ANEXO METODOLÓGICO PARA LA GESTIÓN INTEGRAL DEL RIESGO DE DISTRISEGURIDAD

DS
DISTRISEGURIDAD

2026

Instrumento operativo de aplicación de la Política de Gestión Integral del Riesgo

Código	*ANEDEYP-001*
Versión	*1.0*
Fecha	*Marzo de 2026*
Dependencia líder	*Direccionamiento Estratégico y Planeación*
Aprobación	*Comité de Control Interno Institucional*

Documento metodológico para orientar la identificación, análisis, valoración, control, tratamiento, monitoreo y actualización de riesgos de gestión, fiscales, de seguridad de la información e integridad pública en todos los procesos de la entidad.

CONTENIDO

1. Objeto

El presente anexo metodológico establece los criterios, pasos, herramientas, escalas y lineamientos técnicos para la identificación, análisis, valoración, tratamiento, monitoreo, seguimiento y actualización de los riesgos en Distriseguridad, en desarrollo de la Política de Gestión Integral del Riesgo adoptada por la entidad.

Este documento constituye el instrumento operativo de aplicación institucional y debe ser usado por los procesos para construir, actualizar y monitorear sus mapas de riesgos, así como para consolidar el mapa integral de riesgos de la entidad.

2. Alcance

El anexo metodológico aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación de Distriseguridad; a sus planes, programas, proyectos, actividades, recursos, activos de información, actuaciones administrativas y relaciones con terceros.

- Servidores públicos, directivos, contratistas, supervisores y equipos de apoyo.
- Procesos, procedimientos, planes, programas y proyectos.
- Riesgos asociados a terceros, convenios, operadores, proveedores y contratistas.
- Activos de información, recursos físicos, financieros, tecnológicos y documentales.
- Hechos internos o externos que puedan afectar el cumplimiento de objetivos y la generación de valor público.

3. Marco normativo y técnico

La aplicación del presente anexo deberá estar alineado con los siguientes referentes:

- Constitución Política de Colombia, principios de la función administrativa y del control fiscal.
- Decreto 1499 de 2017, en lo relacionado con MIPG y MECI.
- Decreto 1083 de 2015 y normas reglamentarias aplicables.
- Ley 1474 de 2011, Ley 2195 de 2022 y demás normas asociadas a integridad, transparencia y lucha contra la corrupción.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 de 2025, expedida por el DAFP.
- Lineamientos institucionales de seguridad de la información, archivo, contratación, servicio al ciudadano y control interno.

4. Relación con la política de gestión integral del riesgo

La Política de Gestión Integral del Riesgo define el marco rector, los principios, responsabilidades, lineamientos generales, apetito del riesgo y criterios institucionales de gestión. El presente anexo desarrolla operativamente esa política y traduce sus lineamientos a criterios metodológicos uniformes, aplicables y verificables.

La política y el anexo se complementan, pero no se duplican. La política responde al qué y al para qué; este anexo responde al cómo se realizará.

5. Tipologías de riesgo aplicables

Para efectos metodológicos, Distriseguridad gestionará como mínimo las siguientes tipologías de riesgo:

Tipología	Descripción de aplicación en Distriseguridad
Riesgos de gestión	Eventos que pueden afectar el cumplimiento de objetivos estratégicos, de proceso, de planes, programas o proyectos.

Tipología	Descripción de aplicación en Distriseguridad
Riesgos fiscales	Eventos que pueden ocasionar pérdida, detrimento, uso ineficiente o afectación del patrimonio público.
Riesgos de seguridad de la información	Eventos que afectan la confidencialidad, integridad, disponibilidad o trazabilidad de la información y de los activos asociados.
Riesgos para la integridad pública	Eventos asociados a conductas, decisiones o situaciones que comprometen la ética pública, la transparencia, la legalidad o el interés general.
Otros riesgos institucionales aplicables	Riesgos contractuales, operativos, reputacionales, jurídicos, de continuidad, tecnológicos o de terceros, cuando deban gestionarse de manera específica.

6. Responsables de la aplicación metodológica

La aplicación del presente anexo se desarrollará bajo el esquema de líneas de defensa. La segunda línea de defensa estará liderada por la dependencia Planeación, como responsable principal de la orientación metodológica, articulación institucional, consolidación del mapa integral de riesgos y monitoreo de la aplicación del presente anexo, con apoyo de las demás dependencias que cumplan funciones de soporte en procesos de manera transversal.

Nivel	Responsabilidades metodológicas principales
Línea estratégica	Aprueba lineamientos generales, revisa apetito y tolerancia del riesgo, analiza reportes institucionales y orienta decisiones sobre riesgos críticos.
Primera línea de defensa	Identifica, analiza, valora, controla, trata y monitorea los riesgos en el ámbito de sus procesos, proyectos y actividades.
Segunda línea de defensa	Liderada por la dependencia de Planeación; orienta metodológicamente, acompaña a los procesos, consolida el mapa institucional, monitorea la aplicación de la metodología y articula las tipologías de riesgo con apoyo de las áreas técnicas especializadas.
Tercera línea de defensa	Evalúa de manera independiente la efectividad del sistema de control interno y de la gestión integral del riesgo.

7. Criterios previos para la gestión del Riesgo

Antes de aplicar la metodología, cada proceso deberá considerar como mínimo los siguientes elementos:

- Objetivos institucionales, estratégicos y de proceso.
- Contexto interno y externo del proceso o actividad.
- Cambios normativos, tecnológicos, financieros o contractuales relevantes.
- Interacción con terceros y dependencia de proveedores u operadores.
- Activos de información, recursos públicos, bienes y servicios involucrados.
- Criticidad de las actividades y consecuencias potenciales de su afectación.
- Apetito, tolerancia y criterios de aceptación del riesgo definidos por la entidad.

Para la identificación de riesgos, los líderes de proceso deben asegurar que los objetivos de sus procesos y proyectos estén redactados bajo la metodología SMART, garantizando que sean: S (Específicos), M (Medibles), A (Alcanzables), R (Realistas) y T (En un tiempo determinado). Un objetivo mal formulado impide la identificación precisa de los eventos que pueden obstaculizar su cumplimiento

8. Metodología general para la gestión integral del Riesgo

La metodología institucional se desarrollará en cuatro pasos:

a) identificación y descripción del riesgo.
b) análisis del riesgo inherente;
c) diseño y análisis de controles; y
d) valoración del riesgo residual.

8.1. Paso 1. Identificación y descripción del riesgo

La identificación del riesgo consiste en reconocer y describir los eventos potenciales que puedan afectar el cumplimiento de los objetivos del proceso, plan, programa, proyecto o actividad.

- Objetivo afectado.
- Causas o circunstancias que originan el riesgo.
- Evento de riesgo o situación no deseada.
- Consecuencias o efectos potenciales.
- Tipología del riesgo.
- Proceso, dependencia y responsable.
- Controles existentes y relación con activos, recursos o terceros.

8.1.1. Regla institucional para la redacción del riesgo

La descripción del riesgo deberá formularse en lenguaje claro y verificable, preferiblemente bajo la siguiente estructura:

Redacción no recomendada	Redacción recomendada
Pérdida de documentos.	Posibilidad de pérdida o extravío de expedientes contractuales que afecte la trazabilidad y oportunidad de la supervisión, por debilidades en el control documental.
Fallas en el sistema.	Posibilidad de indisponibilidad de la plataforma de monitoreo que afecte la continuidad operativa y la capacidad de respuesta, por fallas de infraestructura tecnológica o soporte insuficiente.

8.1.2. Fuentes para la identificación del riesgo

- Caracterizaciones y mapas de procesos.
- Resultados de auditorías, seguimientos y planes de mejoramiento.

- Quejas, reclamos, PQRSD y reportes de usuarios.
- Incidentes de seguridad de la información.
- Hallazgos de entes de control y lecciones aprendidas.
- Seguimiento a contratos, proyectos, bienes, inventarios y obligaciones legales.
- Análisis de contexto, DOFA, PESTEL y eventos materializados.

8.2. Paso 2. Análisis del riesgo inherente

El análisis del riesgo inherente corresponde a la valoración inicial del riesgo antes de considerar la efectividad de los controles existentes. Para ello se determina la probabilidad y el impacto, y con su cruce se establece la zona de riesgo inicial.

8.2.1. Escala institucional de probabilidad

La probabilidad corresponde a la posibilidad de ocurrencia de un evento de riesgo que pueda afectar el cumplimiento de los objetivos institucionales, de proceso, de planes, programas o proyectos. Para Distriseguridad, la probabilidad se determinará principalmente con base en la frecuencia anual con la que se ejecuta la actividad que conlleva el riesgo, en armonía con la Guía para la Gestión Integral del Riesgo del DAFP, la cual establece criterios parametrizados por número de veces al año.

Nivel de probabilidad	Frecuencia de la actividad	Valor porcentual
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año	60%

Alta	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y hasta 5000 veces por año	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

8.2.1.1. Criterios de aplicación

Para la correcta valoración de la probabilidad, se deberán observar los siguientes criterios:

a. La referencia es la actividad, no el evento consumado.

La frecuencia debe establecerse con base en el número de veces que se ejecuta la actividad que expone al riesgo, no únicamente en el número de veces que históricamente se ha materializado el evento.

b. El análisis se hace sobre un periodo anual.

La frecuencia deberá estimarse en un horizonte de un año, con base en información histórica, comportamiento del proceso, volumen de operación, criterio técnico del responsable y evidencias disponibles.

c. La valoración debe estar asociada al proceso o actividad específica.

No todas las actividades tienen la misma exposición. Por ello, cada riesgo debe valorarse conforme a la dinámica real del proceso donde se presenta.

d. Se debe privilegiar el uso de información verificable.

Cuando existan registros, estadísticas, bitácoras, reportes del sistema, históricos de operación o datos documentados, estos deberán utilizarse como base principal para la estimación de la frecuencia.

e. En ausencia de datos suficientes, podrá utilizarse criterio técnico sustentado.

Cuando no se cuente con series históricas o registros completos, el líder del proceso podrá estimar la frecuencia con apoyo de su equipo y de la segunda línea de defensa, dejando documentada la justificación del criterio adoptado. La política vigente ya reconocía que la probabilidad podía medirse por criterios de frecuencia o factibilidad, y que en algunos casos aplicaba el criterio experto.

f. Regla especial para actividades de alta recurrencia o componente tecnológico

En procesos con alta recurrencia operativa o componente tecnológico, la frecuencia deberá adaptarse a la naturaleza real de la actividad. La Guía 2025 pone como ejemplo que, en materia de tecnología, una hora de funcionamiento puede considerarse como una unidad de frecuencia para efectos del análisis.

8.2.2. Escala institucional de impacto

El impacto corresponde a las consecuencias que podría generar la materialización del riesgo sobre la entidad, los recursos públicos, los activos de información, la legalidad, la continuidad operativa, la reputación y la ciudadanía.

Nivel	Valor	Criterio orientador de afectación
Leve	20%	Afectación menor, controlable y de bajo efecto sobre el proceso o servicio.
Menor	40%	Afectación acotada con reproceso moderado o impacto institucional interno.

Moderado	60%	Afectación relevante sobre objetivos, tiempos, recursos o usuarios clave.
Mayor	80%	Afectación alta sobre el cumplimiento misional, recursos, información o reputación.
Catastrófico	100%	Afectación crítica con potencial de suspensión, pérdida grave, sanción o daño severo al interés público.

8.2.3. Matriz de calor y niveles de severidad del riesgo inherente

La severidad del riesgo inherente se obtendrá del cruce entre probabilidad e impacto, conforme a la siguiente lectura institucional:

Impacto / Probabilidad	20%	40%	60%	80%	100%
20%	Baja	Baja	Moderada	Moderada	Alta
40%	Baja	Moderada	Moderada	Alta	Alta
60%	Moderada	Moderada	Alta	Alta	Extrema
80%	Moderada	Alta	Alta	Extrema	Extrema
100%	Alta	Alta	Extrema	Extrema	Extrema

La matriz podrá ajustarse en su representación gráfica institucional, siempre que se mantenga la lógica de clasificación y la trazabilidad del análisis realizado.

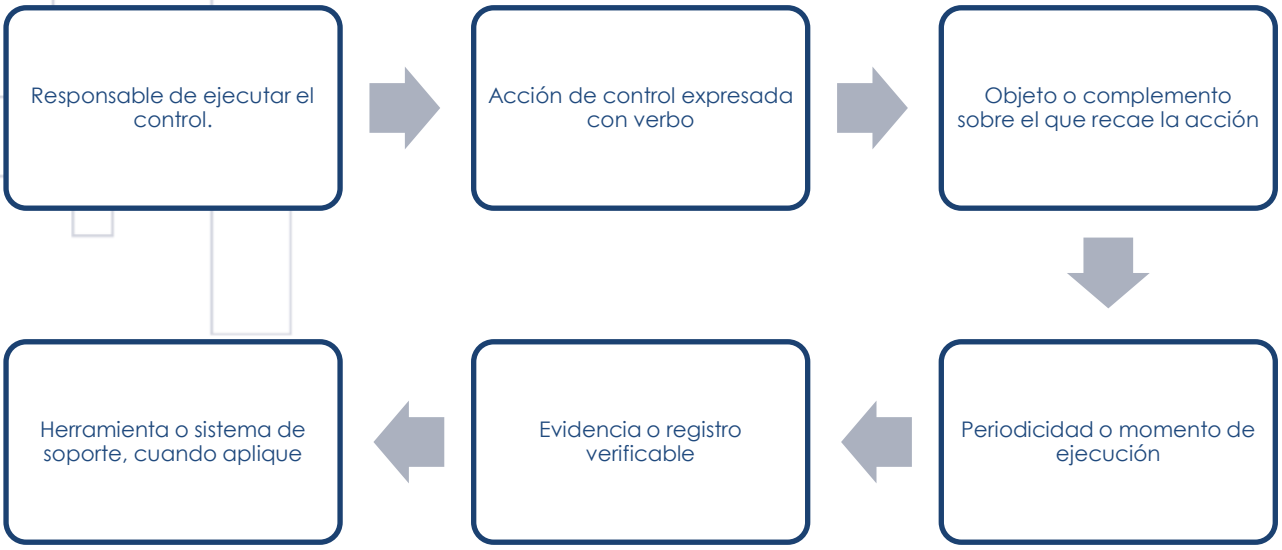
8.3. Paso 3. Diseño y análisis de controles

Una vez analizado el riesgo inherente, se deberán identificar los controles existentes o propuestos para prevenir, detectar o corregir la materialización del riesgo.

8.3.1. Estructura mínima de redacción del control

Todo control deberá redactarse de manera clara, verificable y orientada a su aplicación real. Como regla institucional, la descripción mínima del control deberá

identificar quién lo ejecuta, qué hace, sobre qué elemento actúa, con qué frecuencia y qué evidencia deja.



Componente	Descripción mínima esperada
Responsable	Cargo, rol, dependencia o sistema que ejecuta el control.
Acción	Verbo que describe la actividad de control: verifica, valida, concilia, revisa, autoriza, bloquea, registra, entre otros.
Complemento	Objeto, condición o criterio sobre el cual se aplica el control.
Frecuencia/Periodicidad	Momento o periodicidad con la que se ejecuta el control: diaria, semanal, mensual, por evento, antes de autorizar, entre otras.
Herramienta o Sistema de soporte (Evidencia)	Registro, trazabilidad o soporte que permite verificar la ejecución del control.

Ejemplo de redacción recomendada: *"El profesional responsable de supervisión verifica mensualmente la conciliación de entregables contractuales frente a los informes del contratista y deja acta o registro de validación en el expediente correspondiente".*

8.3.2. Tipos de control

Tipo	Finalidad	Peso orientador
Preventivo	Actúa antes del evento y reduce principalmente la probabilidad de ocurrencia.	25%
Detectivo	Permite advertir desviaciones durante la ejecución y reduce o contiene la exposición mediante alertas o validaciones.	15%
Correctivo	Actúa después del evento para reducir consecuencias, corregir desviaciones o restablecer condiciones de control.	10%

Los pesos orientadores deberán aplicarse conforme a la Guía 2025 del DAFP y podrán ser usados por la entidad para calcular el efecto acumulado de los controles sobre la probabilidad o el impacto, según corresponda. Cuando un control sea atípico o tenga mayor complejidad, la segunda línea podrá justificar técnicamente un tratamiento diferenciado, dejando trazabilidad de la decisión.

8.3.2.1. Forma de implementación del control

Además del tipo de control, la entidad deberá identificar la forma de implementación del control, en tanto este factor incide en su confiabilidad y consistencia operativa.

Forma de implementación	Descripción	Peso orientador
Automático	El control se ejecuta por una herramienta, sistema o parametrización tecnológica sin intervención manual directa en cada evento.	25%
Manual	El control depende de la ejecución humana directa, revisión documental o validación operativa realizada por un responsable.	15%

8.3.3. Criterios de calidad del control

Criterio	Pregunta de verificación
Formalización	¿El control está documentado o definido de manera clara?
Responsable	¿Tiene responsable de ejecución identificado?
Periodicidad	¿Se conoce con qué frecuencia se ejecuta?
Evidencia	¿Deja registro o soporte verificable?
Pertinencia	¿Está directamente relacionado con el riesgo y su causa?

Criterio	Pregunta de verificación
Efectividad	¿Reduce la probabilidad o el impacto de forma demostrable?

Un control débil o inexistente no debe ser considerado para disminuir el riesgo residual. Cuando un control exista, pero no tenga evidencia o no esté funcionando de forma consistente, deberá registrarse como oportunidad de mejora.

8.4. Paso 4. Valoración del riesgo residual

El riesgo residual corresponde al nivel de riesgo que permanece luego de considerar el diseño y funcionamiento de los controles existentes. Para su cálculo, los controles se aplican de manera acumulativa sobre la probabilidad o el impacto.

Ejemplo orientador de aplicación de controles sobre la probabilidad:

Dato	Valor
Probabilidad inherente	60%
Control preventivo aplicado	40%
Resultado después del primer control	36%
Control detectivo aplicado	30%
Resultado después del segundo control	25,2%

La misma lógica podrá aplicarse al impacto cuando existan controles correctivos u otros mecanismos que reduzcan las consecuencias del evento. El riesgo residual deberá ubicarse nuevamente en la matriz de calor para determinar su zona final.

9. Niveles de aceptación del riesgo y tratamiento

La aceptación del riesgo se definirá con base en el nivel residual y en el apetito del riesgo aprobado por la entidad. Como criterio institucional general, Distriseguridad adoptará la siguiente regla de tratamiento:

Zona de riesgo residual	Nivel de aceptación	Tratamiento principal	Frecuencia mínima de seguimiento
Baja	Aceptable	Aceptar y administrar con controles propios del proceso.	Semestral
Moderada	Aceptable con control	Reducir mediante acciones preventivas y mantener seguimiento.	Trimestral
Alta	No deseable	Reducir, evitar o compartir; requiere plan de tratamiento formal.	Trimestral / bimestral
Extrema	No aceptable	Evitar, reducir de manera inmediata o escalar a la alta dirección.	Mensual

Integridad pública o fiscal grave	No aceptable	No podrá aceptarse; exige tratamiento prioritario y escalamiento.	Mensual o inmediato

9.1. Opciones de tratamiento

- **Aceptar el riesgo:** no se adoptan medidas adicionales porque el riesgo residual se encuentra dentro del nivel aceptable definido por la entidad.
- **Reducir el riesgo:** se implementan controles o acciones para disminuir probabilidad, impacto o ambos.
- **Evitar el riesgo:** se suprime la actividad o se modifica sustancialmente para impedir la exposición.
- **Compartir el riesgo:** se distribuye parte del riesgo con terceros, sin transferir la responsabilidad institucional cuando esta siga recayendo en la entidad.
- **Escalar el riesgo:** se eleva a la alta dirección o instancia competente cuando supera el apetito del riesgo o implica decisiones institucionales.

Los riesgos para la integridad pública y aquellos que puedan generar afectación grave al patrimonio público, a la legalidad o a la seguridad de la información no deberán ser tratados como aceptables cuando su nivel residual se mantenga alto o extremo.

10. Monitoreo, seguimiento y actualización

Los riesgos, controles y planes de tratamiento deberán ser objeto de monitoreo periódico por parte de la primera y segunda línea de defensa, y de evaluación independiente por parte de la tercera línea.

Actividad	Responsable principal	Periodicidad orientadora
Seguimiento al control y al plan de tratamiento	Primera línea de defensa	Según la zona de riesgo definida
Consolidación y monitoreo institucional	Segunda línea de defensa	Trimestral
Reporte a comités o alta dirección	Segunda línea / línea estratégica	Trimestral o cuando el riesgo lo amerite
Evaluación independiente	Tercera línea de defensa	Según Plan Anual de Auditoría
Actualización extraordinaria	Proceso responsable con apoyo de la segunda línea	Cuando haya cambios relevantes o materialización del riesgo

- El mapa de riesgos deberá actualizarse cuando cambie el contexto, se modifiquen objetivos, procesos, responsables o controles, o se materialice un riesgo relevante.
- Todo seguimiento deberá dejar evidencia verificable.
- Los riesgos críticos deberán ser escalados oportunamente.
- Las modificaciones significativas deberán quedar registradas en el control de cambios del instrumento o en actas de seguimiento.

11. Materialización del riesgo

Cuando un riesgo se materialice, el responsable del proceso deberá adelantar como mínimo las siguientes acciones:

Paso	Acción requerida
1	Registrar el evento y la fecha de ocurrencia.
2	Describir causas, consecuencias y afectaciones reales.
3	Informar a la instancia correspondiente según la criticidad.
4	Revisar la efectividad de los controles existentes.
5	Definir acciones inmediatas de respuesta y contención.
6	Actualizar la valoración del riesgo y el mapa si aplica.
7	Documentar lecciones aprendidas y acciones de mejora.

12. Indicadores clave de riesgo

Los indicadores clave de riesgo son señales cuantitativas o cualitativas que permiten advertir oportunamente cambios en el comportamiento de un riesgo, en la efectividad de los controles o en la exposición de la entidad.

- Porcentaje de riesgos críticos con seguimiento oportuno.
- Número de riesgos materializados por proceso.
- Porcentaje de acciones de tratamiento vencidas.
- Incidentes de seguridad de la información reportados y cerrados.
- Hallazgos repetitivos asociados a control interno, contratación o gestión documental.
- Tiempo promedio de respuesta frente a riesgos materializados.

- Porcentaje de riesgos con control documentado y con evidencia vigente.

Estructura de Umbrales para Indicadores (KRI): Cada Indicador Clave de Riesgo (KRI) debe contar con umbrales de alerta aprobados por el Comité de Coordinación de Control Interno, representados visualmente mediante un sistema de semaforización que permita distinguir entre valores aceptables y críticos:

- Verde (Bajo): Riesgo bajo control, el valor se mantiene dentro del apetito al riesgo. No requiere acciones adicionales.

- Amarillo (Moderado): Alerta temprana; el riesgo se acerca al umbral de tolerancia. Requiere monitoreo reforzado o revisión de la efectividad de los controles existentes.

- Rojo (Alto): Valor crítico o inaceptable que supera la tolerancia definida. Requiere intervención inmediata de la alta dirección y la activación de planes de contingencia o nuevas acciones de mitigación."

13. Registros e instrumentos

Para la aplicación de este anexo, Distriseguridad deberá mantener como mínimo los siguientes instrumentos:

- Matriz o mapa de riesgos por proceso.
- Mapa institucional integral de riesgos.
- Registro de controles.
- Plan de tratamiento del riesgo.
- Registro de materialización del riesgo.
- Formato o reporte de seguimiento.
- Inventario de activos de información, cuando aplique.
- Soportes de revisión por la segunda línea y reportes a la línea estratégica.

14. Lineamientos específicos por tipología de riesgo

14.1. Riesgos de gestión

Se identificarán respecto de objetivos de proceso, planes, programas, proyectos y actividades. Su análisis deberá considerar causas, controles, impacto operativo y afectación al logro institucional.

14.2. Riesgos fiscales

Deberán identificarse especialmente en actividades relacionadas con administración de recursos públicos, inventarios, contratación, supervisión, pagos, bienes, convenios, recaudos y demás eventos que puedan generar pérdida, detrimento o uso ineficiente del patrimonio público.

- Precisar el recurso, bien o interés fiscal potencialmente afectado.
- Describir la conducta, omisión o circunstancia que podría generar afectación patrimonial.
- Valorar impacto con atención reforzada a la magnitud del posible detrimento.
- Escalar de manera prioritaria los riesgos altos o extremos.

14.3. Riesgos de seguridad de la información

Se gestionarán considerando los activos de información y sus atributos de confidencialidad, integridad, disponibilidad y trazabilidad. Su identificación deberá apoyarse, cuando aplique, en el inventario de activos, amenazas, vulnerabilidades e incidentes reportados.

La identificación de riesgos de seguridad digital partirá obligatoriamente de un inventario clasificado bajo los siguientes 6 pasos establecidos por el Ministerio de TIC y el DAFP:

1. Listado de activos por proceso: Identificar todos los activos dentro del alcance del proceso analizado.
2. Identificación de dueño y custodio: Definir el área responsable (propietario) y quién vela por la protección física o técnica (custodio) del activo.

3. Clasificación por tipo: Categorizar el activo como Información, Software, Hardware, Servicios, Recursos Humanos, entre otros.
4. Clasificación de la información: Evaluar el activo frente a los niveles de Confidencialidad, Integridad y Disponibilidad (Pública, Clasificada o Reservada).
5. Determinación de la criticidad: Asignar el nivel de valor institucional (Alto, Medio, Bajo) según la sumatoria de sus propiedades de seguridad.
6. Identificación de infraestructura crítica cibernética: Determinar si el activo forma parte de la infraestructura esencial del Estado.
7. Identificar el activo o grupo de activos comprometidos.
8. Precisar si el evento afecta disponibilidad, integridad, confidencialidad o trazabilidad.
9. Relacionar amenazas, vulnerabilidades y controles técnicos u organizacionales existentes.
10. Coordinar la valoración con el responsable de seguridad de la información o TIC cuando corresponda.

14.4. Riesgos para la integridad pública

Para la gestión de riesgos de integridad (corrupción, soborno, fraude), Distriseguridad integra los tres pilares operativos del SIGRIP:

Debida Diligencia: Procedimientos para conocer a fondo a las contrapartes (proveedores, contratistas, aliados) antes y durante la relación institucional.

Función de Cumplimiento: Designación formal de un responsable o grupo encargado de velar por la integridad, reportar operaciones sospechosas y capacitar al personal.

Herramientas de Gestión: Adopción de políticas específicas (Antisoborno, Antifraude y ALA/CFT/CFP) y un canal de denuncias con protección al denunciante.

Los riesgos para la integridad pública deberán identificarse y analizarse considerando no solo eventos de corrupción consumada, sino también condiciones de opacidad, discrecionalidad, conflicto de interés, concentración de funciones, debilidad de controles, asimetrías de información o prácticas que puedan comprometer la legalidad, la transparencia y la confianza institucional.

Su análisis deberá articularse con el marco de integridad pública, el código de integridad, la gestión contractual, la administración de bienes y recursos, la atención a grupos de valor y las decisiones que impliquen interacción con terceros o ejercicio de discrecionalidad administrativa.

- Priorizar causas relacionadas con comportamiento, controles débiles o ausencia de segregación de funciones.
- No aceptar como tratamiento final los riesgos residuales altos o extremos.
- Activar, cuando corresponda, rutas institucionales asociadas a integridad, disciplinario o control interno.

15. Glosario básico

Término	Definición operativa
Riesgo	Posibilidad de ocurrencia de un evento que afecte el cumplimiento de objetivos, el uso de recursos públicos, la integridad o la información.
Riesgo inherente	Nivel de riesgo antes de aplicar la efectividad de los controles existentes.
Control	Medida o acción orientada a prevenir, detectar o corregir la materialización del riesgo.
Riesgo residual	Nivel de riesgo que permanece después de aplicar la valoración de los controles.
Apetito del riesgo	Nivel de riesgo que la entidad está dispuesta a asumir para cumplir sus objetivos, dentro del marco legal y de sus capacidades.

Término	Definición operativa
KRI	Indicador clave de riesgo utilizado para monitorear cambios en la exposición o en el comportamiento de un riesgo.

16. Disposiciones de actualización del anexo

El presente anexo metodológico deberá revisarse y actualizarse cuando se presenten cambios relevantes en la normatividad, en los lineamientos nacionales aplicables, en la estructura institucional, en el modelo de operación por procesos, en el apetito del riesgo o en el contexto de la entidad.

Las actualizaciones serán lideradas por la dependencia responsable de planeación o quien haga sus veces, con participación de los procesos y validación de las instancias institucionales competentes.

Toda modificación deberá registrarse en el control de cambios del documento para asegurar el control y trazabilidad del documento.

16.1. Control de cambios

Toda actualización del presente anexo deberá registrarse en el siguiente control de cambios para asegurar trazabilidad documental y metodológica.

Versión	Fecha	Descripción del cambio	Elaboró	Revisó	Aprobó

Apéndice A. Estructura mínima para la matriz de riesgos

La matriz institucional de riesgos podrá administrarse en Excel o en una herramienta especializada, siempre que conserve como mínimo los siguientes campos:

Campo mínimo	Descripción
Proceso / dependencia	Proceso o área responsable del riesgo.
Objetivo asociado	Objetivo institucional, de proceso o de proyecto afectado.
Tipología	Tipo principal de riesgo.
Causas	Factores que originan o facilitan el evento.
Descripción del riesgo	Redacción institucional del evento de riesgo.
Consecuencias	Efectos potenciales o reales.
Probabilidad inherente	Valor antes de controles.
Impacto inherente	Valor antes de controles.
Zona inherente	Resultado del cruce en la matriz de calor.
Controles	Controles existentes y su valoración.
Probabilidad residual	Valor después de controles.
Impacto residual	Valor después de controles.

Campo mínimo	Descripción
Zona residual	Resultado final del riesgo.
Tratamiento	Acción definida para administrar el riesgo.
Responsable	Cargo o dependencia responsable.
Plazo	Fecha objetivo de ejecución o seguimiento.
Evidencia	Soporte verificable.
Frecuencia de seguimiento	Periodicidad mínima.
Estado	Vigente, en revisión, materializado, cerrado u otro.