetivos de sus procesos y proyectos estratégicos incluyendo los riesgos para la integridad pública (Fraude interno, Soborno, Conflicto de Interés, Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva) y los riesgos fiscales, estableciendo medidas de control necesarias para prevenir su materialización, mitigar su impacto o aprovechar las oportunidades surgidas del contexto incluyendo los resultados de las evaluaciones llevadas a cabo por los organismos de control, todo lo anterior alineado con los requisitos legales y o normativos aplicables vigentes.

En consecuencia, la Alta Dirección se compromete a:

a. Proporcionar los recursos necesarios para la administración del riesgo.
b. Integrar la gestión de los riesgos a sus procesos para mejorar la toma de decisiones.
c. Fortalecer el enfoque basado en riesgos para la integración de sus Sistemas de Gestión.
d. Definir la responsabilidad diferenciada basada en el modelo de líneas de defensa.
e. Definir el tratamiento a los riesgos y las oportunidades identificadas en el marco de la administración del riesgo.

f. Articular la administración de los riesgos, para que estos sean gestionados de manera unificada durante el proceso de identificación, valoración y tratamiento de los riesgos, según lo define la Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública.
g. Gestionar adecuada y efectivamente los riesgos sobre los activos de información que afectan el cumplimiento de los objetivos estratégicos de la Entidad.
h. Gestionar adecuada y efectivamente los riesgos para la integridad pública (Fraude interno, Soborno, Conflicto de Interés, Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva) que afectan el cumplimiento de los Objetivos Estratégicos de la Entidad.
i. Gestionar adecuada y efectivamente los riesgos fiscales que afectan el cumplimiento de los objetivos estratégicos de la Entidad.
j. Fomentar la cultura del autocontrol a partir del monitoreo y seguimiento periódico de los riesgos.
k. Actualizar la política de riesgos de acuerdo con los cambios en su contexto y/o normativos aplicables.
l. Asegurarse de que se establezcan medidas de intervención (controles correctivos) cuando estas apliquen como planes de continuidad, contingencia u otras acciones que permitan mitigar los impactos derivados de la materialización.
m. Promover el establecimiento de los planes de mejoramiento a partir del monitoreo y seguimiento periódico de los riesgos, para asegurar la eficacia de los controles.
n. Evaluar la necesidad de actualizar la metodología para la administración de los riesgos en la Entidad, por cambios en el contexto que sean pertinentes a la gestión del riesgo y/o normativos aplicables.
o. Asegurar que se comuniquen en la SAE los resultados globales de la gestión del riesgo.
p. Gestionar todo los relacionado con la prevención y resolución de conflicto de intereses de acuerdo con la normatividad vigente y documentos de la entidad.
q. Comunicar a la Dirección de Planeación y Prospectiva los riesgos que sean materializados o que estén en riesgo inminente de materializarse.
r. Dar cumplimiento a las orientaciones, exhortaciones o recomendaciones que indique la Dirección de Planeación y Prospectiva para la buena y adecuada gestión de los riesgos identificados por la Entidad.

7. PRINCIPIOS ORIENTADORES DE LA GESTIÓN INTEGRAL DEL RIESGO

La Sociedad de Activos Especiales S.A.S. (SAE) orienta su gestión integral del riesgo bajo los siguientes principios institucionales:

1. **Responsabilidad y ejemplo de la Alta Dirección:** La Presidencia y la Alta Dirección lideran la cultura de gestión del riesgo, asegurando que las decisiones institucionales consideren la exposición al riesgo.

2. **Integralidad:** La gestión del riesgo se desarrolla de manera transversal, articulando la planeación, operación, control y gobierno.

3. **Proporcionalidad:** Los controles y acciones se definen según la materialidad y criticidad del riesgo.

4. **Prevención y oportunidad:** Prioridad a la anticipación, detección temprana y respuesta ágil frente a posibles eventos.

5. **Transparencia e integridad:** Las actuaciones institucionales se soportan en evidencia verificable, fomentando la confianza pública.

6. **Mejora continua:** Los aprendizajes de eventos y auditorías alimentan la actualización de la metodología, la política y los mapas de riesgo.

7. **Corresponsabilidad:** Cada líder de proceso es responsable de los riesgos bajo su gestión, en coordinación con la Dirección de Planeación y Prospectiva y la Oficina de Control Interno.

8. **Enfoque basado en datos:** La identificación, valoración y monitoreo de riesgos se fundamenta en información oportuna, confiable y trazable.

8. LÍNEAS DE DEFENSA Y NIVELES DE RESPONSABILIDAD FRENTE A LA GESTIÓN DE RIESGOS

De acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión - MIPG y la dimensión siete de Control Interno, a continuación, se relacionan las líneas de defensa con sus correspondientes niveles de responsabilidad y autoridad establecidos para la administración del riesgo, proporcionando el aseguramiento razonable de la gestión para prevenir la materialización de los riesgos.

Tabla 1. Líneas de defensa y niveles de responsabilidad frente a la gestión del riesgo

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDADES FRENTE A LA GESTIÒN DEL RIESGO
LÍNEA ESTRATÉGICA Define el marco general y supervisa su cumplimiento.	Junta Directiva (para aprobación de política y decisiones estratégicas). Comité Institucional de Coordinación de Control Interno (CICCI). Comité Directivo – Comité Institucional de Gestión y Desempeño. Presidencia / Alta Dirección.	Evaluar el estado del Sistema de Control Interno, acorde con la información generada por parte de las instancias de 2da línea identificadas y la actividad de control definida que materializa las líneas de reporte en cada caso, de acuerdo con el tema del cual son responsables, a fin de generar acciones y una toma de decisiones con enfoque preventivo.
1ra LÍNEA DE DEFENSA Gestiona y controla en origen.	Líderes de proceso, planes, programas y proyectos en: Vicepresidencia Operativa, Vicepresidencia de Sociedades, Vicepresidencia de Activos Muebles e Inmuebles, Vicepresidencia Corporativa; Direcciones Territoriales (Caribe, Occidente, Sur, Centro Oriente); Gerencias (Comercialización de Activos Sociales/No Sociales; Auditoría de Sociedades); Direcciones misionales y de apoyo (Asuntos Legales Misionales, Control de Inventario, análisis/Aislamiento/Valoración).	Identificar, analizar, valorar y tratar los riesgos de su ámbito; definir/ejecutar controles; evidenciar seguimiento en el sistema institucional; reportar oportunamente cambios y materializaciones a Planeación y Prospectiva; promover autocontrol y mejora continua.
2da LÍNEA DE DEFENSA Monitorea, consolida y asegura el	Dirección de Planeación y Prospectiva (líder del proceso de riesgos). Oficina de Tecnologías y Sistemas de la Información.	**Planeación y Prospectiva:** Consolidar el Mapa de Riesgos Institucional, priorizar riesgos críticos, emitir alertas y elevarlas a la

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDADES FRENTE A LA GESTIÒN DEL RIESGO
diseño/efectividad de controles.	Dirección de Talento Humano (GIT de Control Disciplinario Interno). Dirección de Contratación. Dirección Administrativa. Dirección Financiera. GIT de Atención y Servicio a la Ciudadanía. Dirección de Asuntos Legales Misionales. Oficina Jurídica. Oficina de Prensa y Comunicaciones (riesgo reputacional, según competencia).	línea estratégica; proponer mejoras y seguimiento integral. **OTI:** Verificar controles de seguridad/ciberseguridad, continuidad, protección de datos y disponibilidad de sistemas (PETI). **Talento Humano**: Monitorear ciclo del servidor, clima, convivencia, integridad y régimen disciplinario; alertar desviaciones. **Contratación:** Seguimiento a riesgos contractuales (retrasos/incumplimientos); alertas y recomendaciones. **Administrativa/Financiera:** Riesgos logísticos/financieros, tesorería y salvaguarda de recursos; alertas y acciones preventivas. **Asuntos Legales Misionales/Servicio al Ciudadano:** Monitoreo PQRD, tutelas, calidad del servicio; generación de alertas. **Jurídica/Asuntos Legales Misionales:** Riesgos litigiosos/regulatorios; conceptos y alertas. **Prensa/Comunicaciones:** Riesgo reputacional (cuando aplique); gestión de mensajes y alertas.
3ra LÍNEA DE DEFENSA Evaluación independiente.	Oficina de Control Interno	Auditorías basadas en riesgos (énfasis fiscal, para la integridad pública, cumplimiento, alto impacto); informes, alertas y recomendaciones; seguimiento a planes de

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDADES FRENTE A LA GESTIÒN DEL RIESGO
		mejoramiento; reporte al CICCI y a la Presidencia.

Fuente: Elaboración propia con base en la Guía para la gestión integral del riesgo en entidades públicas V7

9. VALORACIÓN DEL RIESGO

La evaluación del riesgo inherente y riesgo residual se calcula según los lineamientos descritos en la Guía para la gestión integral del riesgo en entidades públicas V7.

Ilustración 1. Valoración del Riesgo



Fuente: Elaboración propia

9.1 Criterios para definir el nivel de probabilidad

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.**

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad.

En la tabla 2 se establecen los criterios para definir el nivel de impacto.

Tabla 2. Criterios para definir el nivel de probabilidad

Calificación	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 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 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: Departamento Administrativo de la Función Pública DAFP - Guía para la gestión integral del riesgo en entidades públicas V7

9.2 Criterios para definir el nivel de impacto

El impacto se entiende como la consecuencia económica y/o reputacional que se generaría por la materialización del riesgo. Para la definición de la tabla de criterios se definen **impactos económicos y reputacionales** como variables principales.

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

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

En la tabla 3 se establecen los criterios para definir el nivel de impacto.

Tabla 3. Criterios para definir el 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: Departamento Administrativo de la Función Pública DAFP - Guía para la gestión integral del riesgo en entidades públicas V7

9.3 Lineamientos para los riesgos fiscales

9.3.1 Definición y elementos del riesgo fiscal

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

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

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

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

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.

En este documento, 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 (Potencial Daño)

Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño patrimonial; El riesgo fiscal se relaciona con el evento de potencial efecto perjudicial sobre los recursos, bienes o intereses públicos, mientras que el daño patrimonial es la afectación real y concreta a los mismos, como resultado de una acción u omisión.

9.3.2 Valoración del riesgo fiscal

En esta etapa se realiza la evaluación de riesgos que busca establecer el nivel de riesgo inherente, entendido como la probabilidad de ocurrencia del riesgo, así como su impacto en la gestión fiscal.

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.

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 el patrimonio público es relevante, sin embargo, existen niveles para su valoración.

Determinación del nivel de riesgo inherente: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad.

Para la evaluación del riesgo fiscal, se aplicarán las tablas de frecuencia e impacto, así como la matriz de severidad definidas en los numerales 9.1 y 9.2 de la presente política, las cuales pueden adaptarse a las características propias de la entidad sin alterar los criterios de evaluación.

Nivel de riesgo (riesgo residual): Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles, se debe tener en cuenta que, 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.

9.4 Lineamientos para los riesgos para la integridad pública

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, en la medida que la integridad del Estado se ve comprometida cuando sus instituciones se usan para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas.

9.4.1 Valoración de los riesgos para la integridad pública

Por la naturaleza de los riesgos para la integridad pública, el objetivo de la SAE 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.

En esta etapa se realiza la evaluación de riesgos que busca establecer el nivel de riesgo inherente, entendido como la probabilidad de ocurrencia del riesgo, así como su impacto.

Probabilidad: La probabilidad se entiende como la posibilidad de ocurrencia del riesgo para la integridad pública. 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.

Impacto: El impacto se entiende como la consecuencia económica y/o reputacional que se generaría por la materialización del riesgo. Para la definición de la tabla de criterios se definen impactos económicos y reputacionales como variables principales.

Determinación del nivel de riesgo inherente: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad.

Nivel de riesgo (riesgo residual): Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles, se debe tener en cuenta que, 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.

9.5 Lineamientos para los riesgos de seguridad de la información

9.5.1 Elementos riesgos seguridad de la información

La Sociedad de Activos Especiales S.A.S. (SAE) reconoce la importancia de proteger la confidencialidad, integridad y disponibilidad de la información que gestiona en cumplimiento de su misión y objetivos institucionales. Por ello, incorpora la gestión de los riesgos de seguridad de la información dentro del marco de su Sistema de Gestión Integral de Riesgos (SIGRIP), en articulación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo de Gobierno Digital del Estado colombiano.

La Política de Seguridad y Privacidad de la Información de la SAE se encuentra alineada con el Marco de Referencia de Arquitectura Empresarial de TI y con los lineamientos del Departamento Administrativo de la Función Pública (DAFP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), garantizando la coherencia entre los componentes de seguridad, arquitectura y servicios ciudadanos digitales.

En el desarrollo de la gestión de riesgos de seguridad de la información, la SAE aplicará los controles establecidos en el Anexo A de la Norma Técnica ISO/IEC 27001:2022, considerados como buenas prácticas internacionales en materia de ciberseguridad. Estos controles se seleccionarán con base en

los resultados del análisis de riesgos institucional, atendiendo la naturaleza del activo, las amenazas y vulnerabilidades identificadas, y serán documentados, implementados y monitoreados de acuerdo con las necesidades de cada proceso.

El proceso de identificación, valoración y tratamiento de los riesgos de seguridad se documentará en la Matriz de Riesgos de Seguridad de la Información, la cual contendrá, como mínimo, la siguiente información:

- **Proceso:** Dependencia o proceso responsable del activo de información.
- **Referencia:** Código o número identificador del activo.
- **Activo de Información:** Denominación del activo bajo análisis.
- **Tipo de Activo:** Categoría aplicable (información, software, hardware, servicios, intangibles, infraestructura crítica, recursos humanos o instalaciones).
- **Amenazas y Vulnerabilidades:** Factores que pueden afectar la seguridad del activo.
- **Controles Existentes y Propuestos:** Medidas implementadas o por implementar para mitigar el riesgo.
- **Nivel de Riesgo Inherente y Residual:** Resultado de la valoración según las escalas definidas en esta política.

Los resultados del proceso serán consolidados por la Dirección de Planeación y Prospectiva (DPP), en coordinación con la Oficina de Tecnologías y Sistemas de Información, y presentados al Comité Institucional de Coordinación de Control Interno (CICCI) para su análisis, seguimiento y toma de decisiones.

De esta manera, la SAE garantiza una gestión sistemática, documentada y alineada con los estándares nacionales e internacionales de seguridad de la información, fortaleciendo la confianza institucional y la protección de los activos digitales a su cargo.

9.5.2 Valoración riesgos seguridad de la información

A partir de este punto se incorporan las tablas 2 y 3 que desarrollan la manera en la que se evalúa la probabilidad e impacto de cada riesgo.

Probabilidad: En esta actividad se debe realizar el análisis de probabilidad de la materialización de estos riesgos. Se mide la ***frecuencia*** (Este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo), la ***% Probabilidad Inherente*** (corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa) y ***Probabilidad inherente*** (corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa).

Impacto: En esta actividad se debe realizar el análisis del impacto de la materialización de estos riesgos. Se mide el ***% Impacto Inherente*** (corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa y el ***Impacto Inherente*** (corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa).

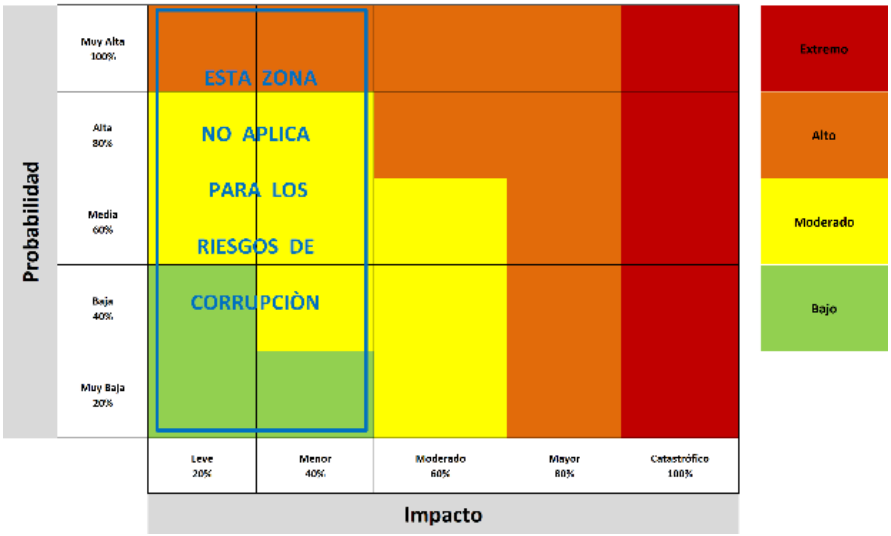
Determinación del nivel de riesgo inherente: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad.

Nivel de riesgo (riesgo residual): En esta etapa se revisa la efectividad de los controles. 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.

10. NIVELES DE SEVERIDAD DEL RIESGO

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial y se definen 4 zonas de severidad en el mapa de calor.

Ilustración 2. Mapa de Calor Niveles de Severidad del Riesgo



Fuente: Guía para la gestión integral del riesgo en entidades públicas V7

El mapa de calor permite visualizar las zonas de riesgo de acuerdo con el nivel de severidad de estos (Bajo, Moderado, Alto y Extremo) permitiendo identificar y priorizar los riesgos asociados que requieren mayor atención. Esto ayuda a la organización a mejorar su administración de riesgos, priorizando los esfuerzos y acciones sobre los riesgos potencialmente de mayor impacto.

11. CAPACIDAD, TOLERANCIA Y APETITO DEL RIESGO

La capacidad, tolerancia y apetito del riesgo están definidos según los niveles de aceptación del riesgo frente al alcance de los objetivos estratégicos de la Entidad.

El apetito del riesgo es el nivel de riesgo que la SAE está dispuesta a asumir en la búsqueda de sus objetivos estratégicos y misionales. Se define en la zona de impacto moderado (≤ 100 SMLV) y una frecuencia de ocurrencia inferior al 60 %, según los criterios institucionales de valoración. El apetito de riesgo refleja la capacidad de la Entidad para asumir riesgos controlados que no comprometan sus resultados ni la confianza pública.

La capacidad del riesgo corresponde al nivel máximo de exposición al riesgo que la Entidad puede asumir sin comprometer su sostenibilidad financiera, el cumplimiento de su misión y su reputación. La capacidad considera factores de impacto financiero, operativo, reputacional y de cumplimiento. La SAE establece su capacidad máxima en 80 %, equivalente a una afectación de hasta 500 SMLV o un impacto reputacional a nivel sectorial.

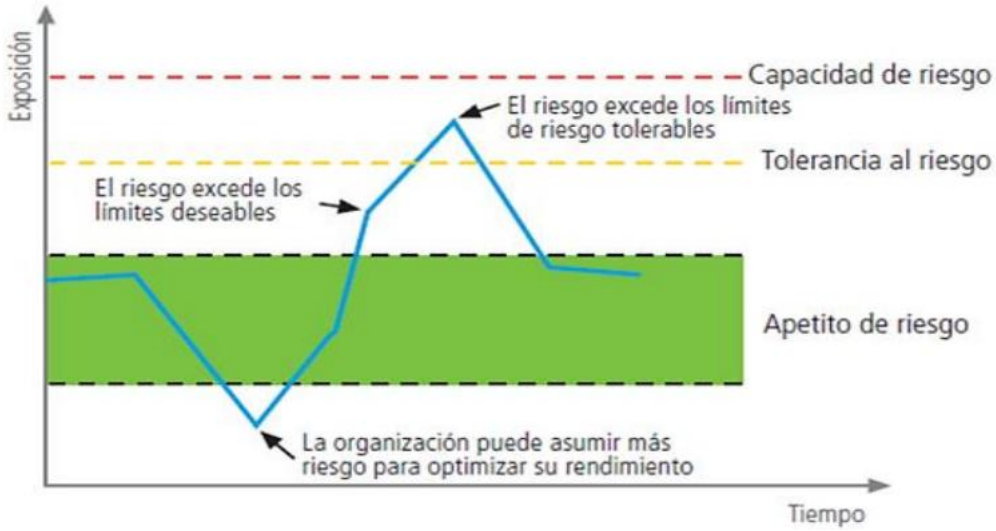
La tolerancia de riesgo representa la desviación aceptable respecto al apetito de riesgo y actúa como una alerta temprana antes de alcanzar la capacidad máxima. La SAE fija su tolerancia en un nivel de 70%, por debajo de la capacidad institucional (80 %), para activar medidas preventivas y correctivas ante tendencias de riesgo crecientes.

Cero tolerancias en riesgos de integridad pública y fiscales: La Entidad mantiene una postura de cero tolerancias frente a los riesgos relacionados con fraude, soborno, conflicto de interés, corrupción,

lavado de activos, financiación del terrorismo, financiación de la proliferación de armas de destrucción masiva y riesgos fiscales, no admitiendo su aceptación en ninguna circunstancia.

Revisión y aprobación de umbrales: Los niveles de apetito, tolerancia y capacidad serán revisados anualmente por la Dirección de Planeación y Prospectiva, validados por el Comité Institucional de Coordinación de Control Interno y aprobados por la Junta Directiva (en caso de que se presenten modificaciones).

Ilustración 3. Capacidad, Límites y Tolerancia del Riesgo



Fuente: Guía para la gestión integral del riesgo en entidades públicas V7

12. TIPOS DE TRATAMIENTO DE LOS RIESGOS

La Sociedad de Activos Especiales – SAE S.A.S. adopta las estrategias de tratamiento previstas en la Guía para la Gestión Integral del Riesgo – Versión 7 (DAFP, 2025), con el fin de decidir la forma de intervención para cada riesgo identificado y valorado:

1. **Evitar el riesgo:** Suprimir la fuente, causa u oportunidad que origina la exposición (ejemplo: Eliminar la actividad, modificar el proceso o la decisión que genera el riesgo).
2. **Reducir el riesgo:** Diseñar o fortalecer controles (preventivos, detectivos y/o correctivos) para disminuir la probabilidad y/o el impacto del riesgo.
3. **Compartir o transferir el riesgo:** Trasladar parcial o totalmente la exposición a un tercero (ejemplo: Aseguradoras, aliados o contratos), manteniendo la responsabilidad institucional sobre la gestión.
4. **Aceptar el riesgo:** Asumir el riesgo cuando su nivel residual se encuentre dentro del apetito institucional y exista justificación documentada y aprobada por la Dirección de Planeación y Prospectiva (DPP), conforme al marco de apetito, tolerancia y capacidad definido en esta Política.

Criterio especial de integridad y fiscal: La SAE mantiene cero aceptaciones para los riesgos de integridad pública (fraude, soborno, conflicto de interés, corrupción, LA/FT/FPADM) y riesgos fiscales.

Gobernanza: La DPP coordina la propuesta de estrategia por cada riesgo; el CICCI analiza riesgos críticos y eleva recomendaciones; la Alta Dirección decide cuando corresponda por materialidad o afectación estratégica.

13. ESTRATEGIA DE TRATAMIENTO Y MONITOREO DE LOS RIESGOS

La Sociedad de Activos Especiales – SAE S.A.S. define la siguiente estrategia para el tratamiento y monitoreo de los riesgos institucionales, garantizando la aplicación de medidas diferenciales de acuerdo con el nivel residual y la naturaleza del riesgo.

Para los riesgos de gestión, el nivel de aceptación aplica únicamente para aquellos que, tras la valoración residual, se ubiquen en zona de riesgo bajo; estos se consideran aceptables y asumidos por la Entidad.

Los riesgos para la integridad pública no tienen niveles de aceptación ni tolerancia, por lo que siempre deben ser objeto de tratamiento y mantenerse, de ser posible, en zona moderada.

En el caso de los riesgos de seguridad de la información, solo serán tolerables los que se ubiquen en zona residual baja, conforme a los lineamientos de la Política de Seguridad y Privacidad de la Información.

Los planes de tratamiento se formularán únicamente para los riesgos clasificados en zona residual extrema, con el fin de reducir su nivel de exposición y fortalecer la efectividad de los controles. Los riesgos altos, moderados y bajos se gestionarán mediante el mantenimiento y mejora continua de controles existentes.

El monitoreo de los riesgos se realizará con base en la zona de riesgo residual, según la siguiente periodicidad:

Tabla 4. Estrategia de Tratamiento y Monitoreo del Riesgo

TIPO DE RIESGOS	ZONA DE RIESGO	ESTRATÉGIA DE TRATAMIENTO	FRECUENCIA DEL MONITOREO
Gestión – Continuidad de Negocio	Baja	Aceptar	Cuatrimestral
	Moderada	Reducir - Mitigar – Transferir	Bimensual
	Alta y Extrema	Reducir - Mitigar - Transferir - Evitar	Mensual
Riesgos para la integridad pública	Moderada	Reducir - Mitigar - Transferir	Bimensual
	Alta y Extrema	Reducir - Mitigar - Transferir - Evitar	Mensual
Fiscales	Moderada	Reducir - Mitigar - Transferir	Bimensual
	Alta y Extrema	Reducir - Mitigar - Transferir - Evitar	Mensual
Seguridad de la Información	Baja	Aceptar	Cuatrimestral
	Moderada	Reducir - Mitigar - Transferir	Bimensual
	Alta y Extrema	Reducir - Mitigar Transferir - Evitar	Mensual

Fuente: Elaboración propia, con base en la Guía para la Gestión Integral del Riesgo – Versión 7 (DAFP, 2025) y lineamientos institucionales de la SAE.

El seguimiento a la implementación de los controles y planes de tratamiento se efectuará de manera cuatrimestral por la Dirección de Planeación y Prospectiva con el objetivo de comprobar que los controles no solo existan, sino que realmente funcionen, y que con base en esa verificación se puedan hacer ajustes para que la gestión del riesgo sea eficaz y alineada con los objetivos institucionales; los resultados se verán reflejados en las bases consolidadas de gestión de riesgos, los planes de tratamiento y los informes institucionales que se presentan al Comité Institucional de Coordinación de Control Interno (CICCI).

14. INDICADORES CLAVE DE RIESGO (KRI)

Los Indicadores Clave de Riesgo (KRI) constituyen herramientas de gestión preventiva que permiten monitorear el comportamiento de los riesgos institucionales, anticipar su posible materialización y evaluar la eficacia de los controles implementados. Su aplicación fortalece la toma de decisiones informadas y la capacidad de respuesta de la entidad ante cambios en el contexto interno o externo.

Cada KRI estará asociado a un riesgo priorizado del Mapa Integral de Riesgos y deberá contar con definición operativa, fórmula, fuente de datos, línea base, umbrales de alerta y responsable designado. Los indicadores se reportarán con base en la zona residual del riesgo: extremo y alto (mensual), moderado (bimensual) y bajo (cuatrimestral).

Los líderes de proceso son responsables de su actualización y análisis; la Dirección de Planeación y Prospectiva (DPP) consolida y valida la información, y presenta los resultados al Comité Institucional de Coordinación de Control Interno (CICCI) y al Comité de Auditoría de Junta Directiva. Cuando un KRI supere los umbrales de alerta, se deberá efectuar un análisis de causa, definir las medidas de mitigación o fortalecimiento de controles y documentar las acciones correctivas o preventivas correspondientes.

15. EVALUACIÓN ANUAL DEL NIVEL DE MADUREZ DEL SISTEMA INTEGRADO DE GESTIÓN

La Sociedad de Activos Especiales (SAE) realizará anualmente la evaluación del nivel de madurez de su sistema de gestión integral de riesgos, empleando el instrumento oficial vigente. La Dirección de Planeación y Prospectiva (DPP) coordinará la autoevaluación con los líderes de proceso, consolidará los resultados institucionales y definirá las acciones de fortalecimiento requeridas. La Oficina de Control Interno (OCI) verificará la trazabilidad de la información y el cumplimiento de los compromisos derivados.

Los resultados de la evaluación se presentarán al Comité Institucional de Coordinación de Control Interno (CICCI) y constituirán insumo para la actualización de la política, la metodología, los mapas de riesgo y los planes de tratamiento, así como para la priorización de acciones en el Plan de Mejoramiento Institucional.

16. AUDITORIA DEL SIGRIP

La Oficina de Control Interno (OCI) desarrollará auditorías basadas en riesgos sobre el Sistema de Integridad y Gestión del Riesgo de la Integridad Pública (SIGRIP) y sobre la gestión integral del riesgo, con el siguiente alcance mínimo:

- Diseño y gobernanza: coherencia entre política, roles, líneas de defensa, umbrales (apetito, tolerancia y capacidad) y lineamientos metodológicos.
- Implementación: aplicación de la metodología en procesos, evidencia de controles y consistencia entre mapas de riesgo, KRIs y planes de tratamiento.
- Efectividad: verificación del desempeño de controles y de la reducción del nivel de riesgo residual.
- Cumplimiento y reporte: trazabilidad de decisiones, oportuno escalamiento al CICCI y seguimiento a planes de mejoramiento.

Las observaciones y recomendaciones se documentarán en los informes de auditoría; la DPP coordinará el plan de acción y el seguimiento al cierre de hallazgos, y la OCI verificará su efectividad.

17. ACCIONES POR SEGUIR EN CASO DE MATERIALIZACIÓN DE RIESGOS

Cuando se materialice un riesgo institucional, la Sociedad de Activos Especiales – SAE S.A.S. deberá ejecutar de manera inmediata las acciones necesarias para contener sus efectos, garantizar la continuidad operativa y establecer medidas de recuperación y mejora.

A. Activación inmediata

El líder del proceso afectado deberá activar las acciones inmediatas de respuesta, priorizando la mitigación del impacto y la protección de los recursos institucionales, la información y la reputación de la Entidad.

Deberá informar de forma inmediata a la Dirección de Planeación y Prospectiva (DPP), quien registrará el evento y consolidará la información necesaria para su análisis.

B. Registro del evento

El evento deberá documentarse en el Formato de Reporte de Riesgos Materializados, incluyendo:

- Fecha y descripción del suceso.
- Causas identificadas y controles que fallaron.
- Impacto generado (financiero, operativo, reputacional, legal).
- Acciones inmediatas adoptadas.
- Responsables y tiempos de ejecución.

C. Plan de tratamiento posterior

La DPP, en coordinación con el líder del proceso, formulará un plan de mejoramiento correctivo, orientado a:

- Eliminar la causa raíz.
- Reforzar o rediseñar los controles.
- Prevenir recurrencias.
- Actualizar el nivel residual del riesgo en el Mapa Institucional.

D. Activación de planes de continuidad o contingencia

Si el riesgo afecta procesos estratégicos, misionales o críticos, se activarán los Planes de Continuidad de Negocio y Contingencia, garantizando la recuperación operativa y la atención oportuna a los grupos de interés.

E. Seguimiento y reporte

La Dirección de Planeación y Prospectiva (DPP) realizará el seguimiento cuatrimestral a la ejecución de las acciones y consolidará la información en los informes institucionales de gestión y control interno.

Los casos relevantes serán presentados al Comité Institucional de Coordinación de Control Interno (CICCI) para análisis, validación y definición de medidas adicionales.

F. Retroalimentación y mejora continua

Los resultados derivados de la materialización de riesgos se incorporarán como insumos para la evaluación de madurez, la actualización del Mapa de Riesgos y, de ser necesario, la revisión de la Política de Riesgos.

18. DIVULGACIÓN DE LA POLÍTICA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS

La divulgación de la Política Integral de Administración de Riesgos de la Sociedad de Activos Especiales – SAE S.A.S. estará a cargo de la Dirección de Planeación y Prospectiva - DPP, garantizando su publicación en la página web institucional, en el enlace de Transparencia, para asegurar la disponibilidad y consulta por parte de todos los grupos de valor e interés.

La Dirección de Planeación y Prospectiva – DPP coordinará la socialización interna de la política mediante eventos de divulgación, capacitaciones y mesas de trabajo con las diferentes dependencias, orientadas a fortalecer la cultura de gestión del riesgo, el control y la integridad.

La SAE definirá y aplicará una evaluación anual del Sistema de Gestión Integral de Riesgos – SIGRIP, que incluirá la revisión de su efectividad, la actualización de los lineamientos metodológicos y la valoración de los Indicadores Clave de Riesgo - KRI definidos en el numeral 14.1.

La Oficina de Control Interno – OCI desarrollará auditorías basadas en riesgos sobre la implementación del SIGRIP, conforme a los criterios establecidos en la presente política y en el Plan Anual de Auditorías Internas, asegurando la trazabilidad y mejora continua.

Los resultados de la evaluación y auditoría se presentarán al Comité Institucional de Coordinación de Control Interno – CICCI y a la Alta Dirección, sirviendo como insumo para la mejora continua del sistema, en concordancia con el Modelo Integrado de Planeación y Gestión – MIPG y la Guía para la Gestión Integral del Riesgo – Versión 7 (DAFP, 2025).

19. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA

La Dirección de Planeación y Prospectiva – DPP realizará el seguimiento y evaluación anual de la implementación de la Política Integral de Administración de Riesgos, con el propósito de verificar su efectividad, coherencia y grado de cumplimiento frente a los objetivos estratégicos institucionales y los lineamientos del Departamento Administrativo de la Función Pública – DAFP.

El seguimiento comprenderá la revisión de los siguientes aspectos:

- Cumplimiento de los lineamientos metodológicos para la identificación, valoración, tratamiento y monitoreo de riesgos.
- Nivel de avance de los planes de tratamiento y efectividad de los controles.
- Cumplimiento de los indicadores clave de riesgo – KRI y tendencias de materialización.
- Madurez del Sistema de Gestión Integral de Riesgos – SIGRIP, conforme con la herramienta de evaluación del Anexo 4 de la Guía para la Gestión Integral del Riesgo V7 del DAFP.
- Oportunidades de mejora y acciones correctivas implementadas en los procesos.

Los resultados del seguimiento serán consolidados por la Dirección de Planeación y Prospectiva y presentados al Comité Institucional de Coordinación de Control Interno – CICCI y a la Alta Dirección, quienes establecerán las decisiones estratégicas necesarias para fortalecer la gestión del riesgo institucional.

El informe anual servirá como insumo para la revisión y actualización de la política, así como para la planeación de las auditorías internas y los ejercicios de autoevaluación del Sistema de Control Interno, promoviendo la mejora continua del SIGRIP y su articulación con el Modelo Integrado de Planeación y Gestión – MIPG.

20. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de Cambios	Justificación del Cambio
1	26/03/2016	Creación del documento	
2	30/03/2022	Se actualiza la política de manera integral y conforme con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5 (DAFP)	Actualización del documento
3	23/07/2024	Se actualiza la política de manera integral y conforme con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V6	Actualización del documento
4	15/11/2025	Actualización integral conforme a la Guía de Gestión Integral del Riesgo V7 (DAFP, 2025) e inclusión de numerales de KRI, Madurez, Auditoría SIGRIP y Divulgación	Actualización del documento

21. CONTROL DE ÚLTIMA APROBACIÓN

Describa las personas que participaron en la documentación del manual desde el ámbito técnico y metodológico, así como los revisores y aprobadores del documento, junto con la información del cargo y área a la cual pertenecen al momento de la documentación.

Etapa	Nombre	Cargo	Área
Elaboración Técnica	Ana Giselly Martinez Montoya Carol Alexandra Campos Vieda	Profesional Especializada grado I Profesional Especializada grado III	Dirección de Planeación y Prospectiva

Etapa	Nombre	Cargo	Área
Acompañamiento metodológico	Ana Giselly Martinez Montoya Carol Alexandra Campos Vieda	Profesional Especializada grado I Profesional Especializada grado III	Dirección de Planeación y Prospectiva
Revisión	Daniel Sebastian Contreras Ortiz	Director de Planeación y Prospectiva	Dirección de Planeación y Prospectiva
Aprobación	Daniel Sebastian Contreras Ortiz	Director de Planeación y Prospectiva	Dirección de Planeación y Prospectiva