

El Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP- es el conjunto de reglas, procesos y herramientas que usa una entidad pública para prevenir, detectar y gestionar riesgos que puedan afectar la transparencia y la legalidad en su gestión.

El SIGRIP se desarrolla con base en la Política para la Gestión Integral de Riesgos que se complementa con el mapa de riesgos y el manual de manejo y gestión de la debida diligencia.

Eje central del SIGRIP:

1. Designación de las funciones de cumplimiento.
2. Herramientas para gestionar:

- Riesgos de integridad (**soborno, fraude, conflicto de intereses**).

Soborno: Consiste en ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida para influir en una actuación u omisión. Puede ser entrante (al servidor de la entidad) o saliente (servidores sobornan a terceros en nombre de la entidad).

Fraude: Esta categoría es un concepto operativo que reúne varias conductas y, cuando un servidor público exige, induce o solicita indebidamente dinero o cualquier utilidad, los hechos pueden configurar el delito de concusión

- Corrupción.
- LA (Lavado de activos).
- FT (Financiación del terrorismo).
- FP (Financiación de la proliferación de armas de destrucción masiva).

Estructura del SIGRIP



Departamento Administrativo de la Función Pública. (2025). Guía para la Gestión Integral del Riesgo en Entidades Públicas (Versión 7). Bogotá D.C., Colombia.

1 Política para la Gestión Integral de Riesgos

La entidad debe definir cómo se van a manejar las situaciones que puedan afectar la transparencia y legalidad en el ejercicio de la función pública. Para ello, debe integrar los riesgos relacionados con el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas (LA/FT/FP), junto con los riesgos generales de gestión, el riesgo fiscal y los riesgos de seguridad de la información, a través de las siguientes etapas:

a Identificación y descripción del riesgo

La entidad debe identificar en qué partes de su gestión pueden existir riesgos y qué áreas podrían verse afectadas, ya sea en el ámbito económico, reputacional, legal o por riesgo de contagio.

Además, debe determinar los factores de riesgo en sus operaciones, es decir, las situaciones que podrían generar impactos negativos o afectar su funcionamiento.

b Análisis del riesgo inherente

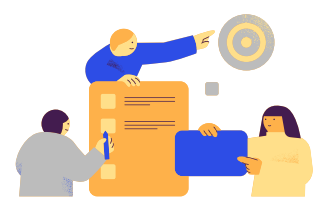
En esta etapa se evalúan los riesgos propios de la entidad antes de aplicar cualquier control. El objetivo es identificar, prevenir, detectar y reportar los riesgos que pueden surgir debido a la naturaleza y funciones de la entidad pública.



c Diseño y análisis de controles

Se deben definir medidas o controles para prevenir o reducir cada riesgo identificado. Para ello, la entidad puede:

- Crear nuevos controles.
- Ajustar los controles existentes.
- Fortalecer procesos.



d Valoración del riesgo residual

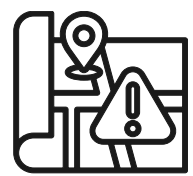
Esta etapa consiste en analizar el riesgo que todavía permanece después de aplicar las medidas preventivas, correctivas o de detección.

La entidad debe evaluar qué tan significativo es este riesgo residual y definir cómo gestionarlo, para asegurarse de que no afecte el funcionamiento de sus operaciones.

2 Mapa integral de riesgos

Es una herramienta descriptiva que resume los resultados del análisis realizado en cada etapa de la Política para la Gestión Integral de Riesgos y permite ver de manera organizada dónde existen riesgos y cómo se relacionan con los procesos de la entidad.

Deben estructurarse de acuerdo con las particularidades de cada proceso y tener en cuenta su complejidad, la interacción con otros procesos dentro de la entidad, la gestión de recursos y servicios, y los usuarios con los que se relaciona, sean internos o externos.



3 Debida diligencia en el conocimiento de las contrapartes

Busca conocer a las contrapartes en todas las interacciones con exposición a riesgos de integridad pública.

Se aplica antes de iniciar cualquier relación y de manera continua durante toda la relación, con actualizaciones periódicas según el nivel de riesgo que represente cada contraparte.



Todo este proceso debe estar registrado y regulado en el Manual de Debida Diligencia de la entidad, para garantizar que se sigan criterios claros y seguros en cada etapa.

4 Función de cumplimiento

La Función de Cumplimiento garantiza que el SIGRIP funcione correctamente, protegiendo la integridad de la entidad pública. Para lograrlo promueve una estructura organizacional clara, con roles y responsabilidades definidos, y asegura su evaluación, actualización y mejora continua, en alineación con los lineamientos de los entes de control.

Además, diseña metodologías e indicadores de riesgo, define criterios de debida diligencia para las contrapartes y establece parámetros para identificar y reportar operaciones inusuales o sospechosas, asegurando que todas las medidas se apliquen de manera efectiva y coherente.

5 Herramientas de gestión del riesgo

Las Herramientas de Gestión del Riesgo son todos los documentos, políticas y lineamientos que respaldan el SIGRIP y permiten que funcione de manera efectiva. Estas herramientas ayudan a prevenir y controlar los riesgos que pueden afectar la integridad de la entidad pública, incluyendo el lavado de activos, la financiación del terrorismo y la proliferación de armas (LA/FT/FP), así como el soborno, el fraude y los conflictos de intereses.

Además, establecen cómo se deben reportar operaciones inusuales o sospechosas y definen los canales de denuncia, garantizando que toda la gestión de riesgos se realice de manera transparente, ordenada y confiable.

