ALCALDÍA
DE PASTO

MANUAL DE GESTIÓN INTEGRAL DE RIESGOS
OFICINA DE PLANEACIÓN DE GESTIÓN INSTITUCIONAL

ALCALDÍA DE PASTO

MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

MANUAL DE GESTIÓN INTEGRAL DE RIESGO

ELABORACIÓN, REVISIÓN Y APROBACIÓN DE DOCUMENTOS		
DATOS	**ELABORADO POR:**	**REVISADO POR:**
FIRMA:	Francisco Castillo	carenforerojurado
NOMBRE:	FRANCISCO CASTILLO NOGUERA	CAREN FORERO JURADO
CARGO:	Profesional Especializado Contratista	Profesional Especializado Contratista

DATOS	**APROBADO POR:**
FIRMA:	
NOMBRE:	NELSON HERNAN ROSERO ERAZO
CARGO:	Jefe Oficina De Planeación De Gestión Institucional

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Alcaldía de Pasto, en cumplimiento de sus responsabilidades constitucionales y legales, debe garantizar que los recursos públicos se utilicen de manera eficiente, que los planes y programas se ejecuten oportunamente y que los servicios a la ciudadanía se presten con calidad, transparencia e integridad.

Para lograrlo, es necesario identificar, analizar y gestionar de manera anticipada los riesgos que puedan afectar el cumplimiento del Plan de Desarrollo, los objetivos institucionales, la prestación de los servicios, la estabilidad financiera y la confianza de la ciudadanía. La gestión integral del riesgo no es un ejercicio aislado ni un requisito formal, sino una herramienta fundamental para la toma de decisiones, la planeación, el control y la mejora continua de la gestión pública.

En este sentido, la Alcaldía de Pasto adopta un enfoque de gestión integral del riesgo alineado con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo Estándar de Control Interno (MECI), la Guía de Gestión Integral del Riesgo – Versión 7 del Departamento Administrativo de la Función Pública y el Decreto 1122 de 2024, que establece el Programa de Transparencia y Ética Pública y el Sistema de Gestión de Riesgos de Integridad Pública.

Este enfoque permite que los riesgos estratégicos, operativos, fiscales, de corrupción, de información y de cumplimiento sean identificados y tratados de manera sistemática, articulando la planeación, la ejecución, el seguimiento y el control, con el fin de prevenir pérdidas, evitar fallas en la gestión, reducir la posibilidad de actos de corrupción y fortalecer la confianza de la ciudadanía en la administración municipal.

La gestión integral del riesgo es responsabilidad de todos los servidores públicos, y de manera especial de los líderes de proceso, secretarios, directores y jefes de dependencia, quienes deben identificar y gestionar los riesgos asociados a sus funciones, apoyados por las instancias de planeación, seguimiento y control institucional.

Este enfoque se complementa con los principios del marco COSO ERM, el cual promueve la integración del riesgo con la estrategia y el desempeño institucional, fortaleciendo la capacidad de la Alcaldía de Pasto para anticiparse a los eventos adversos, tomar decisiones informadas y generar valor público de manera sostenible.

2. OBJETIVO

Establecer el marco institucional, metodológico y operativo para la gestión integral de los riesgos en la Alcaldía de Pasto, con el fin de identificar, evaluar, tratar, hacer seguimiento y controlar los eventos que puedan afectar el cumplimiento de los objetivos institucionales, el Plan de Desarrollo Municipal, la adecuada gestión de los recursos públicos, la integridad, la transparencia y la prestación de los servicios a la ciudadanía. Este manual busca asegurar que todas las dependencias, procesos, programas, proyectos y contratos de la Alcaldía de Pasto gestionen sus riesgos de manera articulada con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo Estándar de Control Interno (MECI) y el Programa de Transparencia y Ética Pública (PTEP), así como los riesgos para la seguridad de la información de los ciudadanos y los sistemas institucionales, promoviendo una cultura de prevención, control y mejora continua en la administración municipal.

3. MARCO LEGAL

Ley/Norma/Requisito	Descripción/criterios que apliquen
Constitución Política de Colombia	Establece los principios de la función administrativa, la responsabilidad de los servidores públicos, la protección del patrimonio público y el deber de garantizar la moralidad, eficacia, economía y transparencia en la gestión pública.
Ley 87 de 1993 – Control Interno	Obliga a todas las entidades públicas a implementar un sistema de control interno que permita identificar, evaluar y controlar los riesgos que puedan afectar el cumplimiento de los objetivos institucionales y la adecuada administración de los recursos públicos.
Ley 489 de 1998	Regula la organización y funcionamiento de la administración pública y exige que las entidades adopten mecanismos de planeación, control y evaluación de la gestión.
Decreto 1083 de 2015	Decreto Único Reglamentario del Sector Función Pública. Establece que las entidades deben implementar sistemas de gestión que integren planeación, control, evaluación y mejora continua.
Decreto 1499 de 2017	Adopta el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo Estándar de Control Interno (MECI), estableciendo la gestión del riesgo como un componente obligatorio de la planeación y el control institucional.

Decreto 648 de 2017	Modifica el Sistema de Control Interno y fortalece la responsabilidad de los líderes de proceso en la gestión de los riesgos que afectan el logro de los objetivos institucionales.
Decreto 1122 de 2024	Establece el Programa de Transparencia y Ética Pública (PTEP) y el Sistema de Gestión de Riesgos de Integridad Pública (SIGRIP), obligando a las entidades a identificar, evaluar y tratar los riesgos de corrupción, integridad, conflicto de intereses y fraude.
Modelo Integrado de Planeación y Gestión – MIPG	Exige que la planeación, ejecución, seguimiento y evaluación de la gestión pública se realicen con base en la identificación y control de los riesgos que puedan afectar el desempeño institucional.
Modelo Estándar de Control Interno – MECI	Establece que la gestión del riesgo es uno de los componentes esenciales del sistema de control interno, orientado a prevenir fallas, pérdidas y desviaciones en la gestión pública.
Guía de Gestión Integral del Riesgo – Versión 7 (Función Pública, 2025)	Define el marco técnico y metodológico obligatorio para la identificación, evaluación, tratamiento, seguimiento y control de los riesgos estratégicos, operativos, fiscales, de corrupción, de información y de cumplimiento en las entidades del Estado.
COSO ERM (2017)	Marco de referencia internacional que orienta la integración de la gestión del riesgo con la estrategia, el desempeño y la toma de decisiones, complementando los lineamientos del MIPG y la Guía de Gestión Integral del Riesgo del Departamento Administrativo de la Función Pública.

4. ALCANCE

El presente Manual de Gestión Integral del Riesgo es de aplicación obligatoria para todas las dependencias, Secretarías, direcciones, oficinas, programas, proyectos, fondos y entidades adscritas o vinculadas a la Alcaldía de Pasto, así como para los procesos, contratos, sistemas de información y actividades que involucren la toma de decisiones, el uso de recursos públicos o la prestación de servicios a la ciudadanía.

La gestión del riesgo deberá aplicarse en los niveles estratégico, misional, de apoyo y de evaluación, y cubrirá los riesgos estratégicos, operativos, fiscales, de cumplimiento, de integridad y corrupción, de información, tecnológicos y reputacionales que puedan

afectar el logro de los objetivos institucionales y el cumplimiento del Plan de Desarrollo Municipal.

Todos los servidores públicos, contratistas y responsables de procesos deberán participar activamente en la identificación, análisis, tratamiento y seguimiento de los riesgos relacionados con sus funciones, de acuerdo con lo establecido en este manual.}

5. DEFINICIONES

- **Control:** Acción, mecanismo (política, proceso, dispositivo) o procedimiento diseñado para prevenir, detectar o corregir un riesgo.

- **Factor de riesgo:** Fuente de donde provienen las amenazas (Talento Humano, Procesos, Tecnología, Infraestructura, Evento Externo).

- **Gestión integral del riesgo:** Proceso continuo mediante el cual la entidad identifica, analiza, evalúa, trata y hace seguimiento a los riesgos que pueden afectar su desempeño.

- **Impacto:** Resultado o consecuencia de un evento que afecta los objetivos. Se mide en términos económicos (SMLMV) o reputacionales.

- **Indicador de riesgo (KRI):** Medida que permite monitorear el comportamiento del riesgo y generar alertas tempranas.

- **Probabilidad:** Posibilidad de que un riesgo ocurra.

- **Plan de tratamiento:** Conjunto de acciones definidas para modificar un riesgo (Reducir, Evitar, Compartir o Aceptar).

- **Riesgo:** Posibilidad de que ocurra un evento que afecte el logro de los objetivos institucionales.

- **Riesgo fiscal:** Evento que puede generar pérdida o afectación de los recursos públicos.

- **Riesgo inherente:** Nivel de riesgo existente antes de aplicar controles.

- **Riesgo de integridad:** Evento relacionado con actos de corrupción, fraude, soborno o conflictos de interés.

- **Riesgo residual:** Nivel de riesgo que permanece después de aplicar los controles existentes.

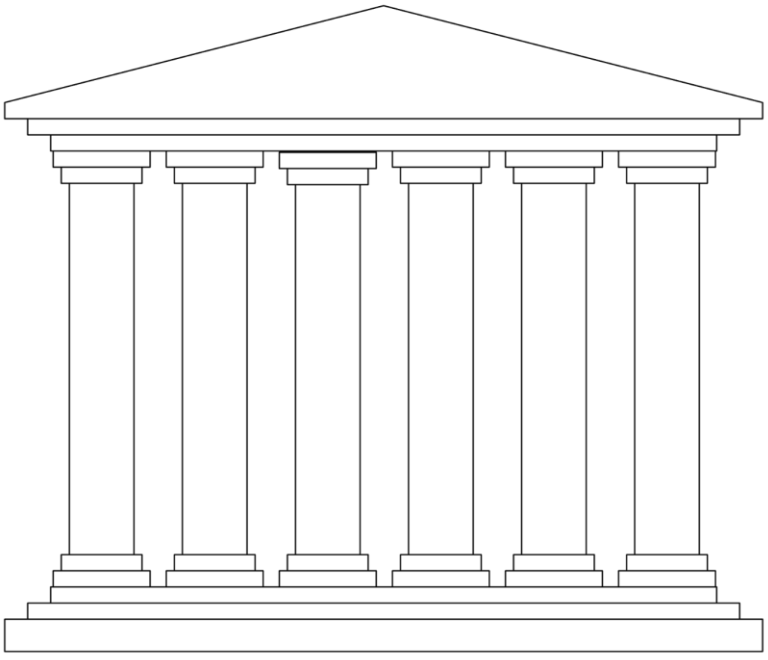
- **SIGRIP:** Sistema de Gestión de Riesgos para la Integridad Pública, enfocado en prevenir la corrupción.

6. MARCO CONTEXTUAL

6.1. PRINCIPIOS DE LA GESTIÓN INTEGRAL DEL RIESGO

La gestión integral del riesgo en la Alcaldía de Pasto se rige por los siguientes principios:

Principios de la Gestión Integral del Riesgo



Enfoque Preventivo
Identificar y abordar los riesgos antes de que se conviertan en problemas.

Enfoque Estratégico
Alinear la gestión del riesgo con los objetivos institucionales.

Responsabilidad del Líder
Cada líder es responsable de los riesgos dentro de su área.

Integración con la Planeación
Incorporar la gestión del riesgo en todos los planes y decisiones.

Transparencia e Integridad
Fomentar la confianza ciudadana a través de prácticas éticas.

Mejora Continua
Revisar y actualizar constantemente los riesgos y controles.

6.2. APETITO Y TOLERANCIA AL RIESGO

La Alcaldía de Pasto define el nivel de riesgo que está dispuesta a aceptar en el cumplimiento de sus funciones, de acuerdo con los siguientes criterios generales:

CONCEPTO	NIVEL DE TOLERANCIA
Riesgos de la integridad pública e integridad	Cero tolerancias
Riesgos de la integridad pública LA/FT/FP	Cero tolerancias
Riesgo fiscal (pérdida de recursos públicos)	Muy Bajo
Riesgos de seguridad de la información	Bajo
Riesgos Gestión	Moderado

Niveles de Tolerancia al Riesgo de la Alcaldía de Pasto

Cuando un riesgo supere estos niveles de tolerancia, deberá ser tratado de manera prioritaria mediante acciones correctivas y de mejora.

6.3. MODELO DE TRES LÍNEAS DE DEFENSA

La Alcaldía de Pasto adopta el Modelo de Líneas de Defensa, establecido en el Modelo Integrado de Planeación y Gestión – MIPG y desarrollado en la Guía de Gestión Integral del Riesgo – Versión 7 del Departamento Administrativo de la Función Pública, como esquema para la asignación clara de responsabilidades frente a la gestión del riesgo.

Este modelo permite garantizar que la identificación, evaluación, tratamiento y seguimiento de los riesgos sea una responsabilidad compartida, articulada y coherente en todos los niveles de la entidad.

Líneas de Defensa en la Gestión del Riesgo

Característica	Primera Línea de Defensa	Segunda Línea de Defensa	Tercera Línea de Defensa	Alta Dirección
Quiénes la conforman	Líderes de proceso y servidores públicos	Oficina de Planeación y Gestión Institucional (OPGI) y dependencias con funciones de orientación y seguimiento	Oficina de Control Interno	Alcalde(a), Secretarios(as), Directivos
Responsabilidades frente a la gestión del riesgo	Identificar, analizar, valorar, diseñar, aplicar, mantener, ejecutar, realizar seguimiento, reportar, actualizar	Definir lineamientos, brindar acompañamiento, consolidar, monitorear, emitir alertas, informar	Evaluar, verificar, evaluar, identificar, reportar, hacer seguimiento	Definir, establecer, tomar decisiones, asignar, promover

	ACTOR	ROL FRENTE A LA GESTIÓN INTEGRAL DEL RIESGO
ENTORNO EXTERNO – ENTES RECTORES	Consejo para la Gestión y Desempeño	Propone, orienta y evalúa las políticas institucionales relacionadas con la gestión y el desempeño, incluyendo la gestión integral del riesgo, en coherencia con el MIPG.
	Consejo Asesor en materia de Control Interno (Función Pública)	Propone la adopción de políticas, lineamientos y buenas prácticas para fortalecer el control interno y la gestión del riesgo en las entidades del Estado.
	Líderes de Política (DAFP y entes rectores)	Definen lineamientos, metodologías y directrices técnicas para la implementación de la gestión integral del riesgo en el sector público.
	Departamento Administrativo de la Función Pública	Lidera la política de control interno y gestión del riesgo, emite la Guía de Gestión Integral del Riesgo y brinda asistencia técnica a las entidades.
ENTORNO INTERNO – LÍNEA ESTRATÉGICA	Comité Institucional de Gestión y Desempeño	Analiza la gestión integral del riesgo institucional, define prioridades de mejora y realiza seguimiento a los riesgos estratégicos y críticos que afectan el Plan de Desarrollo Municipal.
	Comité Institucional de Coordinación de Control Interno	Analiza eventos de riesgo relevantes, riesgos materializados y debilidades del sistema de control interno, y formula recomendaciones para su fortalecimiento.
		• Define y aprueba la Política de Gestión Integral del Riesgo. • Establece el apetito y la tolerancia al riesgo. • Toma decisiones frente a riesgos altos y críticos. • Asigna recursos para la gestión del riesgo. • Promueve el "tono desde la cima" y la cultura de prevención.

TERCERA LÍNEA DE DEFENSA – EVALUACIÓN INDEPENDIENTE	Oficina de Control Interno	• Evalúa de manera independiente la gestión integral del riesgo. • Verifica la correcta aplicación de la metodología institucional. • Evalúa la efectividad de los controles. • Emite recomendaciones y alertas a la Alta Dirección. • Realiza seguimiento a los planes de mejora derivados de la gestión del riesgo. • Entregar a la oficina de planeación de gestión institucional los informes de auditoría donde se refleje la materialización de riesgos identificados en el proceso de auditoría
SEGUNDA LÍNEA DE DEFENSA – ORIENTACIÓN Y SEGUIMIENTO	Oficina de Planeación de Gestión Institucional – OPGI	• Define la metodología, lineamientos y herramientas para la gestión integral del riesgo. • Brinda acompañamiento técnico a los líderes de proceso. • Consolida la información institucional de riesgos. • Monitorea el cumplimiento de ejecución de controles y planes de tratamiento. • Emite alertas tempranas frente a riesgos críticos.
	Otras instancias de segunda línea (según aplique)	• Apoyan el seguimiento, la supervisión y la gestión preventiva de los riesgos asociados a sus competencias específicas (financieros, tecnológicos, contractuales, legales, entre otros).
PRIMERA LÍNEA DE DEFENSA – GESTIÓN OPERATIVA DEL RIESGO	Líderes de Proceso	• Identifican los riesgos asociados a los objetivos del proceso. • Analizan y valoran la probabilidad e impacto de los riesgos. • Diseñan, aplican y mantienen los controles. • Ejecutan los planes de tratamiento del riesgo. • Realizan seguimiento periódico a riesgos, controles e indicadores (KRI). • Reportan información oportuna y veraz. • Mensualmente se debe realizar la reunión de equipos primarios (reunión del líder del proceso con su equipo de trabajo) para verificar el grado de cumplimiento y control de sus riesgos. Debe quedar consignada en acta esta reunión.

	Servidores públicos y contratistas	• Ejecutan los controles operativos definidos. • Cumplen los lineamientos y procedimientos establecidos. • Informan oportunamente situaciones que puedan generar riesgos. • Participan en la identificación y actualización de riesgos.

6.4. TIPOS DE RIESGO

La Alcaldía de Pasto gestionará de manera integral los riesgos que puedan afectar el cumplimiento de sus objetivos, de acuerdo con las siguientes categorías:

1. **Riesgos de Gestión (Operativos y Estratégicos):** Son los eventos asociados a la operación diaria de los procesos que pueden generar fallas en la prestación de los servicios o en el cumplimiento de los planes de desarrollo. Incluyen:
   a. Riesgos Estratégicos: Eventos que impactan el cumplimiento de la misión, visión y objetivos de alto nivel del Plan de Desarrollo Municipal debido a cambios en el entorno o en la planeación estratégica.
   b. Riesgos de Cumplimiento: Eventos derivados de la inobservancia de normas legales, contractuales o políticas internas que exponen a la entidad a procesos sancionatorios o nulidades administrativas.

2. **Riesgos fiscales:** Corresponden a la posibilidad de un efecto dañoso sobre los recursos, bienes o intereses patrimoniales de naturaleza pública del municipio. Se asocian a la gestión fiscal antieconómica, ineficaz o inoportuna en procesos de contratación, pagos, recaudo y custodia de bienes.

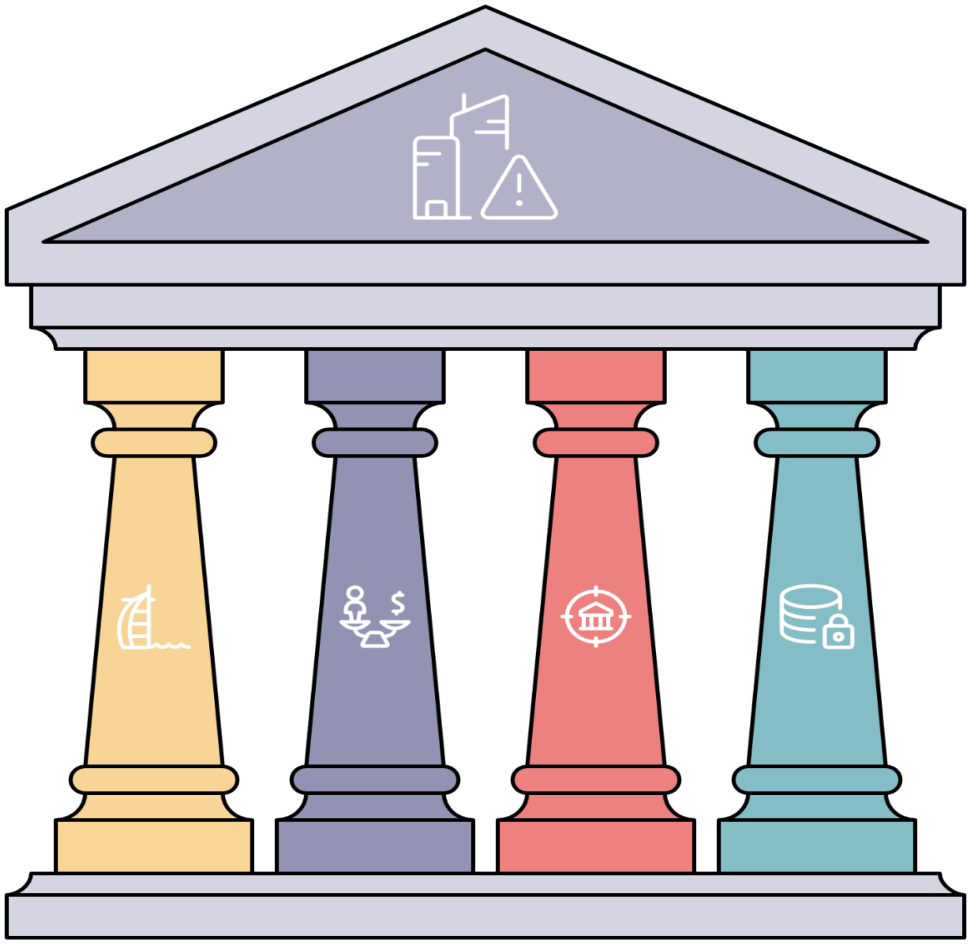
3. **Riesgos para la Integridad Pública (SIGRIP):** Amenazas que comprometen el ejercicio probó del servicio público y la prevalencia del interés general. En el marco del Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, se gestionan las siguientes amenazas específicas:
   a. Corrupción: Desviación de la gestión administrativa para obtener beneficios propios o de terceros.
   b. Soborno y Fraude: Ofrecimiento o aceptación de ventajas indebidas y errores dolosos en informes o trámites.
   c. Conflicto de Intereses: Situaciones donde el interés particular del servidor colisiona con su deber público.
   d. LA/FT/FP: Riesgos de Lavado de Activos y Financiación del Terrorismo.

4. **Riesgos de seguridad de la información:** Eventos que afectan la confidencialidad, integridad y disponibilidad de los activos de información y datos de los ciudadanos.

Incluyen vulnerabilidades tecnológicas en sistemas, bases de datos catastrales, plataformas de recaudo y fallas en la infraestructura digital

a. Acceso no autorizado a datos de ciudadanos
b. Pérdida o alteración de información crítica
c. Ataques cibernéticos a sistemas institucionales
d. Fallas en la continuidad de sistemas misionales

Marco de Riesgos de la Alcaldía de Pasto



Riesgos de Gestión
Eventos que afectan la operación diaria y el cumplimiento de los objetivos estratégicos.

Riesgos Fiscales
Posibilidad de efectos dañinos sobre los recursos y bienes públicos.

Riesgos de Integridad Pública
Amenazas que comprometen el servicio público y el interés general.

Riesgos de Seguridad de la Información
Eventos que afectan la confidencialidad, integridad y disponibilidad de los datos.

6.5. FACTORES DE RIESGO

En el marco de la Gestión Integral de Riesgos de la Alcaldía de Pasto, un factor de riesgo se entiende como la fuente, condición o circunstancia interna o externa que puede dar origen a la materialización de un riesgo, afectando el cumplimiento de los objetivos estratégicos, misionales, operativos, de integridad, tecnológicos y de apoyo de la entidad.

El factor de riesgo constituye el elemento causal del riesgo, es decir, aquello que explica por qué puede ocurrir un evento no deseado, y permite identificar de manera preventiva las debilidades, amenazas o condiciones que inciden en el desempeño institucional y en la generación de valor público.

Este concepto se adopta en concordancia con lo establecido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, expedida por el Departamento Administrativo de la Función Pública, y se articula con los principios del Modelo Integrado de Planeación y Gestión – MIPG.

La identificación y análisis de los factores de riesgo permite a la Alcaldía de Pasto:

- Comprender las causas reales que originan los riesgos institucionales.
- Diseñar controles preventivos y correctivos más efectivos, enfocados en las fuentes del riesgo y no únicamente en sus efectos.
- Priorizar acciones de mejora en los procesos institucionales.
- Fortalecer la toma de decisiones basada en información objetiva y verificable.
- Contribuir a la transparencia, la integridad institucional y la confianza ciudadana.

En este sentido, la gestión del riesgo no se limita a la identificación de eventos adversos, sino que se orienta a intervenir los factores que incrementan la probabilidad o el impacto del riesgo, promoviendo una cultura organizacional preventiva.

De acuerdo con la Guía de Gestión Integral de Riesgos – Versión 7, los factores de riesgo se clasifican según su naturaleza, así:

Matriz de factores de riesgo – Evaluación conceptual

Factor de riesgo (análisis conceptual)	Definición	Tipo de factor en el mapa de riesgos	Criterio de homologación	Ejemplos de factores de riesgo
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 y errores en las actividades realizadas por los servidores. Incluye la estructura organizacional que afecta la capacidad institucional.	Ejecución y Administración de Procesos	Falta de aplicación de procedimientos; falta de segregación de funciones; errores de grabación, autorización o cálculo; falta de supervisión; insuficiencia o alta rotación de personal; incumplimiento normativo o contractual; deficiencias en capacitación.	Retrasos recurrentes en trámites; reprocesos por errores administrativos; pagos mal liquidados; concentración de funciones críticas en un solo servidor; incumplimiento de tiempos legales; debilidades en la supervisión de procesos.
Transacción u Operación (aplica para LA/FT/FP)	Eventos relacionados con transacciones u operaciones realizadas por un cliente o usuario que accede o entrega bienes o servicios a la entidad, a través de canales específicos y en una jurisdicción determinada.	Fraude Externo y Fraude Interno	Contrapartes de la entidad; productos o servicios ofrecidos o requeridos; canales utilizados; jurisdicciones.	Uso de intermediarios no autorizados; operaciones atípicas de usuarios; transacciones sin soportes suficientes; uso indebido de canales de atención; operaciones en zonas de alto riesgo.
Talento Humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la integridad pública.	Relaciones Laborales	Riesgos asociados a competencias, carga laboral, rotación, ética, clima organizacional; fraude interno; soborno; conflictos de interés;	Incumplimiento del Código de Integridad; conflictos de interés no declarados; baja productividad por sobrecarga laboral; prácticas indebidas en el

			corrupción; hurto de activos.	ejercicio del cargo; uso inadecuado de bienes públicos.
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Fallas Tecnológicas	Daños en equipos; caída de sistemas de información o redes; errores de hardware o software; fallas en programas.	Interrupción de sistemas misionales; pérdida de información; indisponibilidad de plataformas digitales; fallas en aplicativos institucionales; accesos no autorizados por debilidades técnicas.
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Daños a Activos Físicos	Derrumbes; incendios; inundaciones; daños a activos fijos.	Deterioro de edificaciones; suspensión de servicios por daños físicos; pérdida de bienes muebles; afectación de la operación por eventos naturales.
Fraude Externo / Usuarios, Productos y Prácticas Organizacionales (según el caso)	Eventos derivados de situaciones externas que afectan a la entidad.	Fraude Externo o Fraude Usuarios, Productos y Prácticas Organizacionales	Fraude externo; suplantación de identidad; asaltos; atentados; vandalismo; alteración del orden público.	Suplantación de ciudadanos; alteración de documentos; actos vandálicos contra sedes; afectación a la operación por disturbios; estafas a nombre de la entidad.

Nota: La presente matriz se construye exclusivamente con base en la evaluación conceptual suministrada y sirve como ejemplo orientador para la identificación de factores de riesgo.

Un mismo riesgo puede tener un factor de riesgo asociado, el cual actúa como causa que incrementa la probabilidad de ocurrencia o el impacto del riesgo. Por tanto, la adecuada identificación de los factores de riesgo es fundamental para:

- Establecer una relación lógica causa–riesgo–consecuencia.

- Evitar duplicidad de riesgos dentro del mapa institucional.
- Facilitar el seguimiento y monitoreo de los controles implementados.

En el Mapa de Riesgos Integral, los factores de riesgo se registran y clasifican conforme a la tipología establecida, permitiendo un análisis estructurado y homogéneo en todos los procesos de la Alcaldía de Pasto.

La gestión de los factores de riesgo en la Alcaldía de Pasto se orienta bajo un enfoque preventivo y de mejora continua, promoviendo la identificación temprana de condiciones que puedan afectar el logro de los objetivos institucionales y fortaleciendo la capacidad de respuesta ante escenarios adversos.

El adecuado tratamiento de los factores de riesgo contribuye al fortalecimiento de la gobernanza, la gobernabilidad y la confianza ciudadana, en coherencia con los principios de eficiencia, eficacia, transparencia y responsabilidad pública.

6.5.1. FUENTES GENERADORAS DEL FACTOR DE RIESGO.

Las fuentes generadoras del factor de riesgo son las situaciones, condiciones, prácticas, comportamientos, eventos o contextos específicos, de origen interno o externo, que dan lugar a la existencia de un factor de riesgo dentro de los procesos de la Alcaldía de Pasto. Mientras el factor de riesgo representa la categoría o tipo de causa que puede originar un riesgo, las fuentes generadoras corresponden al origen concreto y observable que explica cómo y por qué dicho factor se manifiesta en un proceso determinado.

La identificación adecuada de las fuentes generadoras del factor de riesgo permite a la entidad:

- Comprender con mayor precisión las causas reales y específicas que inciden en la materialización de los riesgos.
- Evitar análisis genéricos o superficiales del riesgo.
- Definir controles focalizados y eficaces, orientados a intervenir la causa raíz.
- Facilitar la formulación de planes de tratamiento del riesgo acordes con la realidad institucional.
- Fortalecer la mejora continua de los procesos y la toma de decisiones informadas.

De esta manera, la gestión del riesgo se orienta no solo a mitigar impactos, sino a prevenir la ocurrencia de eventos adversos desde su origen.
Las fuentes generadoras del factor de riesgo pueden clasificarse, de manera general, en internas y externas, sin perjuicio de que un mismo riesgo pueda verse influenciado por ambas.

a. **Fuentes internas:** Son aquellas que se originan al interior de la Alcaldía de Pasto y están asociadas a:

- Debilidades en el diseño, ejecución o seguimiento de los procesos.
- Falta de claridad en roles, responsabilidades o procedimientos.
- Insuficiencia de competencias, capacitación o disponibilidad del talento humano.
- Deficiencias en los sistemas de información o herramientas tecnológicas.
- Prácticas organizacionales inadecuadas o no documentadas.
- Limitaciones en la infraestructura física o tecnológica.

Estas fuentes son, en general, susceptibles de intervención directa por parte de la entidad, mediante acciones de mejora, controles y ajustes en la gestión institucional.

b. **Fuentes externas:** Son aquellas que se originan fuera del ámbito de control directo de la entidad, pero que pueden influir en el cumplimiento de sus objetivos, tales como:

- Cambios normativos o regulatorios.
- Actuaciones de terceros (contratistas, proveedores, operadores externos).
- Factores sociales, económicos, políticos o ambientales.
- Eventos naturales o situaciones de orden público.
- Exigencias de entes de control u organismos externos.

Estas fuentes requieren mecanismos de monitoreo permanente y estrategias de mitigación que permitan reducir su impacto o anticipar sus efectos.
La gestión integral del riesgo se fundamenta en la comprensión de la siguiente secuencia lógica:

Fuente generadora → Factor de riesgo → Riesgo → Consecuencia

- La fuente generadora explica el origen específico del problema.
- El factor de riesgo clasifica la naturaleza de la causa.
- El riesgo es el evento potencial que puede afectar el logro de los objetivos.
- La consecuencia representa el impacto sobre la entidad.

Esta relación permite estructurar de manera coherente el Mapa de Riesgos Integral y facilita la identificación de controles adecuados y medibles.

7. CONTENIDO

7.1. CONTEXTO DE LA ENTIDAD

La Alcaldía de Pasto tiene como objetivo mejorar la calidad de vida de los ciudadanos, impulsar el desarrollo económico y social de la región y garantizar la prestación efectiva de servicios esenciales para la comunidad. Sin embargo, este compromiso se desenvuelve en un entorno cambiante y en constante evolución, caracterizado por modificaciones legislativas, necesidades de la población, recursos limitados y una competencia creciente entre municipios por atraer inversiones y generar oportunidades. Por lo tanto, la entidad establece su contexto a través del análisis DOFA institucional, que permite desglosar y examinar de manera estructurada los elementos internos y externos que influyen en la Alcaldía de Pasto. Se exploran las Debilidades que son áreas internas que requieren mejoras para lograr un desempeño óptimo; las Fortalezas como atributos y capacidades internas que la Alcaldía puede aprovechar para destacar su gestión. Así mismo, se identifican las Oportunidades que son condiciones externas positivas que pueden ser explotadas para beneficio del municipio y finalmente las Amenazas que son factores externos que podrían impactar negativamente a la entidad si no se abordan de manera adecuada.

Para su consulta, el contexto de la Alcaldía de Pasto se encuentra publicado en el siguiente enlace:
https://www.intranetpasto.gov.co/index.php/descargas?download=9549:dofa-institucional-v2

7.2. MODELO DE OPERACIÓN POR PROCESOS

La Alcaldía de Pasto para efectos de la administración del modelo integrado de planeación y gestión - MIPG y con el objetivo de atender las necesidades y garantizar los derechos de la ciudadanía y/o grupos de valor, establece la gestión por procesos, a través de la cual se estandarizan las operaciones de la entidad que interactúan y se consolidan por tipo de proceso, siendo los siguientes: Procesos Misionales, Procesos de Apoyo, Procesos Estratégicos y Procesos de Evaluación y como resultado se genera la cadena de valor y se representa a través del mapa de procesos.
Actualmente, la Alcaldía de Pasto cuenta con 29 procesos que interactúan para garantizar las necesidades, problemas y derechos de la ciudadanía y grupos de valor, y a medida que se incrementen las necesidades y/o cambien los objetivos institucionales, se requerirá la modificación del número vigente de procesos.

Para su consulta, el mapa de procesos de la Alcaldía de Pasto se encuentra publicado en el siguiente enlace:
https://www.intranetpasto.gov.co/index.php/sistemas-de/de-calidad

Para el caso de la Alcaldía de Pasto el Comité Institucional de Gestión y Desempeño es presidido por el Alcalde y está constituido por: el Secretario General, Secretario de

Hacienda, Secretario de Desarrollo Comunitario, Subsecretario de Sistemas de Información, Subsecretario de Talento Humano, Subsecretario de Apoyo Logístico, Subsecretario de Participación, Jefe de la Oficina de Planeación de Gestión Institucional, Jefe de la Oficina Asesora Jurídica de Despacho, Jefe de la Oficina de Comunicación Social, Jefe de Oficina de Archivo y Gestión Documental y Director del Departamento Administrativo de Contratación. La Oficina de Control Interno de Gestión es invitado permanente, con voz, pero sin voto y la Secretaría Técnica es ejercida por el/la jefe de la Oficina de Planeación de Gestión Institucional.

El Comité Institucional de Coordinación de Control Interno es presidido por el alcalde e integrado por: el jefe de la Oficina de Planeación de Gestión Institucional, jefe de Presupuesto, secretario de Gobierno Municipal, secretario general, jefe de la Oficina Asesora Jurídica de Despacho y el delegado del alcalde para la implementación del MECI. La secretaría técnica está a cargo del jefe de Control Interno de Gestión, con voz, pero sin voto.

Para su consulta, los decretos de constitución de cada comité de la Alcaldía de Pasto y las diferentes acciones y/o funciones que cumplen se encuentran publicados en el siguiente enlace: *https://www.intranetpasto.gov.co/index.php/sistemas-de/mipg*

7.3. POLÍTICAS MIPG ALINEADAS A LA GESTIÓN INTEGRAL DE RIESGO

Las políticas que hacen parte del Modelo Integrado de Planeación y Gestión – MIPG se articulan de manera transversal con la gestión integral del riesgo, en tanto permiten **identificar, analizar, evaluar y tratar los eventos** que pueden afectar el logro de los objetivos institucionales y la generación de valor público. Desde la política de planeación institucional, la gestión del riesgo orienta la definición de la ruta estratégica y operativa de la entidad, considerando las necesidades de los grupos de valor, el entorno y los recursos disponibles. A su vez, las políticas de gestión presupuestal, eficiencia del gasto público y compras y contratación pública incorporan la gestión del riesgo para asegurar el uso eficiente, transparente y oportuno de los recursos, mitigando riesgos financieros, contractuales y de corrupción. La política de fortalecimiento organizacional y simplificación de procesos integra el enfoque de riesgo para optimizar procesos, mejorar la eficiencia administrativa y la calidad del servicio, mientras que la política de servicio al ciudadano gestiona los riesgos que puedan afectar el acceso efectivo y oportuno a los derechos de la ciudadanía. De igual manera, la política de seguridad digital aborda los riesgos asociados al entorno tecnológico y digital, fortaleciendo la resiliencia institucional, y la política de transparencia, acceso a la información y lucha contra la corrupción se enfoca en la prevención, detección y tratamiento de riesgos que afecten la probidad, la rendición de cuentas y la confianza ciudadana. La política de integridad promueve la identificación y gestión de riesgos éticos y de conflictos de interés, asegurando comportamientos alineados con el interés general. Finalmente, las políticas de seguimiento y evaluación del desempeño

institucional y de control interno permiten monitorear los riesgos a través de indicadores, generar alertas tempranas, fortalecer los controles y apoyar la toma de decisiones, garantizando que el sistema de gestión y control contribuya efectivamente al cumplimiento de los objetivos estratégicos y misionales de la entidad.

Política	Descripción
Planeación Institucional	Define la ruta estratégica y operativa
Gestión Presupuestal y Eficiencia del Gasto Público	Utiliza los recursos de manera apropiada
Fortalecimiento Organizacional y Simplificación de Procesos	Fortalece las capacidades organizacionales
Servicio al Ciudadano	Garantiza el acceso efectivo y de calidad
Seguridad Digital	Fortalece las capacidades para gestionar riesgos
Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción	Articula acciones para prevenir y detectar riesgos
Integridad	Institucionaliza la cultura de integridad
Seguimiento y Evaluación del Desempeño Institucional	Formula indicadores para medir la gestión
Control Interno	Promueve un ambiente de control adecuado

7.4. POLÍTICA DE GESTIÓN INTEGRAL DE RIESGOS

La Alcaldía de Pasto reconoce que el logro de sus objetivos, la ejecución del Plan de Desarrollo Municipal, la correcta administración de los recursos públicos y la confianza de la ciudadanía dependen de una adecuada gestión de los riesgos que puedan afectar su desempeño institucional.

Por esta razón, la Alta Dirección establece la siguiente Política de Administración del Riesgo, como una directriz obligatoria para todas las dependencias y servidores públicos, orientada a fortalecer la planeación, el control, la transparencia, la integridad y la toma de decisiones en la administración municipal.

> *"La Alcaldía de Pasto se compromete a gestionar sus riesgos de manera integral, proactiva y transparente, como una estrategia fundamental para proteger el patrimonio público, asegurar la integridad de sus servidores y garantizar el cumplimiento de las metas del Plan de Desarrollo Municipal. La gestión del riesgo no es un ejercicio administrativo aislado, sino una capacidad institucional que facilita la toma de decisiones basada en evidencia y el fortalecimiento de la confianza ciudadana, implementando controles preventivos, detectivos y correctivos, así como planes de tratamiento y acciones de mejora, con el fin de reducir la probabilidad de ocurrencia de los riesgos, mitigar sus impactos y mantenerlos dentro de los niveles de tolerancia definidos por la entidad, protegiendo los recursos públicos, la integridad institucional y la confianza de la ciudadanía."*

La Alta Dirección asume un rol activo en la gestión integral del riesgo, estableciendo el "tono desde la cima" y promoviendo una cultura organizacional basada en la prevención, la integridad y la responsabilidad frente al riesgo. La gestión del riesgo se concibe como un insumo estratégico para la toma de decisiones, la priorización de recursos y el seguimiento al desempeño institucional.

Lineamientos de la Política:

- **Cultura de Prevención:** Todos los servidores y contratistas son responsables de identificar y reportar riesgos en sus procesos.
- **Apetito al Riesgo:** La entidad priorizará el tratamiento de riesgos cuya valoración residual sea Alta o Extrema.
- **Integridad Institucional:** Se dará prioridad absoluta a la prevención de riesgos de corrupción y fraude mediante el SIGRIP.
- **Mejora Continua:** Los mapas de riesgos se actualizarán ante cambios en el entorno o cada vez que se materialice un riesgo, asegurando el aprendizaje organizacional.

- **Transparencia:** La información sobre los riesgos y su gestión será pública, fomentando el control social.

7.4.1. Objetivo de la Política de Gestión Integral de Riesgos – Alcaldía de Pasto

La gestión integral de riesgos constituye un elemento transversal de la planeación, la ejecución y el control de la gestión pública, en tanto permite anticipar, prevenir y responder de manera oportuna a los eventos que pueden afectar el cumplimiento de los objetivos institucionales y la generación de valor público. En este sentido, la Alcaldía de Pasto reconoce la importancia de consolidar un enfoque sistemático y articulado de gestión del riesgo, integrado a la estrategia, el desempeño institucional y la toma de decisiones, como base para fortalecer la gobernanza, proteger los recursos públicos y asegurar el cumplimiento del Plan de Desarrollo Municipal.

***OBJETIVO DE LA POLITICA**: Establecer y fortalecer la gestión integral de riesgos en la Alcaldía de Pasto, mediante la adopción de lineamientos, responsabilidades y prácticas sistemáticas que permitan identificar, analizar, evaluar, tratar, hacer seguimiento y controlar los riesgos estratégicos, operativos, fiscales, de integridad y corrupción, de contratación y de seguridad de la información, en todos los niveles de la entidad, con el propósito de disminuir la vulnerabilidad institucional, asegurar el cumplimiento de los objetivos misionales, estratégicos y del Plan de Desarrollo Municipal, proteger los recursos públicos, fortalecer la integridad institucional y generar confianza en la ciudadanía.*

7.4.2. Alcance de la política de gestión integral del riesgo

Con el fin de garantizar una aplicación efectiva y coherente de la gestión integral de riesgos, resulta necesario definir de manera clara el ámbito de cobertura de la política, asegurando que sus lineamientos sean aplicados de forma transversal en toda la organización. La delimitación del alcance permite incorporar no solo los procesos y actividades desarrollados directamente por la entidad, sino también aquellos que, por su naturaleza o modalidad de ejecución, involucran actores externos y pueden generar riesgos críticos que afecten el logro de los objetivos institucionales, la prestación de los servicios y la confianza de la ciudadanía.

***ALCANCE DE LA POLITICA:** La Política de Gestión Integral de Riesgos de la Alcaldía de Pasto aplica a todos los procesos, programas, planes, proyectos y actividades de la entidad, en sus niveles estratégico, misional, de apoyo y de evaluación, y es de obligatorio cumplimiento para la Alta Dirección, servidores públicos y contratistas. De acuerdo con la naturaleza y misionalidad de la entidad, el alcance de la política incluye igualmente a las unidades descentralizadas, así como a los procesos, programas o proyectos tercerizados, ejecutados por particulares u otras entidades públicas a través de contratos, convenios o cualquier otra modalidad de asociación, en los cuales la Alcaldía de Pasto conserve responsabilidades de dirección, supervisión o control. En estos casos, la entidad analizará y gestionará los riesgos que puedan generarse por la operación externa, estableciendo*

acciones de seguimiento, controles y mecanismos de articulación, con el fin de prevenir, mitigar y controlar riesgos críticos que puedan afectar el cumplimiento de los objetivos institucionales, el Plan de Desarrollo Municipal, la adecuada prestación de los servicios, la protección de los recursos públicos y la confianza de la ciudadanía.

7.5. METODOLOGÍA PARA LA GESTIÓN INTEGRAL DEL RIESGO

Para la actualización del presente Manual de Gestión Integral del Riesgo, la Alcaldía de Pasto adopta la metodología definida por el Departamento Administrativo de la Función Pública (DAFP) en la Guía de Gestión Integral del Riesgo – Versión 7, la cual se fundamenta en el conocimiento del contexto institucional, la misión, la visión, los objetivos estratégicos y el modelo de operación por procesos de la entidad. A partir de este reconocimiento, la gestión del riesgo se desarrolla de manera integral y sistemática, mediante la definición de la Política de Administración del Riesgo, la identificación, análisis y evaluación de los riesgos, la determinación e implementación de controles, la definición de planes de tratamiento, el establecimiento de indicadores de riesgo y el seguimiento permanente a su comportamiento.

De manera transversal, la entidad implementa estrategias de comunicación, sensibilización y apropiación dirigidas a todos los servidores públicos y contratistas, con el fin de fortalecer la cultura de gestión del riesgo y asegurar que esta se convierta en una herramienta efectiva para la toma de decisiones, la prevención de eventos adversos y la mejora continua de la gestión institucional.

La gestión del riesgo en la Alcaldía de Pasto se desarrollará de manera sistemática, siguiendo los pasos que se describen a continuación:

Paso 1. Contexto Estratégico y Definición de Objetivos
La gestión del riesgo en la Alcaldía de Pasto inicia con el entendimiento de qué queremos lograr. Antes de identificar riesgos, cada dependencia debe tener total claridad sobre sus objetivos, ya que un riesgo es, por definición, cualquier evento que pueda impedir, retrasar o afectar la consecución de estos.
Este paso asegura que los riesgos identificados estén alineados con:

- El Plan de Desarrollo Municipal (Nivel Estratégico).
- El Mapa de Procesos y Procedimientos (Nivel Operativo).
- Los Planes de Acción Anuales (Nivel de Gestión).

Para cada proceso bajo su cargo, usted debe transcribir el objetivo tal como aparece en el Mapa de Procesos de la entidad. Si el objetivo no es claro, el riesgo será difícil de

medir. Un buen objetivo debe responder a: ¿Qué hacemos?, ¿Cómo lo hacemos? y ¿Para qué lo hacemos?

Ejemplo:
Proceso: Planeación Estratégica
Objetivo del Proceso: "*Orientar el ciclo de la gestión pública territorial mediante la formulación, seguimiento y evaluación del Plan de Desarrollo Municipal, asegurando la articulación de los recursos y la participación ciudadana, para fortalecer la gobernanza y legitimidad de la Alcaldía de Pasto.*"

Paso 2. Identificación de riesgos
Identificar un riesgo es detectar los eventos que pueden impedir el cumplimiento de los objetivos definidos en el Paso 1. Un riesgo no es un hecho que ya pasó (un problema), sino la posibilidad de que algo ocurra en el futuro.

A. *Identificación de Factores de Riesgo (¿Dónde nace la debilidad?)*
Antes de redactar, identifique la fuente o el área donde se origina la debilidad, los factores son:

- Talento Humano: Fallas en las personas (ética, competencias, carga laboral).
- Procesos: Diseño deficiente de manuales o procedimientos.
- Tecnología: Fallas en software, hardware o redes informáticas.
- Infraestructura: Daños físicos en el edificio o muebles.
- Evento Externo: Situaciones ajenas (clima, orden público, cambios de ley).

B. *Estructura Obligatoria de Redacción*
Para que el riesgo sea válido, DEBE seguir esta fórmula exacta:

POSIBILIDAD DE + [Impacto] + por + [Causa Inmediata] + debido a/a causa de + [Causa Raíz]

- Impacto (¿Qué se daña?): Es la consecuencia negativa (económica o reputacional).
- Causa Inmediata (¿Cómo pasa?): La situación más evidente que dispara el riesgo.
- Causa Raíz (¿Por qué pasa?): El origen profundo del problema que debemos atacar con controles.

a. Redactar un riesgo NO es, escribir un problema actual, Escribir una debilidad, Escribir una queja, Escribir una actividad mal hecha
b. Redactar un riesgo SÍ es, describir algo que PUEDE pasar y que afectaría el logro de un objetivo

Antes de escribir un riesgo, pregúntese:

- ¿Esto puede pasar o ya está pasando?
- ¿Afecta un objetivo del proceso?
- ¿Puedo identificar claramente causa y consecuencia?

Si responde sí a las tres → está bien redactado.

Reglas de Oro para la Identificación
-NO redactar riesgos como la negación de un control: Evite decir "No hay cámaras". Lo correcto es "Debido a la debilidad en la vigilancia".
-NO usar hechos consumados: Evite decir "El sistema falló". Diga "Posibilidad de falla en el sistema".
- NO confundir Causa con Riesgo: "La falta de personal" es una causa raíz, no un riesgo. El riesgo es lo que sucede por esa falta de personal (ej: retraso en los pagos).

Ejemplo:
Proceso: Planeación Estratégica.
Factor de Riesgo: Ejecución y Administración de Procesos.
Fuente Generadora: Falta de aplicación de los procedimientos.
Riesgo: Posibilidad de afectación reputacional y pérdida de confianza ciudadana **por** el incumplimiento en el seguimiento al Plan de Desarrollo Municipal **debido a** la falta de una plataforma articulada para el reporte de información por parte de las dependencias.

Paso 3. Evaluación de la probabilidad
Una vez identificados y redactados los riesgos, deberá evaluar la probabilidad, entendida como la posibilidad de que el riesgo ocurra en un periodo de tiempo determinado. La evaluación de la probabilidad no corresponde a una apreciación subjetiva, sino a un análisis basado en la experiencia del proceso, los antecedentes institucionales, la frecuencia con la que se han presentado situaciones similares y las condiciones actuales del entorno interno y externo.

Se deberá estimar qué tan posible es que el riesgo ocurra, utilizando una escala cualitativa (muy baja, baja, media, alta o muy alta), de acuerdo con la experiencia, los datos disponibles y el contexto institucional. No es una apreciación subjetiva basada en el pasado, sino un análisis de la exposición; es decir, qué tan seguido se ejecuta la actividad que puede generar el riesgo durante un año. Si una actividad se realiza miles de veces, el riesgo tiene muchas más oportunidades de aparecer que si solo se realiza una vez al año.

1. Criterios para Definir el Nivel de Probabilidad
La Alcaldía de Pasto adopta la tabla de frecuencias oficial de la Guía V7. Los líderes de proceso deben contar cuántas veces al año se pasa por el "punto de riesgo":

Probabilidad	Frecuencia de la Actividad (Al año)	Porcentaje de Exposición
Muy Baja	La actividad se ejecuta máximo 2 veces por año.	20%
Baja	La actividad se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad se ejecuta de 25 a 500 veces por año.	60%
Alta	La actividad se ejecuta de 501 a 5.000 veces por año.	80%
Muy Alta	La actividad se ejecuta más de 5.000 veces por año.	100%

2. Regla de Aplicación Técnica
Para asignar el nivel, el líder del proceso debe revisar sus manuales de procedimientos y registros. Por ejemplo:

- Planeación Estratégica: Se hace 1 vez al año → Muy Baja.
- Contratación: Si se firman 300 contratos al año → Media.
- Tesorería/Pagos: Si se hacen pagos diarios → Muy Alta.

Ejemplo:
Riesgo Identificado: Posibilidad de afectación reputacional y pérdida de confianza ciudadana **por** el incumplimiento en el seguimiento al Plan de Desarrollo Municipal **debido a** la falta de una plataforma articulada de reporte.
Punto de Riesgo: Consolidación de informes de metas de las dependencias.
Análisis de Frecuencia: Esta actividad se realiza de manera trimestral (4 veces al año) para el Comité de Gestión y Desempeño.
Resultado de Probabilidad: De acuerdo con la tabla de frecuencia, al realizarse 4 veces al año, se asigna una probabilidad **BAJA (40%)**.

Paso 4. Evaluación del impacto
Una vez determinada la probabilidad de ocurrencia del riesgo, deberá evaluar el impacto, entendido como la magnitud de las consecuencias que tendría el riesgo en caso de materializarse.

El impacto se define como las consecuencias que puede ocasionar a la Alcaldía de Pasto la materialización de un riesgo. Para facilitar el análisis y eliminar la subjetividad, la Guía Versión 7 agrupa todas las afectaciones (legales, operativas o sociales) en dos variables principales: **Impacto Económico** e **Impacto Reputacional**. Se deberá estimar qué tan grave sería el efecto del riesgo en caso de que ocurra, considerando impactos financieros, legales, operativos, reputacionales o sobre la ciudadanía.

1. Criterios para Definir el Nivel de Impacto
Cuando un riesgo presente ambos tipos de impacto, se debe tomar siempre el nivel más alto entre los dos para la calificación final.

Nivel de Impacto	Afectación Económica (Presupuestal)	Afectación Reputacional (Imagen)	Porcentaje
Leve	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de solo un área específica de la entidad.	20%
Menor	Entre 10 SMLMV y 50 SMLMV.	Afecta la imagen a nivel interno, junta directiva, accionistas o proveedores.	40%
Moderado	Entre 50 SMLMV y 100 SMLMV.	Afecta la imagen ante algunos usuarios relevantes para el logro de objetivos.	60%
Mayor	Entre 100 SMLMV y 500 SMLMV.	Efecto publicitario sostenido a nivel departamental o municipal.	80%
Catastrófico	Mayor a 500 SMLMV.	Afecta la imagen a nivel nacional con efecto publicitario sostenido en todo el país.	100%

2. Regla de Aplicación Técnica

Los líderes de proceso deben cuantificar el posible daño.

- Si es un riesgo Fiscal, el impacto siempre será económico.
- Si es un riesgo de Gestión o Seguridad, puede ser mayoritariamente reputacional o una mezcla de ambos.

Ejemplo:
Riesgo Identificado: Posibilidad de afectación reputacional y pérdida de confianza ciudadana **por** el incumplimiento en el seguimiento al Plan de Desarrollo Municipal **debido a** la falta de una plataforma articulada para el reporte de información por parte de las dependencias.
Probabilidad (Paso 3): Baja (40%)
Impacto (Paso 4): Mayor (80%)
Análisis de Severidad: Al cruzar una Probabilidad **Baja (40%)** con un Impacto **Mayor (80%)**, el Riesgo Inherente se ubica en la zona **NARANJA**, lo que equivale a un nivel de riesgo **ALTO**

Paso 5. Nivel de riesgo inherente

Una vez evaluada la probabilidad (Paso 3) y el impacto (Paso 4) de cada riesgo, la deberá determinar el nivel de riesgo inherente, entendido como el nivel de exposición al riesgo antes de considerar la aplicación de controles.

El Riesgo Inherente es el nivel de exposición al riesgo que tiene un proceso por su propia naturaleza, antes de aplicar cualquier control para mitigarlo. Este nivel permite a la Alcaldía de Pasto priorizar sus esfuerzos y recursos en los eventos que representan la mayor amenaza para el cumplimiento del Plan de Desarrollo Municipal y la generación de valor público. Se obtiene al combinar la probabilidad y el impacto, lo que permite clasificar el riesgo como bajo, medio, alto o crítico antes de aplicar controles.

1. Matriz de Calor (Niveles de Severidad)

La Alcaldía de Pasto adopta la matriz de calor oficial de la Función Pública, la cual combina los resultados de Probabilidad (Paso 3) e Impacto (Paso 4) para ubicar el riesgo en una de las cuatro (4) zonas de severidad:

- Zona Verde (Bajo): Riesgos con baja exposición que requieren monitoreo básico.
- Zona Amarilla (Moderado): Riesgos que exigen seguimiento periódico y revisión de controles.
- Zona Naranja (Alta): Riesgos críticos que requieren acciones de tratamiento inmediatas.
- Zona Roja (Extremo): Riesgos inaceptables que demandan la atención prioritaria de la Alta Dirección.

2. Regla de Aplicación Técnica

Para determinar el nivel, se debe cruzar el porcentaje de Probabilidad (eje vertical) con el porcentaje de Impacto (eje horizontal). Esta ubicación exacta en la matriz define el "punto de partida" de la gestión del riesgo.

Ejemplo:

Riesgo: Posibilidad de afectación reputacional y pérdida de confianza ciudadana **por** el incumplimiento en el seguimiento al Plan de Desarrollo Municipal **debido a** la falta de una plataforma articulada para el reporte de información por parte de las dependencias.
Probabilidad (Paso 3): Baja (40%).
Impacto (Paso 4): Mayor (80%).
Cálculo del Riesgo Inherente: Al cruzar una Probabilidad **Baja (40%)** con un Impacto **Mayor (80%)**, el Riesgo Inherente se ubica en la zona **NARANJA** de la matriz.
Resultado: El nivel de severidad es **ALTO**. Esto indica que el riesgo es crítico y la dependencia debe proceder obligatoriamente al diseño y valoración de controles para intentar reducir esta severidad hacia la zona verde.

Paso 6. Identificación de controles

Una vez determinado el nivel de riesgo inherente, la Alcaldía de Pasto deberá identificar los controles existentes, en las actividades de control que son acciones concretas, establecidas mediante políticas, procedimientos o directrices institucionales, implementadas para proporcionar una seguridad razonable frente al cumplimiento de los objetivos. Estos controles deben atacar directamente la Causa Raíz identificada en el Paso 2 para ser efectivos.

1. Estructura Obligatoria para la Redacción de Controles

Para que un control sea válido y pueda ser evaluado, debe redactarse siguiendo esta fórmula:

Responsable (Cargo) + Acción (Verbo fuerte) + Complemento (¿Cómo y dónde?)

- Responsable: El cargo de quien ejecuta el control (ej. Jefe de Oficina, Analista).
- Acción: Verbos que indiquen verificación (ej. Verificar, validar, conciliar, cotejar).

- Complemento: Detalles informativos como la fuente, la periodicidad y el soporte documental.

2. Tipologías de Controles (¿Cuándo actúan?)
La Alcaldía de Pasto clasificará los controles según el momento de su ejecución en la cadena de valor:

- Preventivo: Actúa antes de que el riesgo ocurra para evitar la causa raíz.
- Detectivo: Actúa durante la ejecución para identificar desviaciones y errores (genera reprocesos).
- Correctivo: Actúa después de que el riesgo se materialice para mitigar el daño (p. ej., pólizas o backups).

La Alcaldía de Pasto podrá identificar, entre otros, los siguientes tipos de controles:

- Controles administrativos: lineamientos, políticas, manuales, procedimientos y resoluciones.
- Controles operativos: actividades de revisión, validación, seguimiento y supervisión.
- Controles tecnológicos: sistemas de información, plataformas digitales, alertas automáticas y respaldos de información.
- Controles de supervisión: comités, informes periódicos y revisiones por instancias directivas.

Al identificar los controles asociados a cada riesgo, los líderes de proceso deberán tener en cuenta:

- Si el control existe actualmente.
- Si el control está documentado.
- Quién es el responsable de aplicarlo.
- Con qué frecuencia se aplica.

Ejemplo:
Riesgo: Posibilidad de afectación reputacional y pérdida de confianza ciudadana por el incumplimiento en el seguimiento al Plan de Desarrollo Municipal debido a la falta de una plataforma articulada para el reporte de información.
Control Existente 1 (Preventivo): El Líder de Planeación Estratégica (responsable) valida (Acción) mensualmente el cargue de información en los formatos PE-F-022 y PE-F-030 por parte de las dependencias, según el cronograma institucional de seguimiento (Complemento).
Control Existente 2 (Detectivo): El Comité Institucional de Gestión y Desempeño (responsable) coteja (Acción) los resultados consolidados en el Tablero de Control PE-F-024 frente a las

evidencias físicas reportadas por los secretarios de despacho al cierre de cada trimestre (Complemento).

Paso 7. Evaluación de la efectividad de los controles

Una vez identificados los controles existentes, deberá evaluar su efectividad, con el fin de determinar si dichos controles realmente contribuyen a prevenir, detectar o corregir la materialización de los riesgos identificados. La valoración de controles consiste en medir técnicamente qué tanta seguridad ofrece las acciones identificadas en el Paso 6 para mitigar el riesgo. Un control no es efectivo solo porque "exista", sino por **cómo fue diseñado** y **cómo se ejecuta**. El resultado de esta evaluación restará valor a la severidad del Riesgo Inherente.

1. Criterios de Calificación (Atributos de Eficiencia)

La Alcaldía de Pasto adopta la tabla de pesos oficiales de la Función Pública para calificar la eficiencia de cada control:

Atributo	Criterio de Calificación	Peso
Tipo de Control	**Preventivo:** Ataca la causa antes de que el riesgo ocurra.	**25%**
	Detectivo: Identifica el error durante el proceso.	**15%**
	Correctivo: Mitiga el daño después de ocurrido.	**10%**
Implementación	**Automático:** Lo hace un sistema o software sin intervención humana.	**25%**
	Manual: Lo ejecuta una persona directamente.	**15%**

2. Análisis de Formalización (Atributos Obligatorios)

Además del peso anterior, el líder de proceso debe validar que el control cumpla con estos 4 requisitos para ser válido:

- Documentación: El control está en un manual o procedimiento oficial.
- Frecuencia: Se ejecuta de forma periódica o cada vez que ocurre la actividad.
- Evidencia: Deja un rastro o soporte (físico o digital) de su ejecución.
- Ejecución: Se utiliza información confiable (interna o externa) para la revisión.

Un control puede existir en el papel, pero no ser efectivo si no se aplica o si no logra reducir el riesgo.

Para evaluar cada control, los líderes de proceso deberán analizar los siguientes aspectos:

- Existencia: el control está definido y formalizado.
- Documentación: el control se encuentra descrito en manuales, procedimientos o lineamientos.
- Aplicación: el control se ejecuta en la práctica y no solo de manera formal.

- Efectividad: el control reduce la probabilidad o el impacto del riesgo.

Con base en los criterios anteriores, la efectividad de los controles podrá clasificarse de la siguiente manera:

- Alta: el control existe, está documentado, se aplica de manera consistente y reduce significativamente el riesgo.
- Media: el control existe y se aplica, pero presenta debilidades o no siempre se ejecuta de manera uniforme.
- Baja: el control existe solo de forma parcial, no se aplica de manera constante o no logra reducir el riesgo.

Ejemplo:

- **Riesgo:** Posibilidad de afectación reputacional y pérdida de confianza ciudadana por el incumplimiento en el seguimiento al Plan de Desarrollo Municipal debido a la falta de una plataforma articulada para el reporte de información.
- **Valoración del Control 1:** "El Líder de Planeación valida mensualmente el cargue de información en los formatos PE-F-022 y PE-F-030".
  - **Tipo:** Preventivo (25%).
  - **Implementación:** Manual (15%).
  - **Puntaje Total Control 1: 40%**.
- **Valoración del Control 2:** "El Comité de Gestión coteja los resultados consolidados frente a evidencias físicas".
  - **Tipo:** Detectivo (15%).
  - **Implementación:** Manual (15%).
  - **Puntaje Total Control 2: 30%**.

Paso 8. Riesgo residual

Una vez evaluada la efectividad de los controles existentes, deberá determinar el riesgo residual. El Riesgo Residual es el nivel de exposición que permanece una vez aplicada la efectividad de los controles existentes al Riesgo Inherente. Este paso permite a la Alcaldía de Pasto identificar la exposición real y decidir si el nivel de riesgo actual es aceptable o si se requieren acciones de tratamiento adicionales.

1. Aplicación Acumulativa de Controles

Los controles mitigan el riesgo de forma acumulativa. Esto significa que el primer control reduce el riesgo inicial, y el segundo control se aplica sobre el valor que quedó del primero, logrando un desplazamiento real en la matriz de calor.

- Controles Preventivos y Detectivos: Atacan y reducen la Probabilidad.

- Controles Correctivos: Atacan y reducen el Impacto.

2. Clasificación del Riesgo Residual
El resultado final ubicará el riesgo en una nueva posición en la Matriz de Calor:

- Zona Verde (Bajo): Riesgo controlado. Se acepta y se monitorea. Riesgo controlado adecuadamente, sin necesidad de acciones adicionales significativas.
- Zona Amarilla (Moderado): Riesgo tolerable. Requiere seguimiento periódico.
- Zona Naranja (Alta): Riesgo no aceptable. Obliga a definir nuevos controles o planes de acción. Riesgo que requiere la definición de acciones de tratamiento.
- Zona Roja (Extremo): Riesgo crítico. Requiere intervención inmediata de la Alta Dirección.

Ejemplo:
Riesgo: Posibilidad de afectación reputacional por el incumplimiento en el seguimiento al Plan de Desarrollo Municipal debido a la falta de una plataforma articulada.
Riesgo Inherente (Paso 5): ALTO (Probabilidad 40% / Impacto 80%).
Aplicación de Controles (Paso 7): ***Control 1 (Preventivo - 40%):*** Reduce la probabilidad inicial de 40% a 24% (40% x 40% =16%; 40% - 16% = 24%). ***Control 2 (Detectivo - 30%):*** Se aplica sobre el nuevo valor (24%). Reduce la probabilidad a 16.8% (24% x 30% = 7.2%; 24% - 7.2% = 16.8%).
Resultado del Riesgo Residual: Con una nueva probabilidad de 16.8% (Muy Baja) y un impacto que se mantiene en 80% (Mayor), el riesgo se desplaza a la ZONA AMARILLA.
Nivel Final: RIESGO RESIDUAL MODERADO.

Paso 9. Plan de tratamiento del riesgo
Una vez determinado el nivel de riesgo residual, deberá definir el plan de tratamiento del riesgo, El Plan de Tratamiento es el conjunto de acciones seleccionadas para modificar el riesgo residual cuando este supera los límites de tolerancia o el apetito al riesgo definido por la Alcaldía de Pasto. Se aplica obligatoriamente a los riesgos con nivel **Alto** o **Extremo (Crítico)**, con el fin de reducir su probabilidad, mitigar su impacto o ambos. El plan de tratamiento se aplica principalmente a los riesgos cuyo nivel residual sea alto o crítico, y constituye una herramienta clave para fortalecer la gestión institucional y prevenir la materialización de eventos adversos.

1. Opciones de Tratamiento
De acuerdo con la metodología oficial, la dependencia debe seleccionar una o varias de las siguientes estrategias para gestionar el riesgo sobrante:

- Reducir: Implementar nuevos controles o mejorar los existentes para disminuir la probabilidad o el impacto. Es la opción más común en la gestión pública.
- Evitar: Decidir no iniciar o continuar con la actividad que origina el riesgo (por ejemplo, eliminar un activo o proceso que genera demasiada vulnerabilidad).

- Compartir: Distribuir el riesgo con terceros a través de contratos, seguros, convenios o pólizas de cumplimiento.
- Aceptar: No tomar acciones adicionales cuando el nivel de riesgo está dentro del "Apetito al Riesgo" establecido por la Alta Dirección, manteniendo un monitoreo permanente.

2. Requisitos del Plan de Acción
Cada acción de tratamiento debe estar debidamente documentada en la matriz institucional, especificando:

- Tratamiento: La opción seleccionada (Reducir, Evitar, etc.).
- Plan de Acción: Descripción detallada de la nueva medida a implementar.
- Responsable: Cargo específico encargado de la ejecución.
- Fecha de Implementación: Plazo máximo para la ejecución de la acción.
- Seguimiento: Periodicidad con la que se revisará el avance (mensual, trimestral).

Ejemplo:
Riesgo: Posibilidad de afectación reputacional por el incumplimiento en el seguimiento al Plan de Desarrollo Municipal debido a la falta de una plataforma articulada.
Riesgo Residual (Paso 8): MODERADO (Zona Amarilla).
Decisión: Aunque es moderado, la Alcaldía de Pasto decide **REDUCIR** el riesgo para llevarlo a la zona verde.

Tratamiento	Plan de Acción	Responsable	Fecha Implementación	Seguimiento
Reducir	Diseño y puesta en marcha de un Dashboard automatizado para el reporte en tiempo real de metas.	Jefe de la OPGI / Oficina de TIC	30 de junio de 2026	Mensual
Reducir	Actualización del Manual de Seguimiento incorporando sanciones administrativas por mora en reportes.	Secretario de Planeación	30 de agosto de 2026	Trimestral
Aceptar	Monitoreo trimestral de las alertas generadas por el sistema actual mientras se implementa el nuevo.	Líder de proceso	Permanente	Semestral

Paso 10. Indicadores de riesgo (KRI)
Los KRI (Key Risk Indicators) son métricas diseñadas para anticipar la materialización de un riesgo. A diferencia de los indicadores de gestión (que miden resultados pasados), los indicadores de riesgo miden la exposición actual. Su función principal en la Alcaldía de Pasto es actuar como un "velocímetro" que nos avisa cuando estamos superando los límites de seguridad antes de que ocurra un daño.

1. Atributos de un KRI

Para que un indicador sea considerado un KRI efectivo, debe cumplir con tres condiciones:

- Predictivo: Debe avisar con tiempo suficiente para actuar (Alertas Tempranas).
- Comparable: Debe permitir ver la evolución del riesgo mes a mes o trimestre a trimestre.
- Umbralizado: Debe tener límites claros (Verde, Amarillo, Rojo) que disparen acciones automáticas.

2. Definición de Umbrales (Semáforo de Alerta)

Cada indicador debe tener un nivel de tolerancia definido por el líder del proceso:

- Zona Verde (Tolerable): El riesgo está bajo control.
- Zona Amarilla (Alerta): Se requiere revisión inmediata de la efectividad de los controles.
- Zona Roja (Inaceptable): Se deben activar inmediatamente las acciones del Plan de Tratamiento (Paso 9).

Cada indicador de riesgo deberá definir, como mínimo según la hoja de vida indicador PE-F-058:

- Nombre del indicador.
- Fórmula o forma de medición.
- Frecuencia de medición.
- Fuente de información.
- Responsable.
- Umbral de alerta.

Ejemplo:

Riesgo identificado: Posible incumplimiento en el seguimiento al Plan de Desarrollo Municipal.

Indicador de riesgo (KRI):

Elemento	Descripción
Nombre del indicador	Porcentaje de dependencias que entregan información fuera de plazo
Fórmula	(Número de dependencias fuera de plazo / Total de dependencias) × 100
Frecuencia	Mensual
Fuente	Reportes de seguimiento al Plan de Desarrollo
Responsable	OPGI
Umbral de alerta	Mayor al 10 %

Elemento	Descripción Técnica (Hoja de Vida PE-F-058)

Nombre del KRI	Índice de Morosidad en el Reporte de Metas PDM.
Fórmula	(Dependencias con reporte extemporáneo/Total dependencias obligadas a reportar) x 100
Frecuencia	Mensual (para detectar fallas antes del cierre trimestral).
Fuente	Registro de ingresos y logs de la plataforma de Planeación / OPGI.
Responsable	Jefe de la Oficina de Planeación y Gestión Institucional (OPGI).
Umbral de Alerta	**Verde:** <5% **Amarillo:** >5% y <10% **Rojo:** >10%

Análisis ejemplo: Si en el mes de marzo el indicador marca 12%, el jefe de la OPGI no espera a que se acabe el trimestre; activa inmediatamente la acción de tratamiento: "Socializar responsabilidades e implementar alertas de incumplimiento".

Paso 11. Seguimiento y actualización

La gestión del riesgo en la Alcaldía de Pasto es un proceso dinámico y cíclico. El seguimiento tiene como objetivo verificar que los controles sigan siendo efectivos, que los planes de tratamiento se cumplan y que el mapa de riesgos refleje la realidad actual del municipio. Este paso asegura la alineación permanente con el Modelo Integrado de Planeación y Gestión (MIPG). Los riesgos, controles e indicadores deberán ser revisados y actualizados de manera periódica y cuando ocurran cambios relevantes en los procesos, normas o contexto institucional. Se realizará el seguimiento, monitoreo y actualización permanente de los riesgos, con el fin de verificar la efectividad de los controles, el cumplimiento de los planes de tratamiento y la pertinencia de los riesgos identificados frente a los cambios del contexto institucional.

Este paso garantiza que la gestión del riesgo sea un proceso dinámico, continuo y preventivo, y no un ejercicio estático o meramente documental.

1. Las Tres Líneas de Defensa en el Seguimiento

Bajo el esquema de líneas de defensa, el monitoreo se distribuye así:

- Primera Línea (Líderes de Proceso): Autocontrol diario y reporte de alertas.
- Segunda Línea (OPGI / Planeación): Consolidación técnica, análisis de tendencias y apoyo metodológico.
- Tercera Línea (Control Interno): Evaluación independiente y auditoría basada en riesgos para verificar la madurez del sistema.

2. Frecuencia de Seguimiento según Riesgo Residual

La intensidad del monitoreo es directamente proporcional a la gravedad del riesgo que quedó tras aplicar controles:

Nivel de Riesgo Residual	**Instancia de Reporte**	Frecuencia de Monitoreo
Crítico (Zona Roja)	Líder de proceso y equipo de trabajo	Cuatrimestral
Alto (Zona Naranja)		
Medio (Zona Amarilla)		

Bajo (Zona Verde)		

Nota: El reporte de la ejecución de controles debe hacerse a través del formato MC-F-027 Monitoreo de los controles de riesgos y reportarlo por parte del líder del proceso a la Oficina de Planeación de Gestión Institucional de acuerdo con la frecuencia de monitoreo.

3. Disparadores de Actualización Extraordinaria

El Mapa de Riesgos debe actualizarse de inmediato (sin esperar al cronograma) cuando:

- Se materialice un riesgo (ocurra el evento).
- Cambie la normativa nacional o municipal que afecte el proceso.
- Exista un cambio significativo en la estructura organizacional o tecnológica (ej. nuevo software de Planeación).

Ejemplo:
Riesgo: Posibilidad de afectación reputacional por el incumplimiento en el seguimiento al Plan de Desarrollo Municipal.
Nivel Residual (Paso 8): MODERADO (Amarillo).
Acción de Seguimiento: Según la tabla, este riesgo tendrá un seguimiento cuatrimestral.
Evidencia del Seguimiento: En el mes de junio, el Líder de Planeación revisa el KRI (Índice de Morosidad). Si el indicador marca un aumento sostenido (ej. pasó de 4% a 9%), se debe citar a una mesa técnica para ajustar los controles antes de que el riesgo suba a nivel Alto.

8. EVALUACIÓN DIFERENCIADA DE RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN, RIESGOS FISCALES E INTEGRIDAD PÚBLICA – SIGRIP

La Alcaldía de Pasto, en el marco de la gestión integral del riesgo adoptada en el presente manual y de conformidad con la Guía para la Gestión Integral del Riesgo Versión 7 del Departamento Administrativo de la Función Pública (DAFP, 2025), reconoce que tres categorías de riesgo requieren lineamientos y criterios de evaluación diferenciados respecto a los riesgos de gestión ordinarios, por su naturaleza, régimen normativo especial y nivel de tolerancia institucional:

- Los riesgos para la seguridad de la información, en articulación con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Anexo de Gestión de Riesgos de Seguridad Digital del MinTIC.
- Los riesgos fiscales, derivados de la gestión de recursos públicos y articulados con el sistema de control fiscal constitucional.
- Los riesgos para la integridad pública, gestionados en el marco del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), componente del Programa de Transparencia y Ética Pública (PTEP), creado por el Decreto 1122 de 2024.

Este capítulo desarrolla para cada categoría: el marco normativo vigente, la definición y alcance, los criterios específicos de identificación y evaluación, los controles aplicables y los indicadores clave de riesgo (KRI). Todo ello se aplica de manera articulada con la metodología de 11 pasos del Capítulo 7.5 y el modelo de tres líneas de defensa del numeral 6.3 del presente manual, y es de obligatorio cumplimiento para todas las dependencias de la Alcaldía de Pasto.

8.1. RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN

8.1.1. Marco normativo aplicable

Norma / Instrumento	Disposición aplicable para la Alcaldía de Pasto
Ley 1581 de 2012	Protección de datos personales. Obliga a la entidad a garantizar la confidencialidad, integridad y disponibilidad de toda base de datos que contenga información personal de ciudadanos.
Decreto 1377 de 2013	Reglamenta el tratamiento de datos sensibles (salud, datos de menores, información biométrica y financiera). Establece obligaciones de autorización, aviso de privacidad y medidas de seguridad.
Ley 1273 de 2009	Delitos informáticos: tipifica el acceso abusivo a sistemas, daño informático, interceptación de datos y violación de datos personales como conductas penalmente sancionables.
Decreto 1078 de 2015 – Política de Gobierno Digital	Establece los lineamientos de seguridad digital para entidades públicas: gestión de riesgos de seguridad, continuidad de operaciones, protección de infraestructura crítica y respuesta a incidentes.
Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)	Marco técnico para implementar controles de seguridad de la información en entidades del Estado, basado en la norma ISO/IEC 27001:2022.
Guía GIR Versión 7 – DAFP (2025)	Actualiza el enfoque de gestión del riesgo de seguridad de la información, integra los lineamientos del Anexo de Gestión de Riesgos de Seguridad Digital del MinTIC, e introduce criterios diferenciados para la valoración de activos y amenazas digitales.

8.1.2. Definición y alcance

Los riesgos para la seguridad de la información son los eventos que pueden comprometer la confidencialidad, la integridad o la disponibilidad de los activos de información de la Alcaldía de Pasto. Se entiende como activo de información todo dato, sistema, plataforma digital, base de datos, registro físico o electrónico, infraestructura tecnológica y conocimiento institucional necesario para el cumplimiento de los objetivos de la entidad. Estos riesgos aplican a la totalidad de los procesos de la Alcaldía de Pasto que gestionen, almacenen, procesen o transmitan información institucional o de ciudadanos.

Tolerancia institucional:
El nivel de tolerancia para los riesgos de seguridad de la información es BAJO, conforme a la tabla del numeral 6.2 del presente manual. Cualquier riesgo de esta categoría con nivel residual que supere el nivel Bajo requiere plan de tratamiento obligatorio.

8.1.3. Subcategorías de riesgos de seguridad de la información

Conforme a la Guía GIR v7 y al MSPI del MinTIC, los riesgos de seguridad de la información se identifican y clasifican en las siguientes subcategorías:

Subcategoría	Descripción	Ejemplo orientador (aplicable a cualquier proceso)
Confidencialidad	Acceso no autorizado a información reservada o datos personales de ciudadanos por parte de personal no habilitado.	Posibilidad de vulneración de datos personales almacenados en bases de datos institucionales por acceso indebido de terceros, debido a controles de autenticación insuficientes en los sistemas de información.
Integridad	Alteración, manipulación o corrupción dolosa o accidental de información institucional o de datos de ciudadanos.	Posibilidad de modificación no autorizada de registros en sistemas de información críticos, debido a la ausencia de logs de auditoría activos y controles de trazabilidad.
Disponibilidad	Interrupción o pérdida de acceso a sistemas de información que impida la prestación de servicios a la ciudadanía o la operación institucional.	Posibilidad de interrupción de los sistemas misionales de la entidad por fallas en la infraestructura tecnológica, debida a la ausencia de un plan de continuidad del servicio.
Ciberseguridad	Ataques externos (ransomware, phishing, DDoS) o internos a la infraestructura digital de la entidad.	Posibilidad de pérdida total de información financiera y contractual por un ataque de ransomware a los servidores institucionales, debido a la falta de actualización periódica de parches de seguridad.
Privacidad de la información	Tratamiento inadecuado de datos personales de ciudadanos en contravención de la Ley 1581 de 2012, con potencial sanción de la Superintendencia de Industria y Comercio (SIC).	Posibilidad de divulgación no autorizada de datos personales de ciudadanos, debido a la ausencia de una política formal de tratamiento y aviso de privacidad institucional.

8.1.4. Gestión de Incidentes de Seguridad de la Información

El Modelo de Gestión de Incidentes de Seguridad de la Información tiene como propósito establecer un marco metodológico para la identificación, registro, análisis, respuesta, contención, recuperación y mejora continua frente a los incidentes que

puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

Este modelo permite fortalecer la capacidad institucional para prevenir, detectar, responder y recuperar oportunamente la operación frente a eventos que comprometan la seguridad de la información, contribuyendo al cumplimiento de los objetivos institucionales, la continuidad de los procesos y el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7.

Objetivos del Modelo de Gestión de Incidentes

El Modelo de Gestión de Incidentes de Seguridad de la Información tiene como objetivos:

- Definir la estructura de gobierno, los roles, responsabilidades y niveles de autoridad para la gestión integral de los incidentes de seguridad de la información.
- Establecer los mecanismos para la identificación, clasificación, registro, análisis y priorización de los eventos e incidentes de seguridad de la información.
- Garantizar una respuesta oportuna, coordinada y efectiva frente a los incidentes, minimizando su impacto sobre los procesos, los activos de información y la prestación de los servicios institucionales.
- Implementar acciones de contención, erradicación y recuperación que permitan restablecer la operación normal de los servicios afectados en el menor tiempo posible.
- Reducir la probabilidad de materialización de nuevos incidentes mediante la implementación de controles preventivos, detectivos y correctivos derivados del análisis de las causas raíz.
- Consolidar y gestionar las lecciones aprendidas provenientes de los incidentes ocurridos, promoviendo la mejora continua de los controles de seguridad y de los procesos institucionales.
- Mantener un repositorio de incidentes que permita generar información estadística, indicadores y análisis de tendencias para apoyar la toma de decisiones basada en riesgos.
- Establecer mecanismos de seguimiento, monitoreo y reporte que faciliten la medición de la frecuencia, impacto, criticidad, costos y tiempos de respuesta asociados a los incidentes de seguridad de la información.
- Fortalecer la cultura institucional de seguridad de la información mediante la comunicación, sensibilización y capacitación permanente de los servidores públicos y demás partes interesadas.
- Contribuir al proceso de gestión integral del riesgo mediante la actualización de la valoración de riesgos, vulnerabilidades y amenazas identificadas durante la atención de incidentes.

Ciclo de Gestión de Incidentes de Seguridad de la Información

La gestión de incidentes constituye un proceso continuo y de mejora permanente, integrado por las siguientes etapas:

1. **Preparación:** Definición de políticas, procedimientos, responsabilidades, recursos, herramientas y mecanismos de comunicación necesarios para atender los incidentes de seguridad de la información.
2. **Detección y análisis:** Identificación, registro, clasificación, validación y análisis de los eventos e incidentes de seguridad para determinar su naturaleza, alcance, criticidad y nivel de impacto.
3. **Contención, erradicación y recuperación:** Implementación de las acciones necesarias para controlar el incidente, eliminar su causa, restaurar los servicios afectados y garantizar la continuidad de la operación institucional.
4. **Lecciones aprendidas y mejora continua:** Evaluación posterior al incidente para identificar oportunidades de mejora, fortalecer los controles existentes, actualizar las matrices de riesgos, los procedimientos y los planes de tratamiento, promoviendo el aprendizaje organizacional y el incremento del nivel de madurez en la gestión de la seguridad de la información.

N°	Clase de Incidente	Tipo de Incidente	Descripción
1	Contenido Abusivo	Pornografía Infantil – Sexual – Violencia	Pornografía infantil, glorificación de la violencia, otros.
		Spam	«Correo masivo no solicitado», lo que significa que el destinatario no ha otorgado permiso verificable para que el mensaje sea enviado y además el mensaje es enviado como parte de una grupo masivo de mensajes, todos teniendo un contenido similar
		Difamación	Desacreditación o discriminación de alguien
2	Código Malicioso	Malware, Virus, Gusanos, Troyanos, spyware, Dialler, rootkit	Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código.
3	Recopilación de Información	Scanning	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.
		Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).
		Ingeniería Social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
4	Intentos de Intrusión	Intentos de acceso	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).
		Explotación de vulnerabilidades conocidas	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, el búfer desbordamiento, puerta trasera, secuencias de comandos cruzadas, etc.).
		Nueva Firma de Ataque	Un intento de usar un exploit desconocido.
5	Intrusión	Compromiso de Cuenta Privilegiada	Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede han sido causado de forma remota por una vulnerabilidad

		Compromiso de Cuenta sin privilegios Compromiso de Aplicación, Bot	conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una botnet.
6	Disponibilidad	Ataque de denegación de servicio (DoS / DDoS) Sabotaje Intercepción de información	Con este tipo de ataque, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema falla. Algunos ejemplos DoS son ICMP e inundaciones SYN, ataques de teardrop y bombardeos de mail's. DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como Ataques de amplificación DNS. Sin embargo, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o error humano, sin mala intención o negligencia.
7	Información de seguridad de contenidos	Acceso no autorizado a la información Modificación no autorizada de la información	Además de un abuso local de datos y sistemas, la seguridad de la información puede ser en peligro por una cuenta exitosa o compromiso de la aplicación. Además, son posibles los ataques que interceptan y acceden a información durante la transmisión (escuchas telefónicas, spoofing o secuestro). El error humano / de configuración / software también puede ser la causa.
8	Fraude	Phishing	Enmascarado como otra entidad para persuadir al usuario a revelar un credencial privada.
		Derechos de Autor	Ofrecer o instalar copias de software comercial sin licencia u otro materiales protegidos por derechos de autor (Warez).
		Uso no autorizado de recursos	Usar recursos para fines no autorizados, incluida la obtención de beneficios empresas (por ejemplo, el uso del correo electrónico para participar en cartas de cadena de ganancias ilegales) o esquemas piramidales).
		Falsificación de registros o identidad	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otro para beneficiarse de ello.
9	Vulnerable	Sistemas y/o softwares Abiertos	Sistemas «Open Resolvers», impresoras abiertas a todo el mundo, vulnerabilidades aparentes detectadas con nessus u otros aplicativos, firmas de virus no actualizadas, etc.
10	Otros	Todos los incidentes que no encajan en alguna de las otras categorías dadas	Si la cantidad de incidentes en esta categoría aumenta, es un indicador de que el esquema de clasificación debe ser revisado.
11	Test	Para pruebas	Producto de pruebas de seguridad controladas e informadas

Fuente: CSIRT

Clasificación del Riesgo (Posible Incidente de Seguridad)

Código	Clasificación del Riesgo (Posible Incidente de Seguridad)	Dimensión afectada (CID)	Ejemplo
SI-01	Acceso no autorizado a la información	Confidencialidad	Un funcionario consulta información sin permisos.
SI-02	Divulgación no autorizada de información	Confidencialidad	Se envía información reservada a un destinatario equivocado.
SI-03	Fuga o filtración de información	Confidencialidad	Se publica información sensible en internet.
SI-04	Robo de información	Confidencialidad	Extracción de bases de datos institucionales.
SI-05	Pérdida de información	Disponibilidad / Integridad	Eliminación accidental de archivos.
SI-06	Alteración no autorizada de información	Integridad	Modificación indebida de registros.
SI-07	Corrupción de datos	Integridad	Base de datos dañada por fallas o malware.
SI-08	Eliminación no autorizada de información	Integridad	Borrado intencional de documentos.
SI-09	Indisponibilidad del servicio	Disponibilidad	El sistema institucional deja de funcionar.
SI-10	Interrupción de los servicios tecnológicos	Disponibilidad	Caída del servidor o de la red institucional.
SI-11	Pérdida de conectividad	Disponibilidad	Falla en internet o red LAN.
SI-12	Infección por software malicioso	C-I-D	Virus, ransomware, spyware o troyanos.
SI-13	Ataque de ransomware	Disponibilidad / Integridad	Cifrado de servidores y archivos.
SI-14	Ataque de phishing	Confidencialidad	Robo de credenciales mediante correo falso.
SI-15	Suplantación de identidad	Confidencialidad	Uso indebido de cuentas institucionales.
SI-16	Compromiso de credenciales	Confidencialidad	Contraseñas descubiertas o robadas.
SI-17	Uso indebido de privilegios	Confidencialidad / Integridad	Usuario administrador realiza acciones no autorizadas.
SI-18	Denegación de servicio (DoS/DDoS)	Disponibilidad	Saturación de un servicio web.
SI-19	Pérdida o robo de equipos	C-I-D	Hurto de portátil institucional.
SI-20	Daño físico de equipos tecnológicos	Disponibilidad	Incendio, inundación o daño eléctrico.
SI-21	Falla en copias de seguridad	Disponibilidad	No es posible restaurar la información.
SI-22	Recuperación fallida de información	Disponibilidad	El respaldo existe pero no funciona.
SI-23	Configuración insegura de sistemas	C-I-D	Parámetros inseguros permiten ataques.
SI-24	Incumplimiento de políticas de seguridad	C-I-D	No aplicación de controles institucionales.
SI-25	Exposición de datos personales	Confidencialidad	Divulgación de datos protegidos por la Ley 1581.
SI-26	Uso no autorizado de dispositivos externos	C-I-D	Memorias USB con información institucional.
SI-27	Instalación de software no autorizado	C-I-D	Programas sin licencia o sin aprobación TI.
SI-28	Pérdida de trazabilidad de la información	Integridad	No existen registros de auditoría.
SI-29	Incumplimiento de requisitos legales sobre información	C-I-D	Incumplimiento de normas de protección de datos.
SI-30	Compromiso de servicios en la nube	C-I-D	Acceso indebido a plataformas cloud institucionales.

Sigla	Significado
C	Confidencialidad
I	Integridad
D	Disponibilidad

EJEMPLOS DE ACTIVOS DE INFORMACIÓN – AMENZA Y VULNERABILIDAD

Activo de Información	Amenaza	Vulnerabilidad	Clasificación del Riesgo (Incidente)	Consecuencia
Sistema Financiero	Malware	Antivirus desactualizado	Infección por software malicioso (SI-12)	Interrupción del servicio y pérdida de información
Base de Datos de Talento Humano	Acceso indebido	Contraseñas débiles	Acceso no autorizado a la información (SI-01)	Divulgación de datos personales
Página Web Institucional	Ataque DDoS	Firewall insuficiente	Denegación de servicio (SI-18)	Indisponibilidad del portal institucional
Servidor de Archivos	Falla eléctrica	UPS sin mantenimiento	Pérdida de información (SI-05)	Afectación de la continuidad del servicio

TIPOS DE ACTIVOS DE INFORMACIÓN:

- Información y datos de la entidad: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros
- Sistemas de información y aplicaciones de Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- Dispositivos de Tecnologías de información- Hardware: Equipos de cómputo que por su criticidad son considerados activos de información, no sólo activos fijos.
- Soporte para almacenamiento de información: Equipo para almacenamiento de información como USB, Discos Duros, CDs, SAN, NAS.
- Servicios: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- Recursos Humanos
- Instalaciones
- Redes

8.1.5. Criterios de evaluación diferenciados

Se aplican las escalas generales de probabilidad e impacto de los Pasos 3 y 4 del manual, con las siguientes precisiones adicionales obligatorias:

- Cuando el riesgo involucre datos sensibles en los términos del Decreto 1377 de 2013 (datos de salud, de menores de edad, biométricos o financieros), el impacto no podrá calificarse por debajo del nivel Moderado (60%), en razón del régimen especial de protección que establece la Ley 1581 de 2012.

- El impacto debe contemplar la posibilidad de sanciones de la Superintendencia de Industria y Comercio (SIC) derivadas de una brecha de datos personales, adicionales al impacto reputacional y económico definido en la escala general.
- La frecuencia de evaluación de la probabilidad debe considerar, además de la frecuencia de la actividad, el nivel de exposición del sistema a amenazas externas (intentos de vulneración, nivel de criticidad del activo), conforme a los criterios del MSPI del MinTIC.
- Los controles automáticos sobre sistemas de información tienen mayor peso en la evaluación de efectividad (25%) que los controles manuales (15%), razón por la cual se debe priorizar la automatización de controles en los planes de tratamiento de esta categoría.

8.1.6. Controles específicos para riesgos de seguridad de la información

Tipo	Implementación	Ejemplo de redacción correcta (aplicable a cualquier proceso)
Preventivo	Automático	El sistema institucional de gestión de información restringe automáticamente el acceso a los módulos críticos tras tres intentos fallidos de autenticación, generando una alerta inmediata al administrador del sistema.
Preventivo	Manual	El Subsecretario de sistemas de información valida trimestralmente los perfiles de acceso a los sistemas de información, verificando que únicamente el personal activo y autorizado cuente con acceso habilitado por módulo, con registro en el formato de control de accesos.
Detectivo	Automático	El sistema de monitoreo de seguridad genera alertas automáticas ante accesos fuera del horario laboral, desde ubicaciones atípicas o con perfiles de uso no habituales en los sistemas de información críticos.
Detectivo	Manual	El Subsecretario de sistemas de información revisa mensualmente los logs de acceso a los sistemas críticos, identificando accesos no autorizados, intentos de modificación de registros o anomalías operativas.
Correctivo	Manual	El Subsecretario de sistemas de información activa el protocolo institucional de respuesta a incidentes de seguridad en un plazo máximo de cuatro horas ante la detección de una brecha de datos, notificando a la Superintendencia de Industria y Comercio (SIC) conforme al artículo 17 de la Ley 1581 de 2012 y a la Alta Dirección.

No.	Dominio	Control ISO/IEC 27001:2022	Ejemplo de aplicación — Alcaldía de Pasto	Amenaza asociada	Vulnerabilidad asociada	C	I	D	Ciber	Priv
5.1	**5. Organizacional**	Políticas de seguridad de la información	La Alcaldía aprueba y publica la Política de Seguridad y Privacidad de la Información, revisada anualmente por la Alta Dirección.	Ausencia de directrices institucionales formales en seguridad.	Falta de una política de seguridad aprobada y divulgada.	X	X	X		
5.2	**5. Organizacional**	Roles y responsabilidades en la Seguridad de la Información	Se asignan formalmente los roles de Oficial de Seguridad de la Información, Jefe TIC y dueños de activos por proceso.	Actuación sin autoridad definida ante un incidente de seguridad.	Roles y responsabilidades de seguridad no asignados ni comunicados.	X	X	X		
5.3	**5. Organizacional**	Segregación de deberes	Quien solicita la creación de un usuario en el sistema financiero no es quien lo aprueba ni quien lo administra.	Fraude o manipulación interna de la información.	Concentración de funciones incompatibles en una sola persona.	X	X			
5.4	**5. Organizacional**	Responsabilidades de la dirección	Los secretarios de despacho exigen a su personal el cumplimiento de la política de seguridad en cada dependencia.	Incumplimiento generalizado de los controles de seguridad.	Falta de exigencia y seguimiento por parte de los jefes de área.	X	X	X		
5.5	**5. Organizacional**	Contacto con las autoridades	El Jefe TIC mantiene contacto vigente con la Policía Nacional (CAI Virtual), MinTIC y la SIC para reportar incidentes.	Respuesta tardía o inadecuada ante un ciberataque o brecha de datos.	Ausencia de canales de comunicación con autoridades competentes.			X	X	
5.6	**5. Organizacional**	Contacto con grupos de interés especial	La entidad participa en la Red Nacional de Seguridad Digital y en foros del CSIRT de Gobierno.	Desactualización frente a nuevas amenazas y tendencias de ataque.	Aislamiento institucional frente a la comunidad de seguridad digital.				X	
5.7	**5. Organizacional**	Inteligencia de amenazas	El área de TIC recopila boletines de vulnerabilidades del CSIRT de Gobierno para anticipar ataques a los sistemas misionales.	Ataques dirigidos (ransomware, phishing) no anticipados.	Falta de monitoreo de fuentes de inteligencia de amenazas.			X	X	
5.8	**5. Organizacional**	Seguridad de la información en la gestión de proyectos	Todo proyecto de implementación de un nuevo sistema de información incluye un análisis de riesgos de seguridad desde su planeación.	Vulnerabilidades introducidas desde el diseño de nuevos sistemas.	Ausencia de requisitos de seguridad en el ciclo de vida del proyecto.	X	X	X		
5.9	**5. Organizacional**	Inventario de información y otros activos asociados	Cada Secretaría mantiene actualizado el inventario de sus activos de información con su respectivo dueño y custodio.	Pérdida o uso indebido de activos de información no identificados.	Inventario de activos de información inexistente o desactualizado.	X	X	X		
5.10	**5. Organizacional**	Uso aceptable de la información y otros activos asociados	Se socializa y firma el manual de uso aceptable de equipos, correo institucional e internet.	Uso indebido de los recursos tecnológicos institucionales.	Ausencia de normas claras de uso aceptable de activos.	X	X			
5.11	**5. Organizacional**	Devolución de activos	Al terminar un contrato, el funcionario o contratista devuelve equipo, credenciales y documentos mediante acta de paz y salvo.	Fuga de información por parte de personal desvinculado.	Falta de control en la devolución de activos al finalizar el vínculo.	X				X
5.12	**5. Organizacional**	Clasificación de la información	Los documentos y bases de datos se clasifican como públicos, clasificados o reservados conforme a la Ley 1712 de 2014.	Divulgación de información reservada o clasificada.	Información institucional sin clasificar o clasificada de forma errónea.	X				X

5.13	**5. Organizacional**	Etiquetado de la información	Los documentos reservados se marcan con el rótulo "Información Reservada" según el esquema institucional de clasificación.	Manejo inadecuado de información sensible por desconocimiento de su nivel.	Falta de etiquetado visible del nivel de clasificación asignado.	X				
5.14	**5. Organizacional**	Transferencia de información	Se establecen protocolos seguros (cifrado, canales oficiales) para el envío de bases de datos de ciudadanos entre dependencias.	Interceptación o pérdida de información durante su transmisión.	Transferencia de información por canales no seguros (correo personal, USB).	X	X			X
5.15	**5. Organizacional**	Control de acceso	El acceso a los sistemas de información se otorga según el perfil y las funciones del cargo del servidor.	Acceso no autorizado a sistemas o información crítica.	Controles de acceso insuficientes o mal configurados.	X	X			
5.16	**5. Organizacional**	Gestión de identidades	Cada funcionario cuenta con un único usuario institucional, creado, modificado y eliminado mediante procedimiento formal.	Suplantación de identidad dentro de los sistemas de información.	Identidades duplicadas, huérfanas o compartidas entre usuarios.	X	X			
5.17	**5. Organizacional**	Información de autenticación	Las contraseñas institucionales cumplen requisitos de complejidad y se gestionan mediante un procedimiento formal.	Compromiso de las credenciales de acceso de un usuario.	Contraseñas débiles o gestionadas de forma insegura.	X			X	
5.18	**5. Organizacional**	Derechos de acceso	Trimestralmente el Subsecretario de sistemas de información revisa que solo el personal activo tenga acceso habilitado por módulo.	Acceso indebido de personal desvinculado o sin funciones vigentes.	Perfiles de acceso no revisados de forma periódica.	X	X			
5.19	**5. Organizacional**	Seguridad de la información en las relaciones con proveedores	Se evalúan los riesgos de seguridad antes de contratar un proveedor que administrará el sistema de nómina.	Compromiso de la información por parte de un tercero contratado.	Falta de evaluación de riesgos en la vinculación de proveedores.	X	X	X		
5.20	**5. Organizacional**	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Los contratos de tecnología incluyen cláusulas de confidencialidad, protección de datos y niveles de servicio (SLA).	Incumplimiento de las obligaciones de seguridad por parte del proveedor.	Contratos suscritos sin requisitos de seguridad de la información.	X	X	X		X
5.21	**5. Organizacional**	Gestión de seguridad de la información en la cadena de suministro de TIC	Se exige a los proveedores de software y hardware evidenciar buenas prácticas de seguridad en su cadena de suministro.	Introducción de código malicioso a través de un proveedor de TIC.	Falta de control sobre la cadena de suministro tecnológico.		X		X	
5.22	**5. Organizacional**	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	Se audita periódicamente el cumplimiento del proveedor que administra el sistema de gestión documental.	Degradación no detectada del servicio o la seguridad prestada por el proveedor.	Falta de seguimiento al desempeño de los proveedores de TIC.	X	X	X		
5.23	**5. Organizacional**	Seguridad de la información para el uso de servicios en la nube	Antes de migrar el aplicativo de trámites a la nube se valida el cumplimiento de requisitos de seguridad del proveedor cloud.	Pérdida o exposición de información institucional alojada en la nube.	Configuración insegura de los servicios contratados en la nube.	X	X	X	X	
5.24	**5. Organizacional**	Planificación y preparación de la gestión de incidentes de seguridad de la información	Se define y comunica el protocolo institucional de atención de incidentes de seguridad digital.	Respuesta desorganizada ante un incidente de seguridad.	Ausencia de un procedimiento formal de gestión de incidentes.			X	X	
5.25	**5. Organizacional**	Evaluación y decisión sobre eventos de seguridad de la información	El Jefe TIC evalúa cada alerta generada por el sistema de monitoreo para determinar si constituye un incidente.	Escalamiento de un evento menor por falta de valoración oportuna.	Ausencia de criterios para clasificar un evento como incidente.			X	X	

5.26	**5. Organizacional**	Respuesta a incidentes de seguridad de la información	Ante una brecha de datos se activa el protocolo de respuesta en máximo 4 horas, conforme a la Ley 1581 de 2012.	Propagación o agravamiento de un incidente de seguridad.	Falta de un procedimiento documentado de respuesta a incidentes.	X	X	X	X	X
5.27	**5. Organizacional**	Aprender de los incidentes de seguridad de la información	Tras cada incidente se documentan lecciones aprendidas que alimentan la actualización de controles y de la matriz de riesgos.	Recurrencia de incidentes por causas no corregidas.	Ausencia de análisis posterior a los incidentes presentados.		X	X		
5.28	**5. Organizacional**	Recopilación de evidencias	Se conservan los logs y registros de un incidente de acceso indebido para eventuales procesos disciplinarios o judiciales.	Imposibilidad de sustentar legalmente un incidente de seguridad.	Ausencia de procedimientos de preservación de evidencia digital.		X		X	
5.29	**5. Organizacional**	Seguridad de la información durante una interrupción	Ante un corte prolongado de energía se activan controles alternos para proteger la información mientras se restablece el servicio.	Pérdida de protección de la información durante una contingencia.	Falta de controles de seguridad definidos para situaciones de interrupción.	X		X		
5.30	**5. Organizacional**	Preparación de las TIC para la continuidad de negocio	Se cuenta con un plan de continuidad tecnológica que garantiza la disponibilidad de los sistemas misionales ante una contingencia mayor.	Interrupción prolongada de los servicios prestados a la ciudadanía.	Ausencia de un plan de continuidad de TIC probado y actualizado.			X		
5.31	**5. Organizacional**	Requisitos legales, reglamentarios y contractuales	Se mantiene actualizado el listado de normas aplicables (leyes 1581 y 1273, Decreto 1078) y su nivel de cumplimiento.	Sanciones por incumplimiento del marco normativo de protección de datos.	Desconocimiento o desactualización del marco legal aplicable.	X				X
5.32	**5. Organizacional**	Derechos de propiedad intelectual	Se controla que el software instalado en los equipos institucionales cuente con licenciamiento vigente.	Uso de software no licenciado en los equipos institucionales.	Falta de control sobre las licencias de software instaladas.		X			
5.33	**5. Organizacional**	Protección de registros	Los registros contractuales y contables se conservan protegidos según la tabla de retención documental de la entidad.	Pérdida, alteración o destrucción de registros institucionales.	Custodia inadecuada de los registros físicos y electrónicos.	X	X	X		
5.34	**5. Organizacional**	Privacidad y protección de la información de identificación personal (PII)	Se implementa un aviso de privacidad y un procedimiento de autorización para el tratamiento de datos personales de los ciudadanos.	Tratamiento indebido de los datos personales de los ciudadanos.	Ausencia de una política formal de tratamiento de datos personales.	X				X
5.35	**5. Organizacional**	Revisión independiente de la seguridad de la información	La Oficina de Control Interno realiza auditorías anuales independientes al Sistema de Gestión de Seguridad de la Información.	Deficiencias del SGSI no detectadas por los mismos responsables.	Ausencia de revisión independiente y objetiva del sistema de gestión.		X	X		
5.36	**5. Organizacional**	Cumplimiento de políticas, reglas y estándares de seguridad de la información	Se verifica periódicamente que cada dependencia cumpla la política y los procedimientos de seguridad establecidos.	Desviaciones no detectadas frente a la política institucional.	Falta de verificación periódica del cumplimiento normativo interno.		X	X		
5.37	**5. Organizacional**	Procedimientos operativos documentados	Los procedimientos de respaldo, gestión de accesos y atención de incidentes están	Ejecución inconsistente de tareas críticas del área de TIC.	Ausencia de procedimientos operativos formalizados.		X	X		

			documentados y disponibles para el personal de TIC.							
6.1	**6. Personas**	Selección	Se realizan verificaciones de antecedentes judiciales y disciplinarios antes de vincular personal con acceso a sistemas críticos.	Vinculación de personal con antecedentes que representen un riesgo para la entidad.	Ausencia de verificación de antecedentes en los procesos de selección.	X	X			
6.2	**6. Personas**	Términos y condiciones de empleo	Los contratos y actas de posesión incluyen cláusulas expresas de responsabilidad sobre la seguridad de la información.	Desconocimiento de las obligaciones de seguridad por parte del personal.	Ausencia de cláusulas contractuales de seguridad de la información.	X	X			
6.3	**6. Personas**	Conciencia de seguridad de la información, educación y formación	Se realizan jornadas anuales de sensibilización sobre phishing y buenas prácticas de seguridad digital para los servidores públicos.	Caída en ataques de ingeniería social por desconocimiento del personal.	Bajo nivel de cultura y conciencia institucional en seguridad digital.	X	X	X	X	
6.4	**6. Personas**	Proceso disciplinario	Se aplica el régimen disciplinario a un funcionario que incumplió la política de seguridad de la información.	Reincidencia en el incumplimiento de los controles de seguridad.	Ausencia de consecuencias formales ante incumplimientos detectados.		X			
6.5	**6. Personas**	Responsabilidades después de la terminación o cambio de empleo	Al desvincularse un contratista se le recuerda por escrito su deber de confidencialidad vigente después del contrato.	Divulgación de información institucional por parte de exfuncionarios.	Falta de comunicación de responsabilidades posteriores a la desvinculación.	X				X
6.6	**6. Personas**	Acuerdos de confidencialidad o no divulgación	Todo funcionario y contratista firma un acuerdo de confidencialidad antes de acceder a información institucional.	Divulgación no autorizada de información reservada.	Ausencia de acuerdos de confidencialidad firmados por el personal.	X				X
6.7	**6. Personas**	Trabajo remoto	El personal en teletrabajo accede a los sistemas mediante VPN cifrada y equipos institucionales con controles de seguridad.	Acceso inseguro a la información institucional desde ubicaciones remotas.	Conexiones remotas sin cifrado ni control de acceso adecuado.	X	X		X	
6.8	**6. Personas**	Informes de eventos de seguridad de la información	Se habilita un correo y una línea telefónica para que cualquier servidor reporte de forma oportuna un evento sospechoso.	Incidentes de seguridad no reportados que se agravan con el tiempo.	Ausencia de canales claros para reportar eventos de seguridad.			X	X	
7.1	**7. Físico**	Perímetros de seguridad física	El centro de datos de la Alcaldía cuenta con un perímetro físico delimitado y controlado.	Acceso físico no autorizado a las áreas donde se procesa información.	Ausencia de perímetros de seguridad física definidos.	X		X		
7.2	**7. Físico**	Entrada física	El ingreso al centro de cómputo requiere tarjeta de proximidad y registro biométrico.	Ingreso de personas no autorizadas a zonas restringidas.	Controles de entrada física insuficientes o inexistentes.	X		X		
7.3	**7. Físico**	Asegurar oficinas, habitaciones e instalaciones	Las oficinas donde se archivan expedientes con datos sensibles cuentan con cerraduras y control de acceso.	Sustracción de documentos con información sensible.	Oficinas e instalaciones sin medidas físicas de seguridad.	X				
7.4	**7. Físico**	Monitoreo de la seguridad física	Cámaras de videovigilancia monitorean permanentemente el centro de datos y los archivos institucionales.	Acceso físico no detectado a zonas críticas de la entidad.	Ausencia de monitoreo continuo de las instalaciones.	X		X		

7.5	**7. Físico**	Protección contra amenazas físicas y ambientales	El centro de datos cuenta con detección de incendios, control de humedad y protección contra inundaciones.	Pérdida de infraestructura crítica por eventos naturales o desastres.	Ausencia de controles ambientales en las instalaciones críticas.			X		
7.6	**7. Físico**	Trabajar en áreas seguras	Se establecen reglas específicas de acceso y permanencia para el personal que labora en el centro de datos.	Exposición de información en áreas de alta criticidad.	Ausencia de normas de trabajo definidas para zonas seguras.	X				
7.7	**7. Físico**	Escritorio y pantalla limpios	Se exige bloquear la pantalla al ausentarse del puesto y no dejar documentos sensibles sobre el escritorio.	Visualización o sustracción de información dejada a la vista.	Ausencia de una política de escritorio y pantalla limpios.	X				
7.8	**7. Físico**	Emplazamiento y protección de equipos	Los servidores institucionales se ubican en un espacio con control de temperatura y acceso restringido.	Daño o falla de equipos por condiciones ambientales inadecuadas.	Ubicación insegura de los equipos tecnológicos críticos.			X		
7.9	**7. Físico**	Seguridad de los activos fuera de las instalaciones	Los computadores portátiles asignados para trabajo en campo cuentan con cifrado de disco y contraseña de acceso.	Pérdida o hurto de equipos con información institucional fuera de la sede.	Equipos móviles utilizados sin controles de protección.	X		X		
7.10	**7. Físico**	Medios de almacenamiento	Los discos duros y USB institucionales se gestionan, etiquetan y destruyen de forma segura al finalizar su vida útil.	Recuperación de información sensible desde medios de almacenamiento desechados.	Ausencia de control sobre el ciclo de vida de los medios de almacenamiento.	X				X
7.11	**7. Físico**	Servicios públicos de apoyo	El centro de datos cuenta con planta eléctrica y UPS para garantizar el funcionamiento ante cortes de energía.	Interrupción de servicios por fallas en el suministro eléctrico.	Ausencia de respaldo ante fallos en los servicios públicos de apoyo.			X		
7.12	**7. Físico**	Seguridad del cableado	El cableado de red y eléctrico del centro de datos está protegido en canaletas y ductos seguros.	Interceptación o daño de las comunicaciones institucionales.	Cableado expuesto sin protección física adecuada.	X		X	X	
7.13	**7. Físico**	Mantenimiento de equipos	Los servidores y equipos de cómputo reciben mantenimiento preventivo programado por el área de TIC.	Falla de equipos críticos por falta de mantenimiento.	Ausencia de un programa de mantenimiento preventivo.		X	X		
7.14	**7. Físico**	Disposición o reutilización segura de los equipos	Antes de dar de baja un equipo se borra de forma segura toda la información y el software licenciado.	Fuga de información desde equipos dados de baja o reasignados.	Ausencia de un procedimiento de borrado seguro previo a la disposición.	X				X
8.1	**8. Tecnológico**	Dispositivos de punto final de usuario	Los computadores de los funcionarios cuentan con antivirus, cifrado y bloqueo automático por inactividad.	Compromiso de la información a través del equipo del usuario.	Dispositivos de usuario sin controles mínimos de seguridad.	X	X		X	
8.2	**8. Tecnológico**	Derechos de acceso privilegiado	Las cuentas de administrador de los sistemas críticos se asignan solo a personal autorizado de TIC y se auditan.	Abuso de privilegios administrativos sobre los sistemas de información.	Cuentas privilegiadas sin restricción ni supervisión.	X	X		X	
8.3	**8. Tecnológico**	Restricción de acceso a la información	Cada aplicativo restringe el acceso a los módulos según el perfil funcional del usuario.	Acceso a información fuera del alcance de las funciones del cargo.	Restricciones de acceso mal configuradas o inexistentes.	X				

8.4	**8. Tecnológico**	Acceso al código fuente	El código fuente de los aplicativos desarrollados internamente se gestiona en un repositorio con control de versiones y acceso restringido.	Modificación no autorizada del código fuente de las aplicaciones.	Código fuente sin control de acceso ni versionamiento.		X		X	
8.5	**8. Tecnológico**	Autenticación segura	El acceso a los sistemas críticos requiere autenticación multifactor además del usuario y contraseña.	Acceso no autorizado por compromiso de credenciales.	Autenticación basada únicamente en usuario y contraseña.	X			X	
8.6	**8. Tecnológico**	Gestión de la capacidad	Se monitorea el uso de almacenamiento y procesamiento de los servidores para prevenir saturaciones que afecten el servicio.	Indisponibilidad de los sistemas por agotamiento de recursos tecnológicos.	Falta de monitoreo y planificación de la capacidad tecnológica.			X		
8.7	**8. Tecnológico**	Protección contra malware	Todos los equipos institucionales cuentan con antivirus centralizado y actualizado automáticamente.	Infección por virus, ransomware u otro software malicioso.	Equipos sin protección antimalware actualizada.		X	X	X	
8.8	**8. Tecnológico**	Gestión de vulnerabilidades técnicas	Se realizan escaneos periódicos de vulnerabilidades a los servidores y aplicativos misionales, aplicando los parches identificados.	Explotación de vulnerabilidades técnicas conocidas y no corregidas.	Falta de actualización periódica de parches de seguridad.		X	X	X	
8.9	**8. Tecnológico**	Gestión de la configuración	Las configuraciones de seguridad de servidores y equipos de red siguen una línea base documentada y auditable.	Explotación de configuraciones inseguras por defecto.	Configuraciones tecnológicas no estandarizadas ni documentadas.	X	X		X	
8.10	**8. Tecnológico**	Eliminación de información	La información de bases de datos que ya cumplió su tiempo de retención se elimina de forma segura y controlada.	Retención innecesaria de datos personales que incrementa el riesgo de exposición.	Ausencia de procedimientos de eliminación segura de información.	X				X
8.11	**8. Tecnológico**	Enmascaramiento de datos	En los entornos de prueba se enmascaran los datos personales de los ciudadanos usados en producción.	Exposición de datos reales de ciudadanos en ambientes no productivos.	Uso de datos reales sin enmascarar en pruebas y desarrollo.	X				X
8.12	**8. Tecnológico**	Prevención de fugas de datos	Se implementan controles que impiden el envío masivo de bases de datos de ciudadanos por correo electrónico externo.	Fuga masiva de información sensible fuera de la entidad.	Ausencia de controles de prevención de fuga de datos (DLP).	X				X
8.13	**8. Tecnológico**	Copia de seguridad de la información	Los sistemas misionales cuentan con copias de respaldo automáticas verificadas mensualmente por el Jefe TIC.	Pérdida definitiva de información institucional ante una falla o ataque.	Copias de respaldo inexistentes, no probadas o desactualizadas.			X		
8.14	**8. Tecnológico**	Redundancia de las instalaciones de procesamiento de información	Los sistemas más críticos cuentan con servidores redundantes o un sitio alterno de procesamiento.	Interrupción prolongada del servicio ante la falla de un único punto.	Ausencia de redundancia en la infraestructura tecnológica crítica.			X		
8.15	**8. Tecnológico**	Registro	Los sistemas de información generan logs de acceso, cambios y eventos que se almacenan de forma centralizada.	Imposibilidad de detectar o investigar accesos indebidos.	Ausencia de logs de auditoría activos y controles de trazabilidad.		X		X	

8.16	**8. Tecnológico**	Actividades de seguimiento	El sistema de monitoreo de seguridad genera alertas ante accesos fuera de horario o desde ubicaciones atípicas.	Comportamiento anómalo no detectado en redes y sistemas.	Ausencia de mecanismos de monitoreo para detectar brechas de seguridad.			X	X	
8.17	**8. Tecnológico**	Sincronización de reloj	Todos los servidores y equipos institucionales sincronizan su hora con un servidor NTP institucional.	Registros de auditoría inconsistentes que dificultan investigar un incidente.	Relojes de los sistemas de información desincronizados entre sí.		X			
8.18	**8. Tecnológico**	Uso de programas de utilidad privilegiados	El uso de herramientas de administración avanzada en los servidores está restringido y registrado.	Anulación de controles de seguridad mediante herramientas privilegiadas.	Uso irrestricto de programas de utilidad con permisos elevados.	X	X		X	
8.19	**8. Tecnológico**	Instalación de software en sistemas operativos	Los usuarios no cuentan con permisos para instalar software no autorizado en los equipos institucionales.	Instalación de software malicioso o no autorizado.	Usuarios con permisos de instalación sin restricción.		X		X	
8.20	**8. Tecnológico**	Seguridad de redes	La red institucional cuenta con firewall perimetral y segmentación entre las redes administrativa y de invitados.	Intrusión o propagación de ataques a través de la red institucional.	Red institucional sin segmentación ni protección perimetral.	X	X	X	X	
8.21	**8. Tecnológico**	Seguridad de los servicios de red	Se identifican y monitorean los niveles de seguridad exigidos a los servicios de internet e intranet contratados.	Compromiso de la seguridad a través de servicios de red mal gestionados.	Servicios de red contratados sin monitoreo de sus mecanismos de seguridad.			X	X	
8.22	**8. Tecnológico**	Segregación de redes	Los sistemas financieros y de nómina operan en un segmento de red distinto al de la red de usuarios general.	Propagación de un ataque desde la red general hacia sistemas críticos.	Redes institucionales sin segregación entre sistemas críticos y de uso general.	X	X		X	
8.23	**8. Tecnológico**	Filtrado web	Se filtran y bloquean sitios web maliciosos o no autorizados desde la red institucional.	Acceso a contenido malicioso que compromete los equipos institucionales.	Ausencia de filtrado de acceso a sitios web externos.				X	
8.24	**8. Tecnológico**	Uso de la criptografía	Las bases de datos con información personal de ciudadanos se cifran en reposo y en tránsito.	Exposición de información sensible en caso de acceso no autorizado.	Información sensible almacenada o transmitida sin cifrado.	X				X
8.25	**8. Tecnológico**	Ciclo de vida de desarrollo seguro	El desarrollo de nuevos aplicativos institucionales sigue lineamientos de seguridad definidos desde el diseño hasta el despliegue.	Introducción de vulnerabilidades desde el desarrollo de software.	Desarrollo de software sin normas de seguridad establecidas.		X		X	
8.26	**8. Tecnológico**	Requisitos de seguridad de las aplicaciones	Todo aplicativo nuevo o adquirido debe cumplir requisitos mínimos de seguridad antes de su aprobación.	Adquisición de aplicaciones con falencias de seguridad.	Ausencia de requisitos de seguridad exigidos en la adquisición o desarrollo.	X	X			
8.27	**8. Tecnológico**	Arquitectura de sistemas seguros y principios de ingeniería	El diseño de la infraestructura tecnológica institucional sigue principios de seguridad por diseño y defensa en profundidad.	Debilidades estructurales que faciliten un ataque a los sistemas.	Arquitectura tecnológica sin principios de seguridad incorporados.	X	X		X	
8.28	**8. Tecnológico**	Codificación segura	Los desarrolladores de la entidad aplican buenas prácticas de codificación segura para prevenir vulnerabilidades comunes.	Explotación de fallas de programación, como la inyección SQL.	Código desarrollado sin prácticas de codificación segura.		X		X	

8.29	**8. Tecnológico**	Pruebas de seguridad en el desarrollo y aceptación	Antes de poner en producción un aplicativo se realizan pruebas de seguridad y de vulnerabilidades.	Despliegue de sistemas con vulnerabilidades no detectadas.	Ausencia de pruebas de seguridad previas a la puesta en producción.		X		X	
8.30	**8. Tecnológico**	Desarrollo externalizado	Los desarrollos contratados con terceros se supervisan y revisan conforme a los estándares de seguridad de la entidad.	Vulnerabilidades introducidas por desarrolladores externos no supervisados.	Falta de supervisión sobre el desarrollo de software subcontratado.		X		X	
8.31	**8. Tecnológico**	Separación de entornos de desarrollo, evidencia y producción	Los ambientes de desarrollo, pruebas y producción de los sistemas de información están claramente separados.	Afectación del ambiente de producción por cambios de desarrollo o pruebas.	Ambientes de desarrollo y de producción no separados.		X	X		
8.32	**8. Tecnológico**	Gestión del cambio	Todo cambio en los sistemas de información sigue un procedimiento formal de solicitud, aprobación y control.	Cambios no controlados que afecten la operación de los sistemas.	Ausencia de un procedimiento de control de cambios.		X	X		
8.33	**8. Tecnológico**	Información de las pruebas	Los datos usados en los ambientes de prueba se seleccionan y protegen para evitar el uso de información sensible real.	Exposición de información real de ciudadanos durante las pruebas de sistemas.	Uso de información sensible sin protección en ambientes de prueba.	X				X
8.34	**8. Tecnológico**	Protección de los sistemas de información durante las pruebas de auditoría	Las auditorías técnicas a los sistemas de producción se planifican y coordinan previamente con el área de TIC.	Afectación de la operación de los sistemas durante actividades de auditoría.	Pruebas de auditoría no planificadas ni coordinadas con los responsables.		X	X		

8.1.7. Indicadores clave de riesgo (KRI) para seguridad de la información

Nombre del KRI	Fórmula	Frecuencia	Responsable	Umbral de alerta
Índice de incidentes de seguridad reportados	(N.° incidentes reportados / N.° total sistemas críticos) × 100	Mensual	Jefe TIC	Rojo: > 1 incidente en sistemas críticos
Porcentaje de cuentas de usuario sin auditoría de perfil	(Cuentas activas sin revisión en 90 días / Total cuentas activas) × 100	Trimestral	Jefe TIC	Amarillo: > 10 %; Rojo: > 20 %
Cobertura de copias de respaldo (backups) de sistemas críticos	(Sistemas críticos con backup verificado y vigente / Total sistemas críticos) × 100	Mensual	Jefe TIC	Amarillo: < 90 %; Rojo: < 80 %
Tiempo promedio de atención de incidentes de seguridad	Promedio de horas entre detección y resolución de incidentes reportados en el período.	Trimestral	Jefe TIC	Amarillo: > 8 h; Rojo: > 24 h
Porcentaje de servidores capacitados en seguridad digital	(Servidores con capacitación en el año / Total servidores con acceso a sistemas) × 100	Semestral	TH / TIC	Amarillo: < 80 %; Rojo: < 60 %

8.2. RIESGOS FISCALES

8.2.1. Marco normativo aplicable

Norma / Instrumento	Disposición aplicable para la Alcaldía de Pasto
Constitución Política, artículo 267	El control fiscal es una función pública orientada a vigilar la gestión fiscal de la administración y de los particulares que manejen fondos o bienes del Estado.
Ley 42 de 1993	Organiza el sistema de control fiscal. Define los principios de la gestión fiscal (eficiencia, economía, equidad, valoración de costos) y establece el concepto de gestor fiscal.
Ley 610 de 2000	Regula el proceso de responsabilidad fiscal: la materialización de un riesgo fiscal puede dar lugar a un proceso sancionatorio ante la Contraloría con fallo de responsabilidad fiscal y cobro coactivo.
Decreto 403 de 2020	Regula el control fiscal y sus modalidades, incluyendo el control preventivo y concomitante de las contralorías. Define el alcance de los gestores fiscales.
Ley 80 de 1993 y Ley 1150 de 2007	Estatuto General de Contratación Pública. Los incumplimientos de sus principios (selección objetiva, transparencia, responsabilidad) son fuente frecuente de riesgos fiscales.
Ley 1474 de 2011 (Estatuto Anticorrupción)	Amplía la responsabilidad de supervisores e interventores en la gestión contractual, haciendo exigible la diligencia debida como mecanismo de prevención del riesgo fiscal.
Guía GIR Versión 7 – DAFP (2025)	Define la categoría de riesgos fiscales como eventos de efecto dañoso sobre los recursos, bienes o intereses patrimoniales de naturaleza pública.

8.2.2. Definición y alcance del riesgo fiscal

De conformidad con la Ley 42 de 1993, el artículo 6 de la Ley 610 de 2000 y la Guía GIR v7 del DAFP, el riesgo fiscal en la Alcaldía de Pasto se define como la posibilidad de un efecto dañoso sobre los recursos, bienes o intereses patrimoniales del municipio, derivado de una gestión fiscal antieconómica, ineficaz, ineficiente o inoportuna, por acción u omisión de los servidores públicos o contratistas en el ejercicio de sus funciones.

El riesgo fiscal aplica a todo proceso de la Alcaldía de Pasto en el que exista manejo, custodia, recaudo, administración, inversión, disposición o gasto de recursos públicos, sin

importar la naturaleza del proceso. Las situaciones que generan con mayor frecuencia este tipo de riesgo son:

- Procesos de contratación: anticipos no amortizados, pagos sin cumplimiento del objeto contractual, contratos sin supervisión efectiva, procesos sin el procedimiento de selección legal correspondiente.
- Procesos de planeación presupuestal y financiera: adiciones sin sustento técnico, compromisos sin disponibilidad presupuestal, subejecución injustificada al cierre de la vigencia.
- Procesos de tesorería y recaudo: pagos a terceros no autorizados, conciliaciones bancarias con diferencias sin justificar, cartera tributaria sin gestión oportuna de cobro coactivo.
- Procesos de gestión de bienes: pérdida, hurto o deterioro de bienes públicos sin la diligencia debida; bienes no registrados en el inventario institucional.
- Procesos misionales con asignación de recursos del Sistema General de Participaciones (SGP): inversión de recursos en actividades no permitidas o en destinaciones distintas a las definidas legalmente para cada sector.

Tolerancia institucional:
La tolerancia para los riesgos fiscales es MUY BAJA, conforme a la tabla del numeral 6.2 del presente manual. Cualquier riesgo fiscal con nivel residual Moderado o superior requiere plan de tratamiento obligatorio y reporte inmediato a la Oficina de Control Interno. La materialización de un riesgo fiscal puede dar lugar al inicio de un proceso de responsabilidad fiscal ante la Contraloría competente.

8.2.3. Criterios de impacto específicos para riesgos fiscales

Para los riesgos fiscales el impacto se mide en términos económicos (SMLMV), conforme a la escala general del manual. Se deben considerar adicionalmente las implicaciones del proceso de responsabilidad fiscal derivado de la Ley 610 de 2000:

Nivel de impacto	Consecuencia fiscal potencial	Implicación en el proceso de responsabilidad fiscal – Ley 610 de 2000
Leve (< 10 SMLMV)	Detrimento menor. Puede ser subsanable mediante reintegro.	Puede generar hallazgo administrativo de ente de control. No necesariamente da lugar a proceso de responsabilidad fiscal.
Menor (10–50 SMLMV)	Detrimento con posibilidad de proceso leve.	Indagación preliminar de la Contraloría competente.
Moderado (50–100 SMLMV)	Detrimento significativo. Requiere acciones correctivas inmediatas.	Inicio formal del proceso de responsabilidad fiscal.

Nivel de impacto	Consecuencia fiscal potencial	Implicación en el proceso de responsabilidad fiscal – Ley 610 de 2000
Mayor (100–500 SMLMV)	Pérdida grave. Posibilidad de responsabilidad solidaria de supervisores y ordenadores del gasto.	Proceso de responsabilidad fiscal con posibilidad de medidas cautelares sobre bienes del presunto responsable.
Catastrófico (> 500 SMLMV)	Pérdida masiva. Afectación directa de la ejecución del Plan de Desarrollo Municipal.	Proceso de responsabilidad fiscal con fallo con responsabilidad y cobro coactivo.

8.2.4. Articulación con los entes de control fiscal

La gestión de riesgos fiscales debe articularse de manera permanente con:

- Contraloría Municipal de Pasto y Contraloría General de la República (según competencias): ejercen el control preventivo, concomitante y posterior sobre la gestión fiscal de la entidad. Los hallazgos fiscales de sus informes deben retroalimentar directamente los mapas de riesgos de los procesos auditados y generar la actualización inmediata de los controles identificados.
- Planes de mejoramiento derivados de hallazgos fiscales: las acciones correctivas comprometidas en planes de mejoramiento ante las contralorías constituyen planes de tratamiento de riesgos fiscales materializados y deben registrarse en el mapa de riesgos institucional, sin que ninguna de ellas pueda quedar por fuera del sistema de seguimiento de la entidad.
- Comité Institucional de Gestión y Desempeño: debe revisar periódicamente los riesgos fiscales de nivel Alto o Extremo y definir prioridades de tratamiento, con participación del secretario de Hacienda y los líderes de los procesos con mayor exposición fiscal.
- Oficina de Control Interno: evalúa independientemente la efectividad de los controles sobre riesgos fiscales y emite alertas tempranas a la Alta Dirección cuando los indicadores de riesgo superen los umbrales definidos.

B.5. Indicadores clave de riesgo (KRI) para riesgos fiscales

Nombre del KRI	Fórmula	Frecuencia	Responsable	Umbral de alerta
Índice de ejecución presupuestal de inversión	(Valor ejecutado / Valor apropiado vigente) × 100	Mensual	Sec. Hacienda	Amarillo: < 70 %; Rojo: < 50 % al

Nombre del KRI	Fórmula	Frecuencia	Responsable	Umbral de alerta
				cierre del III trimestre
Porcentaje de anticipos sin legalizar en contratos vigentes	(Valor de anticipos sin amortizar / Valor total de anticipos vigentes) × 100	Mensual	Sec. Hacienda / Contratación	Amarillo: > 10 %; Rojo: > 20 %
Tasa de crecimiento de la cartera tributaria sin cobro coactivo	((Cartera actual – Cartera período anterior) / Cartera período anterior) × 100	Trimestral	Sec. Hacienda	Amarillo: > 5 %; Rojo: > 15 %
Porcentaje de contratos vigentes con supervisión formalizada	(Contratos con supervisor designado y actas al día / Total contratos vigentes) × 100	Mensual	Depto. Contratación	Amarillo: < 90 %; Rojo: < 80 %
Hallazgos fiscales de Contraloría con acciones vencidas	(Hallazgos con plazo de acción vencido / Total hallazgos fiscales activos) × 100	Bimestral	Control Interno	Amarillo: > 5 %; Rojo: > 15 %

8.3. RIESGOS PARA LA INTEGRIDAD PÚBLICA – SIGRIP Y PTEP

8.3.1. Marco normativo aplicable

Norma / Instrumento	Disposición aplicable para la Alcaldía de Pasto
Ley 2195 de 2022, artículo 31	Modifica el artículo 73 de la Ley 1474 de 2011 y crea la obligación de implementar el Programa de Transparencia y Ética Pública (PTEP) para todas las entidades del orden nacional, departamental y municipal.
Decreto 1122 de 2024	Reglamenta el artículo 73 de la Ley 1474 de 2011 modificado por la Ley 2195 de 2022. Establece la metodología, estructura y Anexo Técnico del PTEP. Deroga expresamente las normas sobre el Plan Anticorrupción y Atención al Ciudadano (PAAC). Toda mención al PAAC en normas o documentos se entiende referida al PTEP.
Ley 1474 de 2011 (Estatuto Anticorrupción), artículo 73	Define las acciones que debe contener el PTEP, agrupadas en cuatro temáticas: administración de riesgos, redes y

Norma / Instrumento	Disposición aplicable para la Alcaldía de Pasto
	articulación, cultura de legalidad y Estado Abierto, e iniciativas adicionales.
Ley 734 de 2002 (Código Disciplinario Único)	Regula las faltas disciplinarias relacionadas con conflictos de interés, abuso del cargo, omisión y corrupción.
Ley 599 de 2000 (Código Penal)	Tipifica los delitos contra la administración pública: cohecho, concusión, peculado, celebración indebida de contratos, tráfico de influencias, entre otros.
Código de Integridad – DAFP	Define los valores del servidor público. Su apropiación constituye el primer nivel de control preventivo frente a conductas que materializan amenazas a la integridad.
Guía GIR Versión 7 – DAFP (2025)	Redefine los riesgos de corrupción como «riesgos para la integridad pública» y los articula con el SIGRIP y el PTEP como componentes del mapa de riesgos institucional.

8.3.2. El PTEP y el SIGRIP: qué son y cómo se articulan con el mapa de riesgos

El Programa de Transparencia y Ética Pública (PTEP) es el instrumento obligatorio mediante el cual la Alcaldía de Pasto define e implementa acciones para promover una cultura de la legalidad e identificar, medir, controlar y monitorear los riesgos para la integridad que se presentan en el desarrollo de su misionalidad. Fue creado por el Decreto 1122 de 2024, que derogó el anterior Plan Anticorrupción y de Atención al Ciudadano (PAAC), sustituyéndolo en su totalidad. Toda referencia al PAAC en normas o documentos institucionales de la Alcaldía de Pasto debe entenderse referida al PTEP.

El PTEP se estructura en dos componentes definidos en su Anexo Técnico: el Componente Transversal, que establece las condiciones institucionales permanentes (declaración, planeación, supervisión, formación, comunicación y auditoría), y el Componente Programático, que contiene las acciones estratégicas anuales agrupadas en cuatro temáticas: administración de riesgos, redes y articulación, legalidad y Estado Abierto, e iniciativas adicionales.

El Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) es la acción estratégica de administración de riesgos dentro del Componente Programático del PTEP. No reemplaza el mapa de riesgos institucional: sus resultados se integran al mapa de riesgos de cada proceso de la Alcaldía de Pasto, en la categoría «Riesgos para la Integridad Pública» definida en el numeral 6.4 del presente manual.

Instrumento	Función y articulación con el mapa de riesgos de la Alcaldía de Pasto
PTEP – Componente Transversal	Establece las condiciones institucionales permanentes para la ética pública: declaración de integridad, planeación, supervisión, formación, comunicación interna y auditoría. Aplica de manera continua, no anual.
PTEP – Componente Programático	Contiene las acciones estratégicas anuales del PTEP. El SIGRIP es su primera temática (administración de riesgos). Las acciones del componente programático deben estar alineadas con los controles y planes de tratamiento del mapa de riesgos institucional.
SIGRIP	Sistema metodológico para identificar, evaluar, tratar y hacer seguimiento a las amenazas a la integridad pública. Sus resultados se registran en el mapa de riesgos de cada proceso, articulados con la metodología de 11 pasos del presente manual.
Mapa de riesgos institucional	Registro consolidado de todos los riesgos. Los riesgos para la integridad identificados bajo el SIGRIP hacen parte integral del mapa de cada proceso y se gestionan con la misma metodología general, con los criterios adicionales de este capítulo.
Código de Integridad	Complemento cultural: define los valores y comportamientos que previenen conductas que materializan amenazas a la integridad. Su apropiación es el primer mecanismo de control preventivo del SIGRIP.

Precisión normativa importante:
El Decreto 1122 de 2024, artículo 4, deroga expresamente los artículos 2.1.4.1 a 2.1.4.9 del Decreto 1081 de 2015, que regulaban el PAAC. El artículo 2.1.4.4.1.5 establece que toda mención que se haga en normas o en cualquier otro documento al Plan Anticorrupción y Atención al Ciudadano se entiende referida al Programa de Transparencia y Ética Pública. Por tanto, en ningún documento institucional de la Alcaldía de Pasto se debe usar el término PAAC.

8.3.3. Amenazas a la integridad pública gestionadas bajo el SIGRIP

Conforme al Decreto 1122 de 2024 y la Guía GIR v7, las amenazas a la integridad pública que deben identificarse y gestionarse bajo el SIGRIP en todos los procesos de la Alcaldía de Pasto son:

Amenaza a la integridad	Descripción	Ejemplo orientador (aplicable a cualquier proceso)
Corrupción	Desviación de la gestión pública para obtener beneficios propios o de terceros, en detrimento del interés general y del patrimonio público.	Posibilidad de direccionamiento irregular en un proceso de contratación a favor de intereses particulares de un servidor, debido a la ausencia de mecanismos plurales de evaluación e independencia en el proceso.
Soborno	Ofrecimiento o aceptación de pagos, dádivas o beneficios indebidos a cambio de favores en el ejercicio de la función pública.	Posibilidad de recepción de prebendas por parte de servidores en la asignación de beneficios, permisos o decisiones discrecionales, debido a la falta de controles de transparencia en la toma de decisiones.
Fraude	Falsedad o engaño doloso en documentos, informes, registros o procedimientos institucionales para obtener un beneficio indebido o evadir una responsabilidad.	Posibilidad de alteración de registros o datos reportados en sistemas de información para mostrar resultados distintos a los reales, debido a la ausencia de verificación cruzada de fuentes y auditorías de integridad de datos.
Conflicto de intereses	Situaciones en las que el interés particular del servidor colisiona con su deber público, sin que medie declaración formal del impedimento.	Posibilidad de participación de un servidor en la evaluación de una decisión en la que tenga vínculos con los interesados, sin haber declarado oportunamente el impedimento correspondiente.
LA/FT/FP	Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva. Tolerancia institucional: cero.	Posibilidad de uso de contratos, convenios o proyectos de inversión para el ingreso de recursos de origen ilícito al sistema financiero del municipio, debido a controles insuficientes en la verificación de la procedencia de recursos y la identidad de contratistas.

8.3.4. Criterios especiales de evaluación de las amenazas a la integridad

La evaluación de las amenazas a la integridad aplica la misma metodología de probabilidad e impacto del manual, con los siguientes criterios adicionales obligatorios:

- Tolerancia cero para corrupción y LA/FT/FP: independientemente del resultado cuantitativo de la evaluación, cualquier amenaza de estos tipos SIEMPRE requiere controles definidos y un plan de tratamiento activo. No existe zona de riesgo aceptable sin gestión para estas categorías.
- Evaluación del contexto de integridad: el análisis debe incluir factores que elevan la exposición a amenazas de integridad, tales como: volumen de recursos manejados, nivel de discrecionalidad en decisiones, historial de denuncias o investigaciones previas en el proceso y existencia o ausencia de mecanismos de control social y ciudadano.
- Análisis de conflictos de interés: el líder del proceso debe revisar si existen mecanismos formales y activos de declaración de conflictos de interés, y si los servidores los conocen y aplican efectivamente.
- Articulación con el Componente Programático del PTEP: los controles y planes de tratamiento de las amenazas identificadas en el SIGRIP deben estar reflejados y alineados en las acciones del Componente Programático anual del PTEP de la Alcaldía de Pasto.

8.3.5. Acciones del Componente Programático del PTEP expresadas como controles en el mapa de riesgos

Las acciones del Componente Programático del PTEP deben traducirse en controles concretos en el mapa de riesgos del SIGRIP. A continuación, se presentan las principales acciones estratégicas con su expresión como controles institucionales:

Acción estratégica del PTEP	Expresión como control en el mapa de riesgos institucional	Aplicabilidad
1.1 Gestión de riesgos para la integridad pública (SIGRIP)	Los líderes de proceso identifican, evalúan y tratan las amenazas a la integridad en sus mapas de riesgos, con la metodología del presente capítulo, y reportan avances al Comité Institucional de Gestión y Desempeño.	Todos los procesos de la Alcaldía.
1.2 Gestión de riesgos de LA/FT/FP	El jefe del Departamento de Contratación verifica la debida diligencia sobre los contratistas (verificación de antecedentes, origen de recursos y listas de control), con registro en el expediente contractual.	Todos los procesos con capacidad contractual.
1.3 Canales de denuncia	La Oficina de Control Interno verifica bimestralmente el funcionamiento del	Transversal a toda la entidad.

Acción estratégica del PTEP	Expresión como control en el mapa de riesgos institucional	Aplicabilidad
	canal de denuncias institucional y reporta al Comité de Gestión y Desempeño el número, tipo y estado de gestión de las denuncias recibidas.	
1.4 Debida diligencia	El líder del proceso verifica trimestralmente que todos los servidores de su equipo hayan actualizado su declaración de conflicto de interés, dejando evidencia en el expediente de gestión de personal.	Procesos con decisiones discrecionales de alto impacto.
Rotación en cargos de alto riesgo (temática: administración de riesgos)	El secretario o director de la dependencia garantiza la rotación periódica de servidores con funciones de manejo de recursos, evaluación de proveedores o toma de decisiones de alta discrecionalidad.	Tesorería, contratación, pagaduría, asignación de beneficios.
Formación en integridad y Código de Integridad (temática: cultura de legalidad)	La Oficina de Talento Humano certifica anualmente que el 100 % de los servidores de procesos con amenazas de integridad calificadas como Alta o Extrema han recibido formación en ética pública y Código de Integridad.	Todos los procesos, énfasis en contratación y hacienda.
Transparencia en la contratación (temática: Estado Abierto)	El jefe del Departamento de Contratación verifica que el 100 % de los procesos de selección estén publicados íntegramente y oportunamente en el SECOP II antes de cada etapa del proceso.	Proceso de contratación y procesos con capacidad contractual.

8.3.6. Indicadores clave de riesgo (KRI) para riesgos de integridad – SIGRIP

Nombre del KRI	Fórmula	Frecuencia	Responsable	Umbral de alerta
Porcentaje de servidores con declaración de conflicto de interés vigente	(Servidores con declaración actualizada / Total servidores de planta y contratistas) × 100	Trimestral	Talento Humano	Amarillo: < 90 %; Rojo: < 80 %

Nombre del KRI	Fórmula	Frecuencia	Responsable	Umbral de alerta
Porcentaje de denuncias recibidas atendidas oportunamente	(Denuncias atendidas en plazo / Total denuncias recibidas) × 100	Bimestral	Control Interno	Amarillo: < 90 %; Rojo: < 70 %
Número de investigaciones disciplinarias o penales activas por conductas de integridad	N.° de procesos disciplinarios o penales activos por corrupción, fraude, soborno o conflicto de intereses en el período.	Semestral	Control Interno / Jurídica	Rojo: cualquier valor > 0 activa la revisión del mapa del proceso involucrado.
Cobertura del Componente Programático del PTEP ejecutado	(Acciones del PTEP ejecutadas en el período / Total acciones comprometidas en el período) × 100	Semestral	OPGI	Amarillo: < 80 %; Rojo: < 60 %
Porcentaje de procesos contractuales con publicación completa en SECOP II	(Procesos con publicación completa y oportuna / Total procesos adelantados) × 100	Mensual	Depto. Contratación	Amarillo: < 95 %; Rojo: < 85 %

8.4. SEGUIMIENTO, REPORTE Y RESPONSABILIDADES PARA LAS TRES CATEGORÍAS

8.4.1. Instancias de seguimiento bajo el modelo de tres líneas de defensa

Línea de defensa	Actores responsables	Función específica frente a estas tres categorías
Primera línea – Gestión operativa	Líderes de proceso y servidores de cada dependencia.	Identifican, actualizan y aplican controles en los riesgos de SI, fiscales y de integridad de sus procesos. Reportan incidentes e irregularidades oportunamente a la OPGI y a Control Interno.
Segunda línea – Orientación y seguimiento	OPGI (riesgos de integridad y fiscales), Oficina de TIC (seguridad de la información), Secretaría de Hacienda (riesgos fiscales).	Consolidan y analizan información de riesgos. Brindan acompañamiento metodológico. Monitorean los KRI. Emiten alertas tempranas a la Alta Dirección ante señales de deterioro.
Tercera línea – Evaluación independiente	Oficina de Control Interno de Gestión.	Evalúa independientemente la efectividad de los controles de las tres categorías. Verifica la correcta aplicación del SIGRIP, el Componente Transversal del PTEP y la normativa fiscal. Emite informes a la Alta Dirección.

8.4.2. Frecuencia de seguimiento diferenciada por categoría y nivel de riesgo residual

Categoría de riesgo	Seguimiento mínimo nivel Alto o Extremo	Seguimiento mínimo nivel bajo o moderado	Reporte al Comité Institucional de Gestión y Desempeño
Seguridad de la información	Cuatrimestral (líder de proceso).	Cuatrimestral (líder de proceso).	Semestral.
Riesgos fiscales	Cuatrimestral (líder de proceso).	Cuatrimestral (líder de proceso).	Semestral.
Integridad pública – SIGRIP	Cuatrimestral (líder de proceso).	Cuatrimestral (líder de proceso).	Semestral.

9. MATERIALIZACIÓN DE RIESGOS

9.1. Marco Normativo Aplicable

La gestión de la materialización de riesgos en la Alcaldía de Pasto se rige por el siguiente marco normativo:

- **Ley 87 de 1993 – Control Interno:** Obliga a las entidades públicas a establecer mecanismos que permitan detectar, corregir y prevenir fallas en la gestión, incluyendo los eventos adversos que se materialicen.
- **Ley 610 de 2000 – Responsabilidad Fiscal:** Regula el proceso de responsabilidad fiscal ante las Contralorías. La materialización de un riesgo fiscal puede dar lugar a un proceso de responsabilidad fiscal con fallo y cobro coactivo. Obliga a los gestores fiscales a reponer los recursos públicos afectados por una gestión fiscal antieconómica, ineficaz o inoportuna.
- **Decreto 403 de 2020:** Regula el control fiscal preventivo y concomitante. Las Contralorías pueden intervenir en tiempo real cuando detecten riesgos de pérdida de recursos públicos o materializaciones en curso, y emitir alertas tempranas a la entidad para activar acciones correctivas inmediatas.
- **Ley 1474 de 2011 – Estatuto Anticorrupción:** Establece la responsabilidad reforzada de supervisores, interventores y ordenadores del gasto. La omisión en la supervisión que permita la materialización de un riesgo, especialmente fiscal o de integridad, puede acarrear sanciones disciplinarias, penales y fiscales.
- **Decreto 1122 de 2024 – PTEP y SIGRIP:** Ante la materialización de riesgos para la integridad pública, la entidad debe asegurar la continuidad del servicio, actualizar de inmediato el mapa de riesgos y articular las acciones correctivas con el Componente Programático del PTEP, sin perjuicio de las actuaciones que correspondan a otras autoridades.
- **Decreto 1499 de 2017 – MIPG:** Exige que la materialización de un riesgo sea un disparador inmediato de actualización del mapa de riesgos y de fortalecimiento del sistema de control interno, como parte del ciclo de mejora continua PHVA.
- **Guía de Gestión Integral del Riesgo – Versión 7 (DAFP, 2025):** Define la materialización como un riesgo gestionado (evento ocurrido) y establece que la respuesta institucional debe priorizar la continuidad del servicio, el análisis de causa raíz, el rediseño de controles y la consolidación de una base histórica de eventos para el fortalecimiento de los indicadores clave de riesgo (KRI).
- **Ley 734 de 2002 – Código Disciplinario Único:** La omisión en el reporte oportuno de riesgos materializados, el incumplimiento de los controles establecidos o la falta de activación de la ruta de actuación por parte del líder del proceso pueden constituir faltas disciplinarias graves, susceptibles de sanción por parte de la Procuraduría General de la Nación.

- **Ley 1581 de 2012 (Protección de Datos Personales):** Cuando la materialización involucre una brecha de seguridad de información o vulneración de datos personales de ciudadanos, la Alcaldía de Pasto deberá notificar a la Superintendencia de Industria y Comercio (SIC) en los términos del artículo 17 de la ley, adicionalmente a la ruta interna de actuación.

9.2. Definición, Alcance y Naturaleza de la Materialización

La materialización de un riesgo ocurre cuando el evento identificado en el mapa de riesgos —que era una posibilidad— se convierte en un hecho real que genera un impacto negativo sobre los objetivos, los recursos, la integridad institucional o la prestación de servicios a la ciudadanía de la Alcaldía de Pasto. En este momento, la gestión del riesgo pasa de una fase preventiva a una fase de respuesta correctiva, continuidad del servicio y aprendizaje institucional.

Conforme a la Guía de Gestión Integral del Riesgo v7 del DAFP, se debe tener en cuenta que la materialización del riesgo no debe confundirse con la ocurrencia de un delito, falta disciplinaria o conducta generadora de responsabilidad fiscal. Es posible que el riesgo se haya materializado —es decir, que haya un impacto negativo real sobre los objetivos— incluso antes de la vinculación formal a procesos sancionatorios. Por lo anterior, la gestión de la materialización no implica un prejuzgamiento ni sustituye las actuaciones de las autoridades competentes (Contralorías, Procuraduría, Fiscalía), sino que opera de manera complementaria y autónoma, centrada en asegurar la continuidad institucional y la correción de la gestión.

Para los riesgos para la integridad pública (SIGRIP), el riesgo se considera materializado siempre que se advierta un impacto sobre la reputación, la operación, el cumplimiento normativo o que comprometa la ejecución del recurso público, incluyendo las consecuencias de contagio derivadas de actuaciones de partes relacionadas. En el caso del riesgo de LA/FT/FP, toda operación sospechosa —incluso la intentada— debe ser objeto de reporte a las autoridades competentes, independientemente de la materialización del delito.

9.3. Detección y Fuentes de Identificación de Eventos Materializados

La detección oportuna de la materialización de un riesgo es una responsabilidad de todas las líneas de defensa. Un evento materializado puede identificarse a través de las siguientes fuentes:

- **Autodetección por el líder del proceso:** durante la ejecución diaria de actividades o en el ejercicio de revisión mensual de equipos primarios.
- **Activación de un KRI (Indicador Clave de Riesgo):** cuando el indicador supera el umbral rojo definido en el mapa de riesgos, lo cual sugiere que algo no funciona adecuadamente o que el riesgo ya ocurrió.

- **Sistema de PQRD (Peticiones, Quejas, Reclamos y Denuncias):** quejas reiteradas de ciudadanos o usuarios que evidencien fallas en la prestación del servicio asociadas a un riesgo identificado.
- **Canal de denuncias institucional:** reportes de servidores, ciudadanos o terceros sobre conductas o situaciones que constituyen la materialización de un riesgo de integridad.
- **Informe de auditoría o hallazgo de la Oficina de Control Interno:** cuando en el ejercicio de evaluación independiente se detecta la ocurrencia de un evento adverso que corresponde a un riesgo del mapa institucional.
- **Hallazgo fiscal, disciplinario o penal de ente de control externo:** cuando la Contraloría Municipal, la Contraloría General de la República o la Procuraduría formulan hallazgos que evidencian la ocurrencia de un evento de riesgo en los procesos de la entidad.
- **Mesa de ayuda o reportes TIC:** incidentes de seguridad digital, interrupción de sistemas críticos o pérdida de información que activan la ruta de materialización de riesgos de seguridad de la información.

9.4. Ruta Institucional de Actuación ante la Materialización

Ante la ocurrencia o detección de un riesgo materializado, la Alcaldía de Pasto activa de inmediato la siguiente ruta institucional de actuación, bajo el esquema de tres líneas de defensa. Esta ruta es de obligatorio cumplimiento para todos los procesos y dependencias:

- **PASO 1 – Notificación Inmediata (máximo 48 horas):** El Líder del Proceso que detecte o conozca la materialización de un riesgo debe informar de manera inmediata, y en un plazo no mayor a cuarenta y ocho (48) horas, a la Oficina de Planeación de Gestión Institucional (OPGI) y a la Oficina de Control Interno (OCI). La notificación debe realizarse mediante comunicación escrita (correo electrónico institucional, oficio o acta de equipo primario), indicando el riesgo afectado, la fecha de ocurrencia y una descripción preliminar del evento. La omisión de este reporte puede constituir falta disciplinaria en los términos de la Ley 734 de 2002.
- **PASO 2 – Continuidad del Servicio (inmediato):** El Líder del Proceso, con el apoyo de la OPGI, debe activar de manera inmediata las medidas de contingencia necesarias para asegurar la continuidad del servicio público y evitar que el impacto se extienda o profundice. La protección de la prestación del servicio a la ciudadanía es la prioridad, independientemente de las investigaciones o procesos sancionatorios que puedan iniciarse.
- **PASO 3 – Diligenciamiento del Formato de Reporte (máximo 5 días hábiles):** El Líder del Proceso diligencia el Formato de Reporte de Riesgos Materializados (código

F-PE-28) con la información detallada del evento. Este formato debe ser remitido a la OPGI dentro de los cinco (5) días hábiles siguientes a la notificación inicial. La OPGI lo revisará, consolidará y reportará a la OCI.

- **PASO 4 – Análisis de Causa Raíz (máximo 10 días hábiles):** La OPGI convocará una mesa de trabajo con el Líder del Proceso y la OCI para realizar el análisis de causa raíz del evento mediante la técnica de los "5 Por qués" u otras metodologías de análisis de causa (diagrama de Ishikawa, árbol de problemas). No basta con saber qué pasó; se debe profundizar hasta identificar el fallo sistémico que permitió la ocurrencia del evento. Las causas raíz pueden ser de naturaleza humana, tecnológica, normativa, organizacional o ambiental.
- **PASO 5 – Valoración del Impacto Real:** Se cuantifica el impacto real del evento en términos económicos (en SMLMV, conforme a la Ley 42 de 1993 y la Ley 610 de 2000 para efectos de posible responsabilidad fiscal), reputacionales (quejas, denuncias, notas de prensa), operativos (interrupción del servicio, demoras en trámites) y de cumplimiento (sanciones, incumplimientos normativos). Para riesgos de integridad, se deben evaluar adicionalmente las consecuencias de contagio hacia otras áreas o entidades relacionadas.
- **PASO 6 – Actualización Inmediata del Mapa de Riesgos:** La materialización de un riesgo es un disparador obligatorio e inmediato de actualización del mapa de riesgos, sin esperar al próximo ciclo cuatrimestral de monitoreo. El riesgo materializado debe ser reevaluado: si el evento ocurrió, es evidencia de que los controles fueron ineficaces o insuficientes, por lo que deben ser rediseñados. La OPGI brinda los lineamientos metodológicos para la actualización del mapa de riesgos del proceso afectado.
- **PASO 7 – Formulación del Plan de Mejoramiento:** En el marco de la mesa de trabajo entre la OPGI, la OCI y el proceso afectado, se formula el plan de mejoramiento derivado del riesgo materializado. Este plan debe establecer acciones correctivas concretas, responsables, recursos y plazos definidos para evitar la repetición del evento. Si el riesgo materializado involucra hallazgos de entes de control externo (Contraloría, Procuraduría), el plan de mejoramiento comprometido ante dichas entidades debe registrarse en el mapa de riesgos institucional como plan de tratamiento activo, con seguimiento cuatrimestral obligatorio.
- **PASO 8 – Seguimiento al Plan de Mejoramiento y Registro en Base Histórica:** La OCI realiza seguimiento al cumplimiento del plan de mejoramiento. El evento materializado se registra en la base histórica de eventos de la entidad, la cual constituye un insumo fundamental para el fortalecimiento de los Indicadores Clave de Riesgo (KRI), el ajuste de los umbrales de alerta y la mejora continua del sistema de gestión integral del riesgo.
- **PASO 9 – Elevación a instancias superiores (cuando aplique):** Si la materialización involucra riesgos de nivel alto o crítico, pérdida de recursos públicos, riesgos de

integridad o situaciones que comprometan la imagen institucional, la OCI debe elevar el caso al Comité Institucional de Coordinación de Control Interno (CICCI) para que se adopten decisiones estratégicas de corrección y fortalecimiento del sistema. El Comité Institucional de Gestión y Desempeño (CIGD) debe ser informado cuando la materialización afecte metas del Plan de Desarrollo Municipal.

9.5. Estructura del Reporte de Materialización (Formato F-PE-28)

Para cada evento materializado, el Líder del Proceso debe diligenciar el Formato de Reporte de Riesgos Materializados (código F-PE-28) con la siguiente información mínima:

- **Identificación del proceso y del riesgo:** nombre del proceso, código del riesgo en el mapa vigente y transcripción fiel de la descripción del riesgo afectado.
- **Descripción de los hechos:** relato objetivo del evento (Qué, Cómo, Cuándo, Dónde), sin juicios de responsabilidad individual.
- **Tipo y categoría del riesgo materializado:** riesgo de gestión, fiscal, de integridad pública (SIGRIP), de seguridad de la información u otro.
- **Causas de la materialización:** resultado del análisis de causa raíz (técnica de los "5 Por qués" u otras), diferenciando la causa raíz de las causas inmediatas.
- **Consecuencias del evento:** impacto económico real (en SMLMV si aplica), reputacional, operativo y de cumplimiento.
- **Estado del control fallido:** descripción del control que debía prevenir o detectar el evento, razón por la cual no fue efectivo y valoración de su efectividad real.
- **Medidas de contingencia adoptadas:** acciones inmediatas tomadas para detener el daño, proteger el servicio y preservar evidencias.
- **Acciones correctivas propuestas (Plan de Mejoramiento):** acciones definidas para evitar la repetición del evento, con responsable, plazo y recursos requeridos.
- **Notificaciones externas requeridas:** indicar si el evento requiere notificación a la Superintendencia de Industria y Comercio (brecha de datos), a la Contraloría (pérdida fiscal), o a otras autoridades competentes, con registro de la fecha y medio de notificación.

9.6. Reporte Cuatrimestral de Riesgos Materializados a la Oficina de Control Interno

Sin perjuicio del reporte inmediato establecido en el Paso 1 de la ruta de actuación, la Alcaldía de Pasto establece como parte del ciclo ordinario de monitoreo un reporte cuatrimestral consolidado de riesgos materializados, alineado con la frecuencia de seguimiento y monitoreo definida en el Paso 11 de la metodología y en el Procedimiento de Monitoreo de Riesgos (PE-P-015). Este reporte opera bajo el siguiente esquema:

- **Periodicidad:** CUATRIMESTRAL. Los tres cuatrimestres del año son: enero-abril, mayo-agosto y septiembre-diciembre. La OPGI debe enviar el informe consolidado a la Oficina de Control Interno dentro de los primeros quince (15) días del mes siguiente al cierre de cada cuatrimestre (mayo, septiembre y enero del siguiente año).
- **Contenido del informe cuatrimestral de materializaciones:** número y tipo de riesgos materializados en el período; proceso(s) afectado(s); nivel de impacto real; estado del plan de mejoramiento; controles rediseñados; lecciones aprendidas; actualizaciones al mapa de riesgos realizadas; y notificaciones externas efectuadas a entes de control o autoridades durante el cuatrimestre.
- **Responsable de la consolidación:** El equipo de trabajo de MIPG de la OPGI, con el apoyo de los líderes de proceso. El Jefe de la OPGI aprueba el informe antes de remitirlo a la OCI.
- **Revisión por la OCI:** la Oficina de Control Interno revisa el informe consolidado, verifica la suficiencia de las acciones correctivas adoptadas y, si detecta situaciones críticas, omisión de controles o patrones de recurrencia, eleva la situación al Comité Institucional de Coordinación de Control Interno (CICCI) mediante oficio formal.
- **Base histórica de eventos:** la OPGI mantiene y actualiza cuatrimestralmente la base histórica de riesgos materializados de la entidad. Esta base, alimentada con los reportes PE-F-28 de cada proceso, es el insumo principal para la revisión y ajuste de los Indicadores Clave de Riesgo (KRI) y para la evaluación anual de madurez de la gestión integral del riesgo.

9.7. Responsabilidades por Líneas de Defensa ante la Materialización

- **Primera línea – Líder del Proceso y servidores públicos:** detectar y notificar la materialización en máximo 48 horas; activar medidas de contingencia inmediatas; diligenciar el formato F-PE-28; participar en el análisis de causa raíz; ejecutar las acciones correctivas del plan de mejoramiento; actualizar el mapa de riesgos del proceso con el acompañamiento de la OPGI; reportar avances en la reunión mensual de equipos primarios.
- **Segunda línea – OPGI y otras instancias de segunda línea:** recibir y revisar el reporte PE-F-28; convocar la mesa de trabajo para el análisis de causa raíz; brindar lineamientos metodológicos para la formulación del plan de mejoramiento y la actualización del mapa de riesgos; informar a la OCI; consolidar el informe cuatrimestral de materializaciones; mantener la base histórica de eventos; emitir alertas tempranas a la Alta Dirección cuando los patrones de materialización indiquen fallas sistémicas.

- **Tercera línea – Oficina de Control Interno:** evaluar de manera independiente la suficiencia e idoneidad de las acciones correctivas adoptadas; verificar el cumplimiento del plan de mejoramiento; elevar al CICCI los casos críticos; incluir los riesgos materializados en la agenda de auditoría basada en riesgos; emitir informe a la Alta Dirección sobre el comportamiento institucional de la materialización de riesgos.
- **Alta Dirección y Comités (CICCI y CIGD):** analizar los riesgos materializados de nivel alto o crítico; tomar decisiones estratégicas sobre la asignación de recursos para la corrección; aprobar ajustes en la política y apetito al riesgo cuando los patrones de materialización así lo justifiquen; revisar el cumplimiento de planes de mejoramiento comprometidos ante entes de control externo.

9.8. Aprendizaje Institucional y Mejora Continua a partir de la Materialización

La Alcaldía de Pasto entiende la materialización de un riesgo no solo como un evento adverso, sino como una oportunidad de aprendizaje institucional y de fortalecimiento progresivo de la gestión integral del riesgo. En este sentido, la información derivada de cada evento materializado debe alimentar los siguientes mecanismos de mejora continua:

- **Actualización de los Indicadores Clave de Riesgo (KRI):** cada materialización es un dato histórico que permite revisar si los umbrales de alerta del KRI asociado al riesgo eran adecuados, y ajustarlos para anticipar mejor eventos futuros similares.
- **Revisión y rediseño de controles:** los controles que fallaron en prevenir o detectar el evento deben ser rediseñados, priorizando la migración de controles manuales a controles automáticos cuando sea posible, en concordancia con las acciones de fortalecimiento de la madurez de la gestión integral del riesgo.
- **Capacitación dirigida:** cuando la causa raíz de la materialización involucre deficiencias en el conocimiento o aplicación de procedimientos por parte de los servidores, la Subsecretaria de Talento Humano y la OPGI deben incluir una jornada de formación específica en el plan de capacitación institucional del siguiente cuatrimestre.
- **Socialización de lecciones aprendidas:** la OPGI incluirá en el informe cuatrimestral un apartado de "lecciones aprendidas" derivadas de los riesgos materializados en el período, con carácter informativo para todos los procesos de la entidad, con el fin de fortalecer la cultura de prevención y el aprendizaje organizacional.
- **Insumo para la evaluación de madurez:** la dimensión "Resiliencia y Mejora" del modelo de madurez de la gestión integral del riesgo (Capítulo 10 de este manual) se evaluará tomando como insumo el comportamiento de las materializaciones durante la vigencia, su tratamiento oportuno y la efectividad de las acciones correctivas adoptadas.

10. MADUREZ DE LA GESTIÓN INTEGRAL DEL RIESGO

La Alcaldía de Pasto entiende la Gestión Integral del Riesgo como una capacidad dinámica que debe evolucionar hacia la excelencia. El Nivel de Madurez es la medida en que la cultura de riesgo está imbuida en la toma de decisiones, la operación diaria y la generación de valor público. Esta evaluación se realizará anualmente en el último bimestre de cada vigencia bajo los parámetros del Modelo Integrado de Planeación y Gestión (MIPG).

La Entidad realizará el seguimiento permanente a la administración de los riesgos identificados, con el fin de verificar la eficacia de los controles definidos, la pertinencia de las acciones de tratamiento y la evolución del nivel de riesgo, en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG versión 7.

Como resultado del seguimiento, se podrán:

- Ajustar los riesgos identificados.
- Modificar los controles existentes.
- Definir nuevas acciones de tratamiento.
- Actualizar los mapas de riesgos por proceso.

La administración del riesgo se desarrollará bajo el enfoque de mejora continua, aplicando el ciclo PHVA (Planear, Hacer, Verificar y Actuar), garantizando la actualización permanente del manual y su articulación con la planeación institucional.

10.1. DIMENSIONES DE EVALUACIÓN

Para determinar el nivel de madurez, la entidad analizará cinco (5) dimensiones clave de acuerdo con la Guía V7:

- **Liderazgo y Compromiso:** Grado de involucramiento de la Alta Dirección en la revisión de riesgos críticos y asignación de recursos.
- **Integración Estratégica:** Nivel de alineación entre los riesgos identificados y el cumplimiento de las metas del Plan de Desarrollo Municipal.
- **Cultura y Apropiación:** Capacidad de los servidores públicos para identificar riesgos de manera autónoma en sus tareas diarias.
- **Análisis de Datos (KRI):** Uso efectivo de indicadores de riesgo para la toma de decisiones preventivas.
- **Resiliencia y Mejora:** Capacidad de la entidad para aprender de los riesgos materializados y fortalecer sus controles.

10.2. NIVELES DE MADUREZ

La Alcaldía de Pasto clasificará su gestión en los siguientes estados:

Nivel de Madurez	Descripción Técnica (Referencia Guía V7)
Inicial	Gestión del riesgo fragmentada, reactiva y cumpliendo solo requisitos mínimos legales.
Básico	Existe una metodología definida y aplicada, pero el riesgo aún no influye en la planeación estratégica.
Gestionado	Los riesgos se monitorean con indicadores (KRI) y existe una cultura de reporte en las dependencias.
Integrado	La gestión del riesgo es parte esencial de la toma de decisiones y la planeación presupuestal.
Optimizado	El riesgo es una ventaja estratégica; la entidad se anticipa a los cambios del entorno de manera proactiva.

10.3. ACCIONES PARA EL FORTALECIMIENTO

Los resultados de la medición de madurez (obtenidos a través del autodiagnóstico institucional o evaluaciones de Control Interno) darán lugar a:

- Planes de Capacitación Dirigidos: Refuerzo en las áreas con menor apropiación.
- Automatización de Controles: Migración de controles manuales a tecnológicos para aumentar la eficiencia.
- Ajuste del Apetito al Riesgo: Revisión anual de qué niveles de riesgo está dispuesta a aceptar la entidad para innovar en sus servicios.

11. CONTROL DE CAMBIOS

No. REVISIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA DE APROBACIÓN	VERSIÓN ACTUALIZADA
1	Se mantiene estructura conceptual, con precisiones en los siguientes aspectos: 1. Ajustes en definición de riesgos y otros conceptos relacionados con la gestión del riesgo. 2. Se articula la institucionalidad de MIPG con la gestión del riesgo 3. En paso 1 identificación del riesgo estructura propuesta para la redacción del riesgo. 4. En paso 2 valoración del riesgo: se precisa análisis de probabilidad e impacto y sus tablas de referencia, así como el mapa de calor resultante. 5. Para el diseño y evaluación de los controles se ajusta tabla de calificación. 6. Se amplía el alcance de la seguridad digital a la seguridad de la información.	10- ago-21	03
2	Se actualiza el Manual con base a la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 emitida por el DAFP, en los siguientes aspectos: 1. Se mantiene la estructura conceptual para la administración del riesgo. 2. Se incluyen lineamientos para los riesgos fiscales, de contratación y seguridad de la información. 3. Se adicionan responsabilidades frente a la gestión del riesgo de todas las líneas de defensa. 4. Se establece el apetito del riesgo por tipo de riesgo para la entidad. 5. Se fortalecen las acciones frente a la materialización de riesgos. 6. Se establece la frecuencia de seguimiento a riesgos.	5- oct-2023	04
3	Frente a los cambios en los roles de la gestión de los riesgos, se realizaron los siguientes cambios: La segunda línea de defensa se encargará de Apoyar al monitoreo de los controles establecidos por la primera línea de defensa de los temas a su cargo y supervisar la eficacia e implementación de las prácticas de gestión del riesgo, acorde con la información suministrada por los líderes de proceso. Promover ejercicios de autoevaluación para identificar riesgos no detectados. Al identificar dichos riesgos deberán informar de inmediato para proceder con la actualización correspondiente del mapa de riesgos.	30- ago-2024	05

	Frente al Cambio en Tratamiento frente a la materialización del riesgo: Se incluyeron las actividades de la segunda línea de defensa así: ● Revisar la información reportada en el formato de reporte de riesgos materializados, código: F-PE-28. ● Informar a la oficina de Control Interno y convocar a mesa de trabajo con los involucrados. ● En el marco de la mesa de trabajo, brindar los lineamientos para la formulación del plan de mejoramiento del riesgo materializado y la actualización del mapa de riesgos. ● Realizar seguimiento al plan de mejoramiento. Frente a los cambios en Frecuencia de seguimiento por tipo de riesgos, se tuvieron en cuenta: Riesgos de Gestión, Contratación, Seguridad de la Información, Fiscales y de Corrupción, en cuento a la zona de riesgo residual de BAJO Y MODERADO la periodicidad del cambio a Cuatrimestral y frente a la zona de riesgo residual ALTO Y EXTREMO la frecuencia BIMENSUAL Es de aclarar que los lideres de procesos realizarán sesiones con su equipo de trabajo de manera mensual para el seguimiento interno de sus riesgos Se incluye la aprobación de los anexos del manual frente a las directrices emitidas por la Función Pública frente a la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6		
6	1. Se actualiza el manual para alinearlo con la Guía de Gestión Integral del Riesgo – Versión 7 (2025) del Departamento Administrativo de la Función Pública, incorporando el enfoque de gestión integral del riesgo y ajustando el lenguaje institucional. 2. Se fortalece la Introducción, objetivo y alcance, incorporando el enfoque preventivo, estratégico y transversal de la gestión del riesgo, articulado con el Plan de Desarrollo Municipal, MIPG y MECI. 3. Se actualiza el marco legal, incorporando el Decreto 1122 de 2024, el Programa de Transparencia y Ética Pública (PTEP), el SIGRIP y la referencia al marco COSO ERM como complemento técnico.	1/09/2026	06

	4. Se reformula la Política de Administración del Riesgo, adoptando la denominación Política de Gestión Integral del Riesgo, fortaleciendo el rol de la Alta Dirección, el "tono desde la cima" y la relación riesgo–estrategia–desempeño. 5. Se incorpora el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, redefiniendo los riesgos de corrupción como amenazas a la integridad, y articulándolos con el PTEP, conforme a la normativa vigente. 6. Se actualizan los criterios de apetito y tolerancia al riesgo, estableciendo niveles diferenciados por tipo de riesgo, incluyendo la política de cero tolerancias frente a riesgos de integridad y corrupción. 7. Se incorporan los Indicadores Clave de Riesgo – KRI como herramienta de monitoreo y alerta temprana, articulados con la metodología de seguimiento y la toma de decisiones institucionales. 8. Se ajusta y detalla la metodología de gestión del riesgo, fortaleciendo la identificación, análisis, valoración, tratamiento, seguimiento y actualización de riesgos, conforme a la Guía v7. 9. Se incorpora el concepto de evaluación de la madurez de la Gestión Integral del Riesgo, orientado a la mejora continua y al fortalecimiento progresivo del sistema institucional de gestión del riesgo.		