Interior

Guía para la Gestión Integral del Riesgo

Presentación de apoyo · Versión 7 · 2025

Subdirección de Proyectos para la Seguridad y la Convivencia Ciudadana

Abril 2026

Ruta de la presentación

Una lectura sencilla de la guía para explicar en equipo.

Interior

1. Contexto y novedades V7
2. Ámbitos de riesgo
3. Riesgos generales de gestión
4. Riesgo fiscal
5. Seguridad de la información
6. Integridad pública / SIGRIP
7. Controles, tratamiento y KRI

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025).

¿Qué trae la versión 7?

Actualiza el enfoque hacia una gestión integral del riesgo.

Interior

Estructura común

Mantiene una base metodológica general aplicable a las diferentes tipologías.

COSO-ERM y apetito

Profundiza conceptos de riesgo, madurez y apetito de riesgo.

Riesgo fiscal

Precisa el enfoque preventivo y actualiza ejemplos.

Integridad pública

Incorpora SIGRIP y riesgos asociados a corrupción, fraude, soborno, conflicto de intereses y LA/FT/FP.

Seguridad de la información

Despliega pasos metodológicos y ejemplo práctico.

Caja de herramientas

Actualiza anexos y matriz del mapa de riesgos.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · págs. 3-4.

Articulación de los ámbitos de riesgo

La guía propone una sola política institucional para gestionar los riesgos.



Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · pág. 48.

1. Riesgos generales de la gestión

Afectan la operación normal y el cumplimiento de objetivos institucionales.

¿Qué son?

- Situaciones que pueden afectar procesos, servicios, planes, programas o proyectos.
- Se analizan a partir del contexto interno y externo, objetivos y factores de riesgo.
- Incluyen riesgos operativos, estratégicos, tecnológicos, externos, de talento humano, entre otros.

Pregunta guía

¿Qué puede impedir, retrasar o afectar la entrega del producto, servicio o resultado esperado?

Ejemplos
Demoras en trámites o proyectos
Errores en información reportada
Fallas tecnológicas o de infraestructura
Incumplimiento de requisitos del proceso

Controles y evidencias
Procedimientos actualizados y socializados
Validaciones previas y listas de chequeo
Seguimiento periódico a indicadores
Actas, reportes, matrices y soportes de revisión

Clave para exponer: este riesgo no es “algo malo que ya pasó”; es una posibilidad que se anticipa para proteger el cumplimiento del proceso.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · capítulo III.

Cómo redactar un riesgo

La redacción debe permitir entender evento, causa e impacto.

Evento potencial

¿Qué puede ocurrir?

Causa raíz

¿Por qué podría ocurrir?

Impacto

¿Qué afectaría?

Ejemplo sencillo

“Posibilidad de retraso en la atención de solicitudes, por ausencia de seguimiento oportuno al flujo de trabajo, generando incumplimiento de términos y afectación en indicadores de oportunidad.”

Recomendación: evitar frases generales como “falta de gestión” o “incumplimiento” sin precisar causa, evento e impacto.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · estructura metodológica capítulo III.

2. Riesgo fiscal

Se enfoca en prevenir afectaciones al patrimonio público.

Definición práctica

Posibilidad de un efecto dañoso sobre recursos, bienes o intereses patrimoniales públicos, causado por un evento potencial.

No debe confundirse con el daño patrimonial ya materializado. El riesgo fiscal es preventivo; el hallazgo fiscal o daño patrimonial corresponde a otra etapa.

Enfoque preventivo

Gestión fiscal

Ejemplos
Pérdida o hurto de bienes
Prescripción de cobro
Pagos sin soportes suficientes
Errores en liquidaciones o inventarios

Controles clave
Inventarios y conciliaciones periódicas
Supervisión contractual documentada
Alertas de vencimientos y obligaciones
Revisión jurídica, técnica y financiera

Pregunta de identificación: ¿en qué actividades se manejan, custodian, administran o deciden recursos, bienes o intereses patrimoniales del Estado?

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · págs. 74-88.

Cuadro de apoyo: identificación del riesgo fiscal

Cinco pasos que ayudan a estructurar el análisis.

Interior

1

Punto de riesgo

Actividad donde se realiza gestión fiscal.

2

Área de impacto

Recurso, bien o interés patrimonial expuesto.

3

Efecto económico

Consecuencia económica potencial.

4

Causa raíz

Origen real que puede generar el evento.

5

Descripción

Redacción clara del riesgo fiscal.

Ejemplo de lectura: “Pérdida de bienes muebles por omisión en la aplicación del procedimiento de ingreso, custodia, salida e inventario.”

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · figura y pasos del capítulo IV.

3. Riesgos de seguridad de la información

Se analizan sobre activos de información y sus propiedades.

Interior

C

Confidencialidad

Acceso autorizado a la información.

I

Integridad

Información completa, exacta y sin alteraciones no autorizadas.

D

Disponibilidad

Información accesible cuando se necesita.

Activos típicos
Bases de datos
Expedientes físicos o digitales
Aplicaciones y sistemas
Equipos, servidores y redes

Amenazas / vulnerabilidades
Caída de sistemas o redes
Errores de software o hardware
Accesos no autorizados
Pérdida o alteración de información

Controles
Inventario y clasificación de activos
Copias de seguridad
Gestión de accesos y perfiles
Planes de continuidad y respuesta

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · capítulo V, págs. 93-104.

Cuadro de apoyo: ruta para seguridad de la información

La matriz parte del inventario y criticidad de los activos.

Interior

1

Inventariar activos

Identificar información, sistemas, soportes y responsables.

2

Clasificar criticidad

Valorar confidencialidad, integridad y disponibilidad.

3

Analizar amenazas

Reconocer amenazas y vulnerabilidades aplicables.

4

Definir controles

Establecer controles técnicos, administrativos y físicos.

5

Reportar y seguir

Registrar eventos, evidencias e indicadores.

Mensaje para la entidad: no se gestiona “la tecnología” en abstracto; se gestionan activos de información concretos, con responsables y criticidad definida.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · capítulo V.

4. Riesgos para la integridad pública

La versión 7 amplía el enfoque tradicional de corrupción.

Incluye conductas que afectan el ejercicio íntegro de la función pública:

- Corrupción.
- Soborno.
- Fraude.
- Conflicto de intereses gestionado inadecuadamente.
- Lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva: LA/FT/FP.

Puntos de riesgo	Controles / evidencias
Contratación y supervisión	Debida diligencia de contrapartes
Trámites y permisos	Declaración y gestión de conflictos
Subsidios, recursos o beneficios	Segregación de funciones
Manejo de información reservada	Canales de denuncia y trazabilidad

Clave: estos riesgos no van separados; deben gestionarse junto con los riesgos de gestión, fiscal y seguridad de la información.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · capítulo VI, págs. 120-129.

Cuadro de apoyo: elementos del SIGRIP

Sistema de Gestión de Riesgos para la Integridad Pública.

Interior

Política integral

Define mecanismos para identificar y valorar todos los riesgos.

Mapa de riesgos

Incluye riesgos para la integridad pública dentro de la gestión institucional.

Toma de conciencia

Formación y comunicación interna y externa.

Documentación

Información documentada, trazabilidad, archivo y protección de datos.

Operación y mejora

Seguimiento periódico y actualización del sistema.

Para exponerlo fácil: el SIGRIP ordena la forma de prevenir, documentar y hacer seguimiento a riesgos que comprometen la integridad pública.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · capítulo VI.

Diseño y análisis de controles

Un control debe estar bien diseñado y funcionar en la práctica.

Interior

Preventivo

Actúa antes de que ocurra la causa.

Ej.: validación previa, segregación de funciones.

Detectivo

Identifica desviaciones durante o después del evento.

Ej.: conciliaciones, reportes, alertas.

Correctivo

Permite corregir o mitigar efectos cuando el riesgo se materializa.

Ej.: plan de mejora, recuperación, ajuste del procedimiento.

Al revisar un control, pregunte: ¿tiene responsable?, ¿frecuencia?, ¿evidencia?, ¿actúa sobre la causa?, ¿se ejecuta realmente?, ¿reduce probabilidad o impacto?

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · capítulo III.

Tratamiento y seguimiento

Después de valorar el riesgo residual se decide qué hacer.

Interior

Aceptar

Cuando el nivel está dentro de lo tolerable.

Reducir / mitigar

Implementar acciones para disminuir probabilidad o impacto.

Transferir / compartir

Trasladar parte del riesgo mediante mecanismos válidos.

Evitar

Suspender o rediseñar la actividad que genera el riesgo.

Plan de tratamiento

- Acciones concretas.
- Responsable.
- Fecha o periodicidad.
- Evidencia esperada.

Seguimiento

- Verificar ejecución de controles.
- Revisar materializaciones.
- Actualizar matriz cuando cambie el contexto.
- Reportar alertas.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025).

Indicadores clave de riesgo - KRI

Alertas tempranas para monitorear exposición y severidad.

¿Para qué sirven?

- Permiten identificar señales de alerta antes de la materialización.
- Ayudan a detectar tendencias o cambios en el nivel de exposición.
- Complementan los KPI de proceso y fortalecen el enfoque preventivo.

Ejemplos:

PQRS próximas a vencer · porcentaje de soportes incompletos · incidentes de seguridad · hallazgos recurrentes · alertas de supervisión.



Diferencia útil: un KPI mide desempeño del proceso; un KRI alerta sobre exposición al riesgo.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · págs. 163-169.

Roles y líneas de responsabilidad

La gestión del riesgo no corresponde a una sola dependencia.

Línea estratégica	**Alta dirección / Comités**	Define política, apetito, seguimiento y decisiones.
Primera línea	**Líderes de proceso**	Gestiona riesgos, controles, evidencias y planes de tratamiento.
Segunda línea	**Planeación, calidad, riesgos, jurídica, TI**	Acompaña metodología, consolida, asesora y monitorea.
Tercera línea	**Control interno**	Evalúa de forma independiente y recomienda mejoras.

Mensaje clave: quien ejecuta el proceso también debe gestionar sus riesgos; Planeación acompaña, pero no reemplaza al dueño del proceso.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025).

Ejemplo de aplicación institucional

Modelo sencillo para llevar la guía a un proceso real.

Interior

Proceso / trámite

Presentación, evaluación, viabilización y seguimiento de proyectos.

Objetivo protegido

Asegurar que los proyectos cumplan requisitos técnicos, financieros y jurídicos, con trazabilidad y oportunidad.

Riesgo gestión	Riesgo fiscal	Integridad / SI
Demora en revisión o respuesta	Pagos sin soporte suficiente	Conflictos de interés
Documentos incompletos	Deficiencias en supervisión	Accesos indebidos a información
Baja trazabilidad del flujo	No reporte oportuno de novedades	Pérdida o alteración documental

Controles ejemplo: listas de chequeo, revisión por roles, actas de comité, informes de supervisión, radicados, trazabilidad SIPI, seguimiento de términos y matriz de evidencias.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025) · adaptación didáctica.

Cierre: ideas para dejar claras

Mensaje final para una exposición sencilla.

Interior

1. **La versión 7 no cambia solo nombres: ordena una gestión integral del riesgo.**
2. **La entidad debe gestionar riesgos de gestión, fiscal, seguridad de la información e integridad pública bajo una política común.**
3. La matriz es un instrumento; lo importante es el análisis, los controles, el tratamiento y la evidencia.
4. Los KRI permiten pasar de reaccionar a anticiparse.
5. Cada proceso debe aterrizar la guía a sus actividades reales.

Fuente base: Función Pública, Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025).