ANEXO

Metodología para la Gestión Integral de Riesgos

Unidad de Información y Análisis Financiero - UIAF

Versión 1

Marzo 2026

	PREPARÓ	REVISÓ	APROBÓ
FIRMA:			
CÓDIGO:	397	406, 391, 408, 398, 395, 394, 293, 399, 341, 165, 302	390
CARGO:	Profesional Especializado OAP	Subdirector SAO, subdirector SAE, subdirector de SAN, subdirectora STI, subdirectora SAF, jefe OAJ, jefe OAI, jefe OAP, jefe OCII (E), Profesional Especializado OAP, Profesional Especializado OAP	Director General
FECHA:	27 de febrero 2026	20 de marzo de 2026	20 de marzo de 2026

Tabla de Contenido

Lista de Tablas

Lista de Ilustraciones

1. ESQUEMA METODOLÓGICO APLICABLE A LA GESTIÓN INTEGRAL DE RIESGOS

El Departamento Administrativo de la Función Pública (DAFP), en articulación con la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), emiten la metodología para la Gestión Integral del Riesgo. Esta herramienta ha sido actualizada para dar cumplimiento a la Ley 2195 de 2022 y al Decreto 1122 de 2024, incorporando lineamientos robustos para la identificación y tratamiento de riesgos a la integridad pública y la seguridad de la información.

Bajo este marco nacional, la Unidad de Información y Análisis Financiero (UIAF) adopta formalmente la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas (Versión 7, noviembre de 2025). Esta adopción se complementa con el Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG Versión 6) y los principios del modelo internacional COSO ERM 2017, con el fin de fortalecer la gobernanza y promover estándares de excelencia técnica en la gestión del riesgo.

1.1. Institucionalidad y Gobernanza en la UIAF

Para garantizar una gestión sistémica y preventiva, la UIAF articula su operación a través de las instancias de decisión reguladas por el Decreto 1499 de 2017, la Ley 87 de 1993 y el Decreto 648 de 2017:

- **Comité Institucional de Gestión y Desempeño:** encargado de la implementación y seguimiento de las políticas de desarrollo institucional, asegurando que la gestión del riesgo esté alineada con la plataforma estratégica de la Unidad.
- **Comité Institucional de Coordinación de Control Interno:** actúa como la instancia de articulación estratégica para la supervisión del sistema de control, evaluando la efectividad de los controles y el cumplimiento de los umbrales de riesgo definidos.

Para la UIAF, la administración del riesgo no es un proceso aislado, sino una capacidad institucional que se despliega de manera sistémica. Antes de iniciar con el ciclo metodológico,

es imperativo realizar el conocimiento de la Entidad, el cual establece el contexto estratégico y operativo necesario para una gestión precisa.

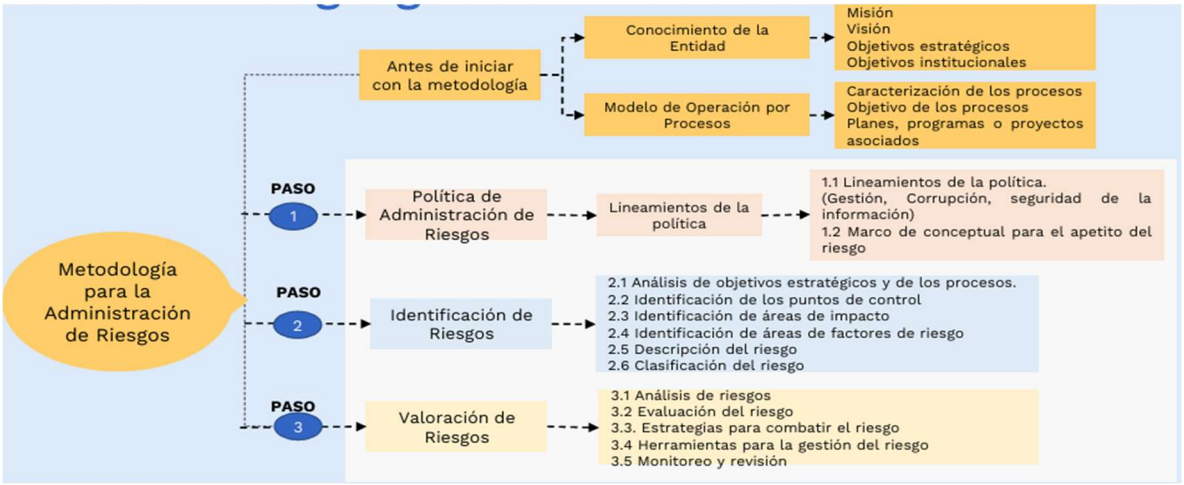
El presente desarrollo metodológico contiene las siguientes fases:

Fase Preliminar: conocimiento de la entidad
Consiste en analizar el contexto general para entender la complejidad y el entorno de la Unidad. Esta base determinará el éxito en la aplicación de la metodología.

- **Plataforma Estratégica:** consulta y alineación con la Misión, Visión, Objetivos Estratégicos e Institucionales.
- **Modelo de Operación por Procesos:** revisión de las caracterizaciones, objetivos de los procesos y los planes, programas o proyectos asociados.

Esquema metodológico: la metodología se desarrolla a través de tres pasos fundamentales que garantizan la trazabilidad desde la política hasta el monitoreo:

Ilustración 1.Esquema metodológico riesgos



Fuente: Manual metodología riesgos_v7 7

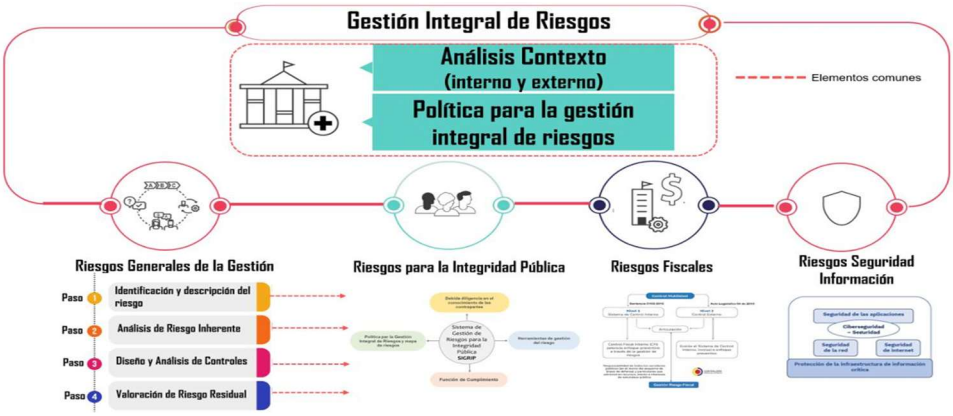
La metodología para la Administración del Riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de ésta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de

comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada, tal como se muestra a continuación:

Dada la naturaleza misional de la UIAF como unidad de inteligencia, la entidad opera bajo un modelo de cumplimiento estricto donde la tolerancia al riesgo es mínima o nula en procesos críticos (seguridad de la información y reserva legal). Por lo tanto, la gestión se centra en la mitigación total y el control riguroso, sustituyendo la definición de 'apetito' por el cumplimiento de estándares de seguridad nacional.
Considerando que el establecimiento del Contexto de la Entidad y el análisis del entorno estratégico ya se encuentran desarrollados en el documento base de este anexo, el presente apartado se constituye como la guía metodológica para la ejecución operativa. En consecuencia, partiendo de dicha base estratégica, se procede con la aplicación técnica del Paso 2: Identificación de Riesgos, fase donde se materializa el reconocimiento de las amenazas que podrían comprometer la misión de inteligencia financiera de la UIAF.

A continuación, se muestra la articulación estratégica con la gestión de riesgos:

Ilustración 2. Articulación contexto estratégico y gestión del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

A partir de la imagen anterior y para la identificación de los riesgos de la Entidad, primero debemos entender la tipología de riesgos para hacer toda la gestión respectiva.

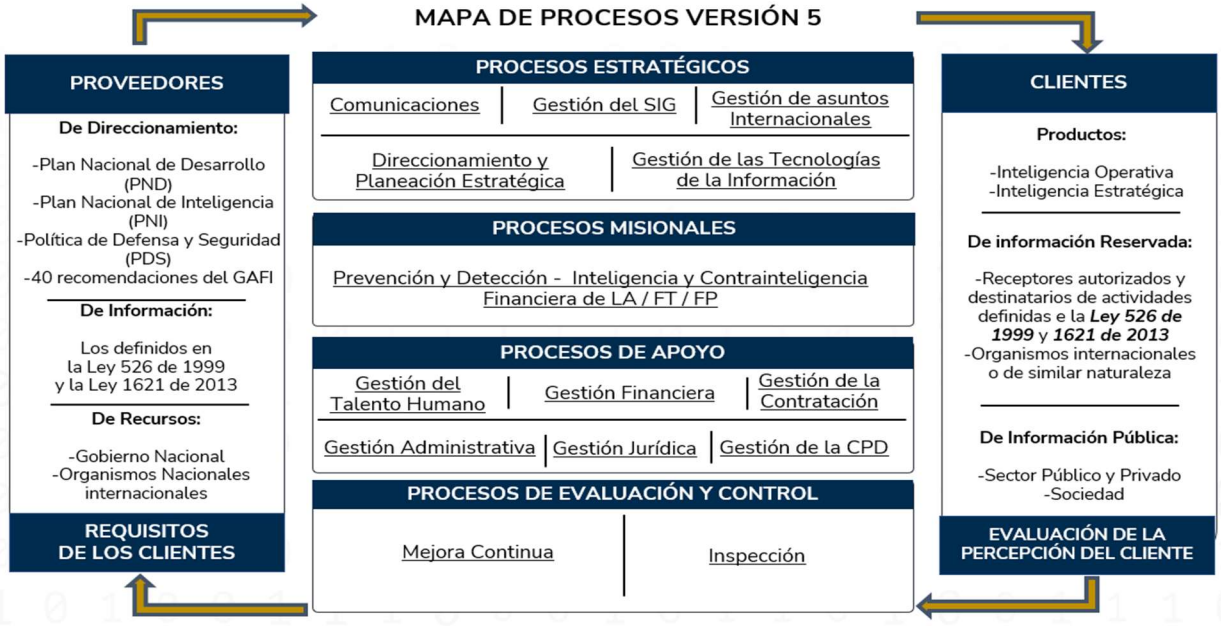
2. METODOLOGÍA

2.1. Tipologías de Riesgos

Para la identificación de los riesgos en cada uno de sus tipos, la UIAF se basa en la operación por procesos y se identifican por cada uno de los procesos vigentes a la fecha.

A continuación, se muestra el mapa de procesos vigente en la Entidad.

Imagen 3. Mapa de procesos v5



Fuente: OAP

De acuerdo con el mapa de procesos institucional, a continuación, se describen cada una de los tipos de riesgos que se deben identificar para la gestión integral de riesgos institucionales.

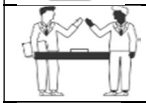
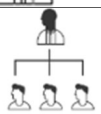
2.2. Riesgos de gestión

Son los riesgos asociados a la operación de cada uno de los procesos institucionales. Aquí se tiene en cuenta la cadena de valor institucional.

Para la identificación de los riesgos de gestión en cada proceso, se debe tener en cuenta los factores de riesgos y sus descriptores. Estos factores son: Ejecución administración de procesos, Transacción u Operación aplica para LA-FT-FP, Talento Humano, Tecnología, Infraestructura, Evento externo.

A continuación, se describen los descriptores por cada factor.

Tabla 1. Descriptores riesgos de gestión – Talento humano

Ejecución 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, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional.	
	Falta de aplicación de los procedimientos
	Falta segregación de funciones
	Errores de grabación, autorización
	Falta de supervisión o interventoría
	Errores en cálculos para pagos internos y externos
	Alta rotación o insuficiencia de personal
	Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
	Acciones contrarias a las leyes o acuerdos contractuales
	Falta de capacitación y otros temas relacionados con el personal

Fuente: OAP

Tabla 2. Descriptores riesgos de gestión – Transacción u operación aplica para LA/FT/FP

Transacción u operación aplica para LA-FT-FP: eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	
	Contrapartes de la entidad (naturales o jurídicas)
	Productos (bienes o servicios) que oferta/requiere
	Canales utilizados para la operación
	Jurisdicciones (nacional o territorial)

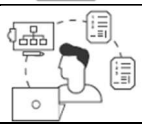
Fuente: OAP

Tabla 3. Descriptores riesgos de gestión – Talento humano

Talento humano: eventos relacionados con las conductas o comportamientos de los servidores públicos que afectan la Integridad Pública.	
	Fraude Interno
	Soborno
	Gestión inadecuada de conflicto de Intereses
	Corrupción
	Hurtos activos

Fuente: OAP

Tabla 4. Descriptores riesgos de gestión – Tecnología

Tecnología: eventos relacionados con la infraestructura tecnológica de la entidad.	
	Daño de equipos
	Caída de sistemas de información y aplicaciones
	Caída de redes
	Errores en hardware o software
	Errores en programas

Fuente: OAP

Tabla 5. Descriptores riesgos de gestión – Infraestructura

Infraestructura: eventos relacionados con la infraestructura física de la entidad.	
	Derrumbes
	Incendios
	Inundaciones
	Daños a activos fijos

Fuente: OAP

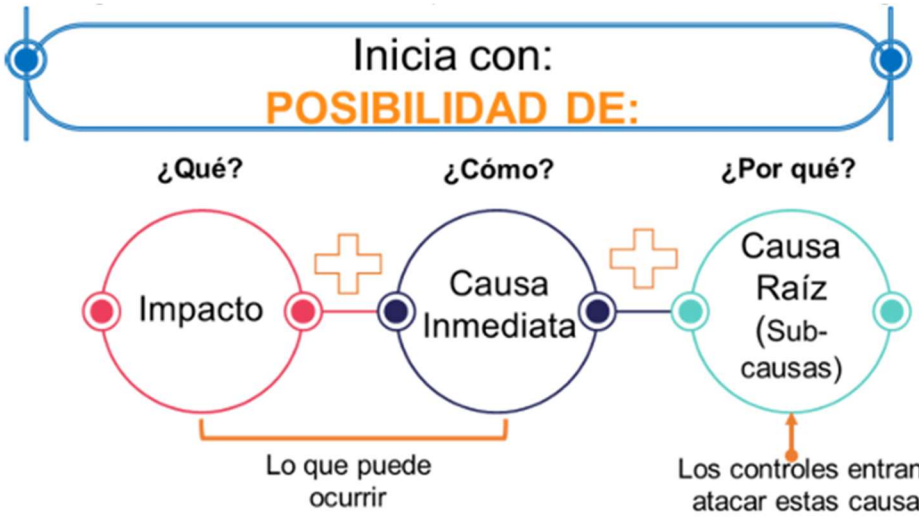
Tabla 6. Descriptores riesgos de gestión – Evento externo

Evento externo: eventos por situaciones externas que afectan la entidad.	
	Fraude externo
	Suplantación de identidad
	Asalto a la oficina
	Atentados, vandalismo, orden público

Fuente: OAP

A partir de los factores anteriores el paso a seguir es la descripción del riesgo y con el fin de hacer una redacción adecuada se toma la estructura propuesta así:

Ilustración 3. Estructura de redacción del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

De acuerdo con la anterior y para plantear el evento no deseado es decir *el qué puede ocurrir* el suceso evento que si ocurre puede afectar el logro de los objetivos institucionales se tienen los siguientes elementos:

- **Impacto:** las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la organización la materialización del riesgo.
- **Causa inmediata:** circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

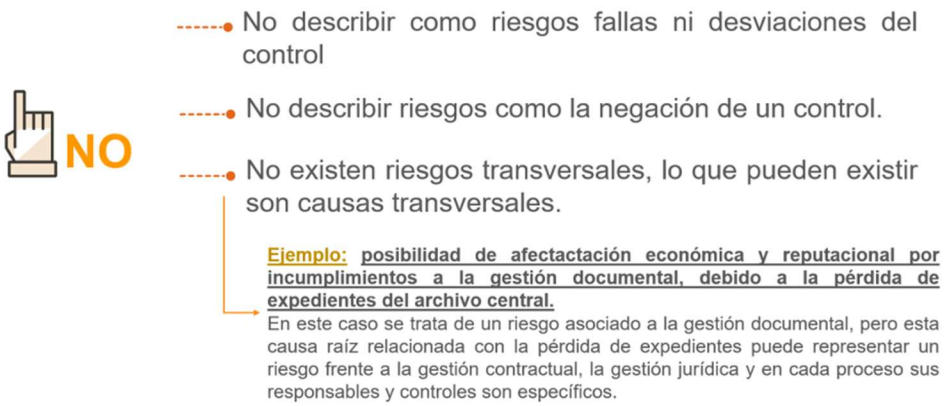
  Para tener en cuenta la descripción debe ser específica, clara y no genérica y expresado en términos de *qué podría pasar.*

- **Causa raíz:** se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles. Puede haber más de una causa para un mismo riesgo.

Para tener en cuenta en la identificación de las causas pueden ser de características humanas, tecnológicas, normativas, ambientales, organizacionales.

Con el fin de redactar adecuadamente el riesgo se debe tener en cuenta lo siguiente:

Ilustración 4. Premisas para redacción adecuada el riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Una explicación de la imagen anterior sería así:

- **Evento no deseado y sus posibles consecuencias:** ¿Qué puede pasar?
- **Causas:** ¿Por qué puede pasar?
- **Tipología:** ¿A qué categoría pertenece?
- **Factor de riesgo:** ¿Qué condición aumenta su probabilidad?

Un ejemplo de lo anterior sería el siguiente:

Tabla 7. Caracterización del riesgo

Evento no deseado ¿Qué puede pasar?	Causa ¿Por qué puede pasar?	Tipología ¿A que categoría pertenece?	Factor de riesgo ¿Qué condición aumenta su probabilidad?
Un agente de inteligencia deja olvidada una carpeta con información de la Entidad	Por no tener un lineamiento de sacar documentos físicos de las instalaciones y el funcionario tuvo un descuido.	**Ejecución administración de procesos** Falta de aplicación de los procedimientos Falta de capacitación y otros temas relacionados con el personal	A causa de la falta de un control de salida (registro de libros o carpetas) en los puntos de acceso de la entidad.

Fuente: OAP

Probabilidad: para determinar la probabilidad o la posibilidad de ocurrencia del riesgo se debe tener en cuenta la exposición al riesgo. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Para determinar la probabilidad del riesgo se deben definir las actividades del proceso. Un ejemplo para ello es el siguiente:

- **Riesgo:** posibilidad de afectación reputacional por falta de una prohibición de sacar documentos físicos de las instalaciones y el funcionario tuvo un descuido a causa de falta de un control de salida (registro de libros o carpetas) en los puntos de acceso de la entidad.
- **Actividad:** traslado y manejo de documentos clasificados entre dependencias.
- **Frecuencia: cuantas veces se realiza la actividad:** una vez al día.

La exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la siguiente imagen se establecen los criterios para definir el nivel de probabilidad.

Ilustración 5. Criterios para definir el nivel de probabilidad

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Siguiendo con el mismo ejemplo y de acuerdo con los criterios de la imagen anterior, si la actividad se realiza una vez al día en un periodo de 1 año, quiere decir que se realiza 365 veces lo que corresponde a una probabilidad media.

Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año

Impacto: el impacto son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. El impacto se medirá en términos económicos y reputacionales como se muestra en la siguiente imagen.

Ilustración 6. Criterios para definir el nivel de impacto

Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico-100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Continuando con el mismo ejemplo se debe tener en cuenta si el riesgo afecta reputacional mente de la siguiente manera:

- El riesgo afecta la imagen de algún área de la organización.
- El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
- El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
- El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
- El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Riesgo: posibilidad de afectación reputacional por falta de una prohibición de sacar documentos físicos de las instalaciones y el funcionario tuvo un descuido a causa de falta de un control de salida (registro de libros o carpetas) en los puntos de acceso de la entidad.

- **Probabilidad:** Media 60%
- **Afectación económica:** Mayor a 50 SMLMV y menor a 100 SMLMV

- **Afectación reputacional:** El riesgo afecta la imagen de algún área de la organización. Esta afectación reputacional corresponde a un nivel leve. 20%

Para calcular el resultado del impacto inherente, se toma la afectación económica y la reputacional y se toma la mayor. En este caso se tiene afectación económica en un nivel medio 60% y la afectación reputacional en un nivel leve 20%. El resultado para este ejemplo queda así:

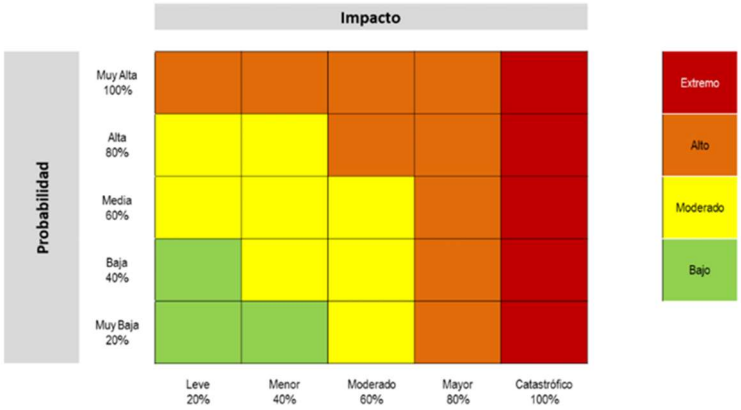
Tabla 8. Impacto ejemplo

Riesgo	Porcentaje de impacto	Nivel de impacto
Posibilidad de afectación reputacional por falta de una prohibición de sacar documentos físicos de las instalaciones y el funcionario tuvo un descuido a causa de falta de un control de salida (registro de libros o carpetas) en los puntos de acceso de la entidad.	60%	Moderado

Fuente OAP

Análisis de severidad: para el análisis de severidad se definen 4 niveles que son: Extremo, alto, moderado y bajo.

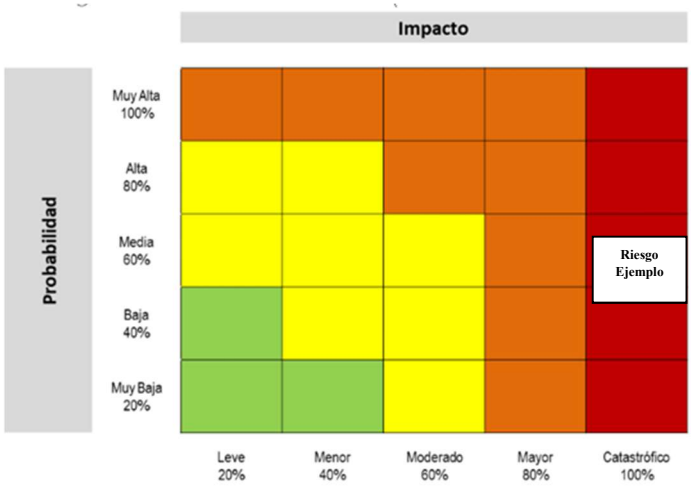
Ilustración 7. Niveles de severidad de riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Para el ejemplo identificado en el cual la probabilidad es media y el impacto es medio se ubica como se muestra a continuación.

Ilustración 8. Nivel de severidad ejemplo



Fuente: OAP

2.2.1. Diseño y Análisis de Controles

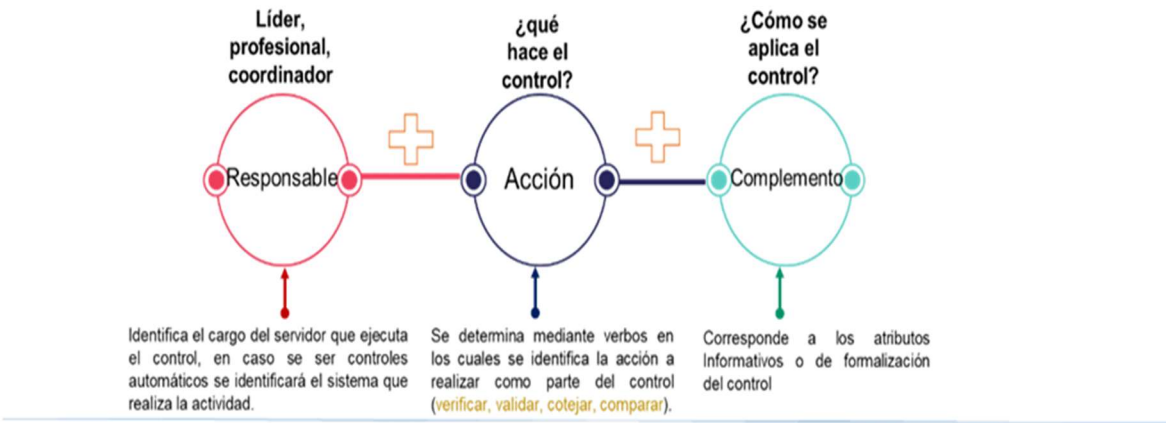
Las actividades de control son acciones concretas y con unos atributos específicos que son establecidas a través de políticas, procedimientos u otras directrices o documentos institucionales e implementadas con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos.

La identificación y diseño de las actividades de control se fundamentan en un análisis técnico que integra el conocimiento experto de los líderes de proceso con la base documental de la entidad (manuales, guías y procedimientos). Este enfoque asegura que cada control esté alineado con la realidad operativa y ataque directamente las causas raíz y los factores de riesgo identificados.
Para garantizar su efectividad, el diseño de estas actividades incorpora atributos críticos como la asignación clara de responsables, la segregación de funciones y niveles de autoridad adecuados, permitiendo así una mitigación real de la exposición al riesgo en el quehacer institucional.

2.2.2. Estructura para la descripción del control

La estructura propuesta se define a continuación:

Ilustración 9. Estructura para la redacción de control



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Atributos del control:

- **Responsable:** determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional. Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización.
- **Acción:** determina para qué se realiza el control, se utiliza verbos fuertes como: verificar, validar, conciliar, comparar, revisar, cotejar, detectar.
- **Atributos informativos o de formalización del control:** corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado.

Tabla 9. Atributos del control

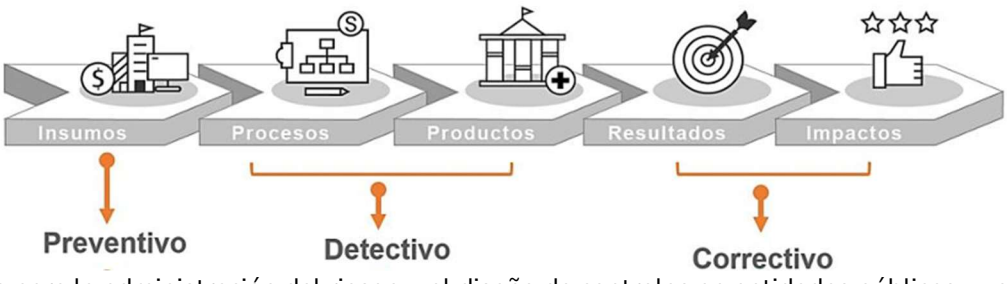
Atributo Informativo o de formalización del control	Descripción
Documentación	Se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
Frecuencia	Corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
Evidencia	Permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
Ejecución	Permite establecer cómo se ejecuta el control.

Fuente: OAP

Adicional a la anterior estructura se tienen los tipos de controles. Con el fin de establecer la tipología de controles para su posterior validación, es necesario acudir al ciclo de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo, o bien una combinación de estos.

Para determinar esta tipología se tiene en cuenta la cadena de valor de los procesos de la siguiente manera:

Ilustración 10. Tipología de controles



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

- **Control preventivo:** accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

- **Control detectivo:** accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** accionado en la salida del proceso y después de que se materializa el riesgo, Se debe tener en cuenta que los controles que se contemplan en esta tipología usualmente tienen que ver con pólizas de seguro, copias de seguridad bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez materializado, los cuales se implementan de forma preventiva

Nota: Control manual: ejecutados por personas. Control automático: ejecutados por un sistema o software previamente programado o diseñado.
A continuación, se muestra la valoración para cada tipo de control.

Ilustración 11. Valoración de controles

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

La formalización del control se da a partir de la siguiente información:

Documentación

- **Procedimiento:** basados en la estructura del modelo de operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
- **Sistemas de información:** sistemas de información de apoyo a la ejecución del control (si existen).
- **Otros esquemas:** políticas de operación, manuales o guías específicas.

Frecuencia

- **Siempre que se ejecuta la actividad / Periódicamente (diario, mensual, bimestral, trimestral, semestral):** la oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.

Evidencia

- **Con registro manual / Con registro electrónico:** se deja evidencia o rastro de la ejecución del control.

Ejecución (Fuentes de información internas o externas)

- **Interna / Externa:** registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
- **Mixtas:** combinación de datos de fuentes internas y externas formales.

Para el ejemplo de riesgo que llevamos la identificación de los controles serían los siguientes:

Ilustración 12. Descripción del riesgo ejemplo

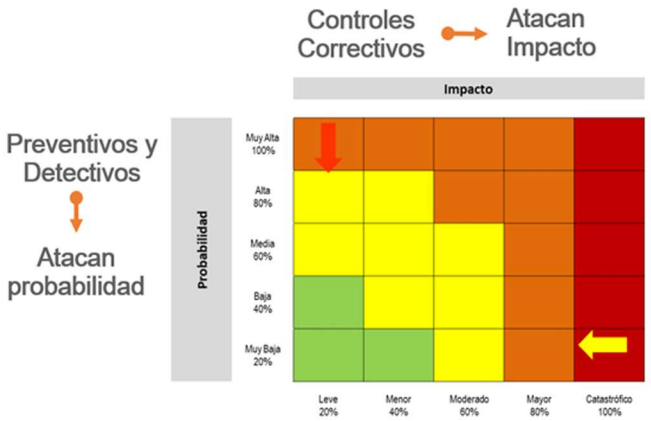
Riesgo	Control	Periodicidad	Tipo de control	Peso del control	Implementación	Peso de la implementación	Documentación	Frecuencia	Evidencia	Ejecución
Posibilidad de afectación reputacional por falta de una prohibición de sacar documentos físicos de las instalaciones y el funcionario tuvo un descuido a causa de falta	Establecer procedimiento de prohibición absoluta de retirar documentos con nivel de clasificación (Secreto/Reservado) de las zonas seguras.	Permanente	Preventivo	25%	Manual	15%	Procedimientos	Diario	Con registro manual	Interna
	Implementar una minuta en las esclusas de salida donde el personal de seguridad de la entidad una inspección visual y registre que ningún funcionario porta carpetas o expedientes sin un "Salvo Conducto	Permanente	Detectivo	15%	Manual	15%	Procedimientos	Diario	Con registro manual	Interna

Riesgo	Control	Periodicidad	Tipo de control	Peso del control	Implementación	Peso de la implementación	Documentación	Frecuencia	Evidencia	Ejecución
de un control de salida (registro de libros o carpetas) en los puntos de acceso de la entidad.	de Documentación" debidamente autorizado.									
	Realización de arqueos aleatorios sobre el inventario de documentos entregados a los analistas contra lo que efectivamente reposa en sus archivos físicos, para detectar faltantes de manera temprana.	Trimestral	Correctivo	10%	Manual	15%	Procedimientos	Trimestral	Con registro manual	Interna

Fuente OAP

A partir de esta tabla anterior, el siguiente paso es aplicar estos controles a la matriz de severidad y para ello se tiene en cuenta la siguiente imagen.

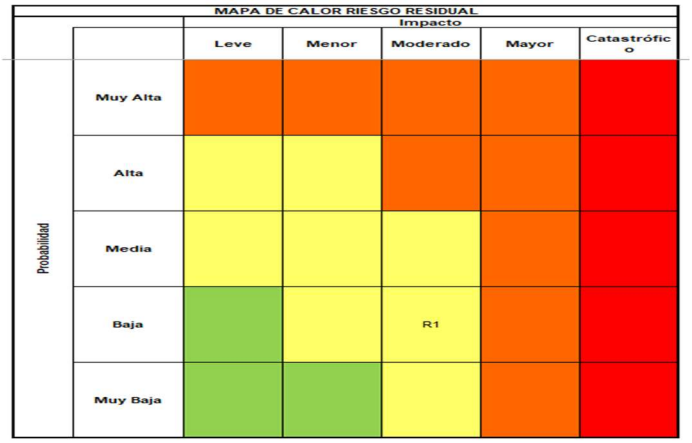
Ilustración 13. Movimiento en la matriz de calor acorde a los controles



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Esta imagen anterior muestra el movimiento de los ejes de probabilidad e impacto luego de aplicar los controles. De acuerdo con los controles del riesgo del ejemplo ésta es la imagen que se obtiene que es el riesgo residual:

Ilustración 14. Riesgo residual



Fuente: OAP

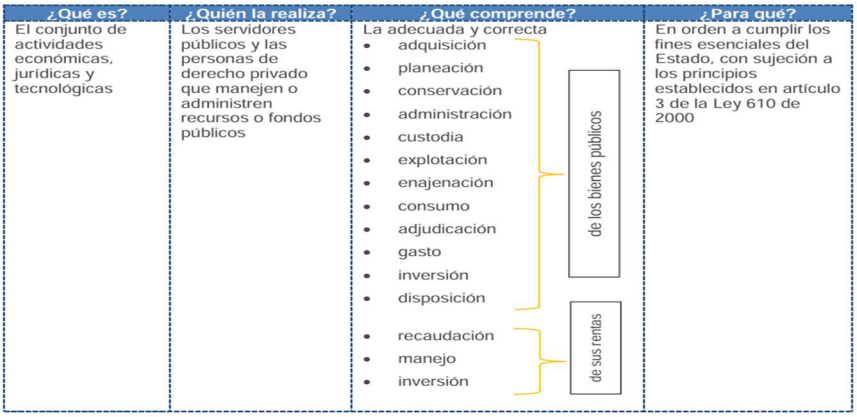
Riesgo ejemplo

La imagen muestra que el riesgo pasa a probabilidad baja y se mantiene en impacto moderado.

2.3. Riesgos Fiscales

A partir de la siguiente imagen lo que se busca es orientar el análisis de la operación de la UIAF para identificar y gestionar los riesgos que puedan provocar un daño patrimonial al Estado. Los componentes de la gestión fiscal son los siguientes:

Ilustración 15. Componentes de la gestión fiscal



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Lo que se busca con la gestión de riesgos fiscales es gestionar de manera efectiva los recursos, bienes e intereses patrimoniales de naturaleza pública, con el fin de prevenir efectos dañosos, lo cual a la vez permite mitigar la posibilidad de afectación al patrimonio por parte de los diferentes gestores fiscales.

2.3.1. Elementos del riesgo fiscal

El riesgo fiscal se define así: **efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.**

- **Efecto dañoso:** es el daño que se generaría sobre los recursos, los bienes y/o intereses 73 patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.
- **Evento potencial:** hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos, los bienes y/o los intereses patrimoniales de naturaleza pública.

A continuación, se resume el riesgo fiscal de la siguiente manera:

Ilustración 16. Definición de riesgo fiscal

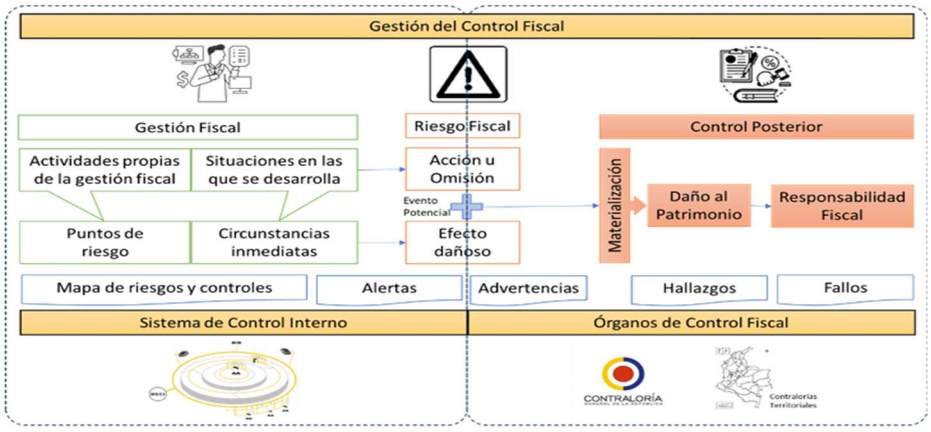
Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso (Potencial Daño)

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Nota: en el modelo multinivel, la gestión del riesgo fiscal corresponde a todos los responsables de la implementación y sostenibilidad del sistema de control interno, mientras que la determinación de hallazgos fiscales y el establecimiento de la responsabilidad sobre el daño patrimonial corresponderá al órgano de control fiscal.

En la siguiente imagen se observa la relación entre el sistema de control interno y los órganos de control fiscal

Ilustración 17. Gestión del control fiscal



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

La imagen anterior muestra la relación que existe entre el sistema de control interno y los órganos de control, el cual es de vital importancia para la identificación de los riesgos fiscales de la UIAF y su gestión.

2.3.2. Identificación de riesgo fiscal

Para la identificación de riesgos ficales se deben seguir los siguientes pasos.

Ilustración 18. Pasos para la identificación de riesgo fiscal

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Puntos de riesgo y de circunstancias inmediatas: los puntos de riesgo fiscal son eventos en los que potencialmente se genera riesgo fiscal para lo cual es pertinente prestar especial atención a aquellas en las cuales se han generado advertencias, alertas, hallazgos fiscales o fallos con

responsabilidad fiscal. En cuanto a las circunstancias inmediatas son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo.

Para la identificación de los puntos de riesgo se debe tener en cuenta la siguiente:

- Identificar los procesos que realizan control fiscal.
- Tomar como guía los puntos de riesgos identificados para identificarlas dentro de los procesos de la Entidad. Con esto se pueden identificar puntos de riesgo fiscal y circunstancias inmediatas.
- Identificar las advertencias que la Contraloría haya hecho a la Entidad y en qué proceso, así como las alertas reportadas en el Sistema de Control Interno – SCI.

Se recomienda realizar un análisis de causas muy juicioso al interior de la Entidad y no hacer copia de las que se emiten por el órgano de control.

Identificación de áreas de impacto: dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Para esta identificación se debe tener claro lo siguiente:

- **Bienes públicos:** son todos aquellos muebles e inmuebles de propiedad pública (bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público (aquellos cuyo uso pertenece a todos los habitantes del territorio nacional) y bienes fiscales (aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos).
- **Recursos públicos:** son los dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Intereses patrimoniales de naturaleza pública:** son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica.

2.3.3. Identificación del efecto económico

El efecto económico del riesgo fiscal es el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público. Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales representan un efecto económico.

A continuación, se relacionan efectos económicos que no son riesgos fiscales:

- Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.
- Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público.
- Multas impuestas por hechos que no comportan gestión fiscal.
- Existencia de actuación de cobro coactivo por parte de la entidad.
- Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.
- Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su “normal uso” (máquinas eléctricas, computadores, celulares, etc.)

2.3.4. Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro.

La causa raíz es un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

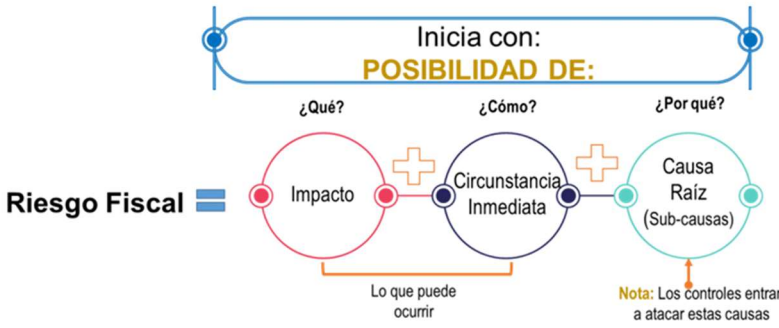
2.3.5. Descripción del riesgo fiscal

Para redactar un riesgo fiscal, se debe tener en cuenta:

- **Iniciar con la expresión:** posibilidad de, dado que nos estamos refiriendo al evento potencial.
- **Impacto:** corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre el área de impacto (recursos públicos, bienes o intereses patrimoniales de naturaleza pública).
- **Circunstancia inmediata:** corresponde al cómo. Se refiere a aquella situación en la que se presenta el riesgo; pero no constituye la causa principal que lo genera.
- **Causa raíz:** corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño. Es la condición necesaria del riesgo, de tal forma que, si ese hecho no se produce, el daño no se genera.

Lo anterior se puede ver de la siguiente manera:

Ilustración 19. Descripción del riesgo fiscal



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

De acuerdo con la anterior imagen se tiene la siguiente:

- **Impacto:** Se refiere al QUÉ, posibilidad de efecto dañoso sobre los intereses patrimoniales.
- **Circunstancia inmediata:** se refiere al CÓMO, por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora.
- **Causa raíz:** se refiere al POR QUÉ, a causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

La descripción del riesgo quedaría como “Posibilidad de efecto dañoso sobre los intereses patrimoniales por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora a causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo”.

2.3.6. Valoración del riesgo fiscal

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

- **Probabilidad:** la probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.
- **Impacto:** considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso recae sobre un bien, recurso o interés patrimonial de naturaleza pública.
- **Determinación del nivel de riesgo inherente:** a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad.

Para evaluar el riesgo fiscal se utiliza la misma manera que se realiza con los riesgos de gestión.

2.3.7. Valoración de controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Los controles pueden ser preventivos, detectivos o correctivos dependiendo el momento (antes, durante o después) en que se accionen respecto a la actividad que origina el riesgo fiscal (punto de riesgo). Los controles preventivos buscan asegurar que no se presente la causa raíz, los controles detectivos buscar tomar medidas ante la ocurrencia de la causa raíz para evitar que se produzca el efecto dañoso y los controles correctivos actúan ante el daño potencial, procurando detener su materialización o reparando el daño causado.
Para la redacción de los controles se realiza de la misma manera que para los controles de los riesgos de gestión.

El riesgo residual se calcula de la misma manera que en los riesgos de gestión y el movimiento en el mapa de calor se realiza de la misma manera.

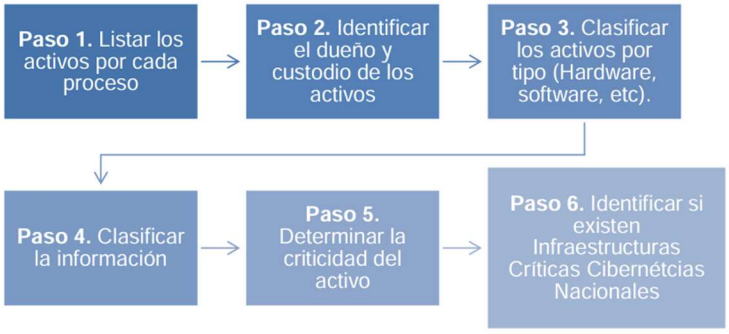
2.4. Riesgos de seguridad de la información

Los riesgos de seguridad de la información permiten incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información de la UIAF.

2.4.1. Identificación de riesgos de seguridad de la información

Para la identificación de los activos de información se deben tener en cuenta los lineamientos establecidos por el MinTIC para ello. Los pasos para la identificación son los siguientes:

Ilustración 20. Pasos para la identificación y valoración de activos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Se deben listar cada uno de los activos de información de la entidad luego, para cada activo se deben registrar:

- **Proceso:** proceso de la Entidad al que pertenece el activo de información.
- **Identificador:** se sugiere que el identificador sea una concatenación del código de la dependencia según la Tabla de Retención Documental (TRD) + número consecutivo.
- **Tipo:** Define el tipo de Activo de Información.

Tabla 10. Tipos de activos de información

Tipo de activo de información	Descripción
Información y datos de la UIAF	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	N/A
Instalaciones	N/A
Redes	N/A

Fuente: OAP

- **Oficina:** dependencia o proceso que está identificando el activo de información.
- **Serie documental:** serie documental del área, dependencia o proceso que se encuentra identificando el activo.
- **Subserie documental:** subserie documental del área, dependencia o proceso que se encuentra identificando el activo.
- **Nombre:** nombre completo del activo de información.
- **Descripción:** descripción resumida de manera clara para identificar el activo de información.
- **Nombre del responsable de la producción de la información (Propietario del activo):** Nombre del área, dependencia, proceso responsable de producir el activo de información.
- **Fecha de generación de la información:** fecha en la que el activo de información fue incluido en el inventario – TRD.

- **Nombre del responsable de la información (Custodio del activo):** corresponde al nombre del área, proceso o dependencia encargada en la Entidad de la custodia o control de la información o implementación de controles de protección.
- **Fecha de ingreso del activo al archivo:** fecha en la que el activo ingresa al archivo de gestión.
- **Soporte de registro:** de acuerdo con el Decreto 2609 de 2012:

Tabla 11. Descripción de los tipos de soporte de registro

Soporte de registro	Descripción
Físico	(análogo)
Digital	(electrónico) Este campo se diligencia si el Tipo de activo es "Información"
N/A	Para el resto de los tipos de activos se debe seleccionar N/A

Fuente: OAP

- **Medio de conservación:** de acuerdo con el Decreto 2609 de 2012 el archivo institucional es la instancia administrativa de custodiar, organizar y proteger.
- **Formato:** identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: hoja de cálculo, imagen, audio, video, documento de texto, etc.
- **Idioma:** establece el idioma, lengua o dialecto en que se encuentra la información.

Luego de hacer la identificación y descripción de los activos de información, se realiza la clasificación de acuerdo con la propiedad correspondiente: disponibilidad, integridad y confidencialidad.

Para cada activo se define el nivel de criticidad de la propiedad específica, para cada propiedad, Alta, Media y Baja, que corresponden con Criterios de Clasificación para cada una de las propiedades de la Información como se va a continuación.

Ilustración 21. Criterios de clasificación de activos

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

El nivel de clasificación del activo corresponderá con el resultado de la sumatoria de la tabla de criterios de clasificación siguiente:

Ilustración 22. Niveles de clasificación de activos

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

2.4.2. Nivel de criticidad del activo

- **Es infraestructura critica cibernética nacional:** se define si el activo corresponde con los criterios de infraestructura critica cibernética descritos en los "lineamiento para la identificación de las infraestructuras críticas cibernéticas" del MSPI.
- **Información publicada:** se define si el activo está publicado en la intranet, en internet o no está publicado.

Tabla 12. Estado de la información

Estado de la información	Descripción
Publicada	Si la información es publica y se puede consultar en un sitio web (interno o externo) o un sistema de información del Estado. Interno - Intranet Externo - Internet
No publicada	Si la información se encuentra en la Entidad, pero no se encuentra en un sistema de información o sitio web.

Fuente: OAP

- **Lugar de consulta o ubicación:** indica la URL, sitio web o sistema de información donde puede ser consultada la información si esta se encuentra pública, el lugar de consulta si no está publicada o ubicación física.

Ilustración 23. Clasificación de activos

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)						
Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	Es Infraestructura Critica cibernética	Información publicada	Lugar de consulta o ubicación

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

2.4.3. Índice de información clasificada

Tabla 13. Índice de información clasificada

Índice de Información Clasificada y Reservada	Descripción
Objeto legítimo de la excepción	La identificación de la excepción que, dentro de las previstas en los artículos 18 y 19 de la Ley 1712 de 2014, cobija la calificación de información reservada o clasificada. Si la respuesta es NO se debe marcar no aplica (N/A) en los demás campos sobre el índice de información clasificada y reservada.
Fundamento constitucional o legal	Indica el fundamento constitucional o legal que justifica la clasificación o la reserva, señalando expresamente la norma, artículo, inciso o párrafo que la ampara.

Índice de Información Clasificada y Reservada	Descripción
Fundamento jurídico de la excepción	Indica la norma jurídica que sirve como fundamento jurídico para la clasificación o reserva de la información.
Excepción total o parcial	Según sea integral o parcial la calificación, las partes o secciones clasificadas o reservadas. Indicar si la totalidad del documento es clasificado o reservado o si solo una parte corresponde a esta calificación.
Fecha de clasificación (DD/MM/AAAA)	Fecha en que se calificó la información como reservada o clasificada.
Tiempo de clasificación	Tiempo que cobija la clasificación o reserva. La clasificación es ilimitada en años, la reserva solo puede durar el tiempo establecido por la ley.

Fuente: OAP

Ilustración 24. Índice de información clasificada

ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA (DECRETO 103 DE 2015)					
Objeto legítimo de la excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción total o parcial	Fecha de clasificación (DD/MM/AAAA)	Tiempo de clasificación

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

2.4.4. Activos de información – datos personales.

- **¿Contiene datos personales?:** ¿El activo de información contiene datos personales? SI – NO
- **¿Contiene datos personales de niños, niñas o adolescentes?:** son los datos personales de los niños, niñas y adolescentes, cuyo tratamiento está prohibido, salvo que se trate de datos de naturaleza pública. Ej. Registro civil.
- **Tipos de datos personales:** si cuenta con datos personales seleccione el tipo, en caso contrario seleccione N/A.

Tabla 14. Tipos de datos personales

Tipos de datos personales	Descripción
Dato personal público	Toda información personal que es de conocimiento libre y abierto para el público en general. Ejemplo: Número de identificación apellidos.
Dato personal privado	Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general. Ejemplo: Dirección de residencia y No. teléfono.
Dato semiprivado	Es semiprivado el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector y grupo de personas. Ejemplo: fecha y lugar de nacimiento

Fuente: OAP

- **Finalidad de la recolección de los datos personales**: la finalidad de la recolección justifica por la cual el dato es capturado, almacenado y mantenido en la Entidad.
- **Existe la autorización para el tratamiento de los datos personales:** seleccionar si se cuenta o no con la autorización de la recolección y tratamiento.

Ilustración 25. Datos personales

DATOS PERSONALES (LEY 1581 DE 2012)				
¿Contiene datos personales?	¿Contiene datos personales de niños, niñas o adolescentes?	Tipos de datos personales	Finalidad de la recolección de los datos personales	Existe la autorización para el tratamiento de los datos personales

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Nota: *Posterior a la identificación, clasificación y valoración de los activos de información compilados en la Matriz de Activos de Información por los líderes de los procesos, se debe enviar la matriz para su consolidación y validación por parte de la Oficina Asesora Jurídica para finalmente ser presentada ante el Comité Institucional de Gestión y Desempeño.*

El resultado de esta actividad es la **Matriz del Inventario de Activos de Información** que es el insumo principal para la Gestión de Riesgos de Seguridad de la Información proceso que se encuentra descrito en la Guía.

A partir de la matriz de inventario de activos de información y de acuerdo con el nivel de criticidad se realiza el correspondiente análisis de riesgos.
Como ejemplo se tiene el siguiente:

Listado y registro de activos:

Ilustración 26. Registro de activos

Proceso	Identificador	Tipo	Oficina	Serie documental	Subserie documental
Gestión de nomina	Gestión Financiera	Software	Financiera	001	00001
Gestión de nomina	Gestión Financiera	Software	Financiera	001	00001

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Activo de información

Ilustración 27. Activos de información

Nombre	Descripción	Nombre del responsable de la producción de la información (Propietario del activo)	Fecha de generación de la información	Nombre del responsable de la información (Custodio del activo)
Software de gestión de nómina (Pagosnet)	Software de gestión de nomina	Director TI	12/03/2025	Analista nomina
Informe pagos de nómina periodo: ene-2025 a marzo-2025	Informe de los pagos de nómina realizados den el periodo: ene-2025 a marzo-2025	Director Financiero	12/03/2025	Analista nomina
Fecha de ingreso del activo al archivo	**Soporte de registro**	**Medio de conservación**	**Formato**	**Idioma**
22/11/2000	Digital	Sistemas de Información corporativos	Software de gestión de nomina	Español
22/11/2000	Digital	Sistemas de Información corporativos	Software de gestión de nomina	Español

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Clasificación de activos

Ilustración 28. Clasificación de activos de información

Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	¿Es Infraestructura Crítica Cibernética?	Información publicada	Lugar de consulta o ubicación
Clasificada / Uso Interno = Medio	Alto	Alto	ALTA	No	Publicada (Interno - Intranet)	Intranet
Clasificada / Uso Interno = Medio	Alto	Alto	ALTA	No	Publicada (Interno - Intranet)	Sharepoint

Objeto legítimo de la excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción total o parcial	Fecha de clasificación (DD/MM/AAAA)	Tiempo de clasificación
N/A	N/A	N/A	N/A	N/A	N/A
Si	artículo 18 de la ley 1712 de 2014	artículo 18 de la ley 1712 de 2014	Reserva parcial	15/03/2025	15 años

¿Contiene datos personales?	¿Contiene datos personales de niños, niñas o adolescentes?	Tipos de datos personales	Finalidad de la recolección de los datos personales	Existe la autorización para el tratamiento de los datos personales
N/A	N/A	N/A	N/A	N/A
Si	No	Dato semiprivado	Realizar el pago de nomina	Si

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Matriz riesgos de seguridad la información

Con base en la criticidad se realiza el proceso de gestión de riesgos, la cual registra en la Matriz de Riesgos de Seguridad de la Información, con respecto al activo de información se registran los siguientes datos.

Ilustración 29. Matriz de riesgos de seguridad de la información

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN			
Proceso	Referencia	Activo de Información	Tipo de Activo

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

- **Proceso:** proceso al cual se encuentra asignado el activo de información.
- **Referencia:** es el número del ítem del activo de información.
- **Activo de información:** es el nombre del activo de información.
- **Tipo de activo:** corresponde a una de las siguientes categorías.

Tabla 15. Tipos de activos de información

Tipo de activo
Información
Software
Hardware
Servicios
Intangibles
Infraestructura crítica cibernética nacional
Recursos humanos
Instalaciones y otros servicios

Fuente: OAP

2.4.4.1. Identificación de áreas de impacto

El área de impacto es la consecuencia negativa en los objetivos de la organización en caso de materializarse un riesgo o las que por causa de incidentes de seguridad de la información tenga consecuencias en la gestión de la entidad.

2.4.4.2. Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos.

- **Amenaza:** causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022). Pueden ser Deliberadas (D), Fortuitas (F) o Ambientales (A).
- **Vulnerabilidad:** debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

A continuación, se definen las amenazas y las vulnerabilidades más comunes:

Tabla 16. Amenazas

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F

Tipo	Amenaza	Origen
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: OAP

Tabla 17. Vulnerabilidades

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección

Tipo	Vulnerabilidades
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: OAP

2.4.5. Descripción del riesgo

En este paso se identifica el tipo, la descripción y la clasificación del riesgo.

Tipo de riesgo: Este campo solo admite uno de estos 3 valores

- Pérdida de Disponibilidad
- Pérdida de Integridad
- Pérdida de Confidencialidad

Descripción del riesgo: en este campo se describe la situación específica que da como resultado el correspondiente riesgo.

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Clasificación del riesgo: este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad.

2.4.6. Análisis de riesgo inherente

De aquí en adelante se aplica la misma metodología para los riesgos de gestión.

Determinar la probabilidad

En esta actividad se debe realizar el análisis de probabilidad de la materialización de estos riesgos.

- **Frecuencia:** este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.
- **% Probabilidad inherente:** este campo corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa.
- **Probabilidad inherente:** este campo corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa. (igual que los riesgos de gestión).

Ilustración 30. Probabilidad riesgos

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

Determinar impacto

En esta actividad se debe realizar el análisis del impacto de la materialización de estos riesgos.

- **% Impacto inherente:** este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa.
- **Impacto inherente:** este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa.

Ilustración 31. Impacto riesgos

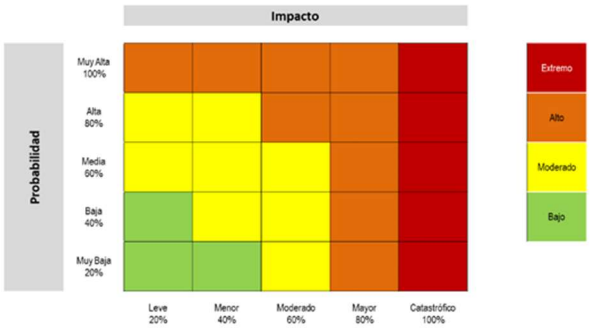
Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico-100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

2.4.7. Análisis de Severidad

Zona de riesgo inherente: en este campo se determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto.

Ilustración 32. Zonas de riesgos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

2.4.8. Diseño y análisis de controles

Estructura para la descripción del control

En esta actividad se seleccionan los controles que se establecerán para mitigar los riesgos.

- **No de control:** este campo es un consecutivo de los controles a establecer.
- **Control Anexo A:** este campo corresponde al control seleccionado del Anexo A de la norma 27001:2022.
- **Descripción del control:** este campo corresponde a una descripción de la forma en la cual el control seleccionado será implementado en la entidad. *NOTA: se recomienda establecer para cada control técnico el correspondiente control administrativo, de tal manera que estos se complementen y potencialicen.*

Valoración de controles

Afectación

En esta actividad se establece la afectación que tendrá la implementación del control sobre la Probabilidad o el Impacto del riesgo.

- **Probabilidad:** en este campo se especifica si el control pretende modificar la probabilidad de ocurrencia de riesgo.
- **Impacto:** en este campo se especifica si el control pretende modificar el impacto de ocurrencia de riesgo.

Atributos

En esta actividad se establecen los Atributos de la implementación del control, donde se consideran atributos de eficiencia y los de formalización del control.

Ilustración 33. Valoración de controles

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 7

La formalización del control se realiza de la misma manera establecida anteriormente en los riesgos de gestión.

Valoración del riesgo residual

Se lleva a cabo de la misma manera establecida para los riesgos de gestión.

2.4.9. Plan de implementación de controles

En esta actividad se establece un plan para implementar los controles y poder realizar el correspondiente seguimiento.

Tabla 18. Plan de implementación de controles

PLAN DE IMPLEMENTACIÓN DE CONTROLES					
Tratamiento	**Plan de Acción**	**Responsable**	**Fecha de implementación**	**Seguimiento**	**Estado**
En este campo se especifica el tipo de tratamiento que se realizará entre 4 opciones disponibles. **Reducir:** implementar controles para reducir la probabilidad o el impacto. **Compartir:** compartir las consecuencias de la materialización del riesgo, por ejemplo, a través de la adquisición de una póliza. **Aceptar:** cuando el nivel del riesgo está por debajo del apetito establecido por la alta dirección. **Evitar:** cuando se decide eliminar el activo que es fuente del riesgo: por ejemplo, dar de baja un servidor.	En este campo se especifica la identificación del Plan de acción con el cual se realizará la implementación de dicho control.	En este campo se especifica el cargo de quien implementa el control.	En este campo se especifica la Fecha máxima de implementación del control.	En este campo se especifica la periodicidad del seguimiento a la implementación del control.	En este campo se especifica el estado de la implementación del control.

Fuente: OAP

2.5. Integración de Riesgos de SST y Ambientales

Si bien la presente Política de Riesgos adopta un enfoque holístico bajo el Modelo Integrado de Planeación y Gestión (MIPG), se establece una distinción metodológica para los riesgos de Seguridad y Salud en el Trabajo (SST) y Ambientales. Debido a su naturaleza técnica, requerimientos legales específicos y matrices de impacto diferenciadas, estos riesgos se

integran en este sistema para garantizar la unidad administrativa, pero su identificación, valoración y control se rigen por los estándares técnicos propios de sus respectivos sistemas de gestión, asegurando así una respuesta especializada sin perder la visión integral de la entidad.

2.5.1. Identificación Riesgos de Seguridad y Salud en el Trabajo

2.5.1.1. Identificación de los Peligros y Valoración de Riesgos en SST

El propósito general de la identificación es entender los peligros que se pueden generar en el desarrollo de las actividades, con el fin que la entidad pueda establecer los controles necesarios, al punto de asegurar que cualquier riesgo sea aceptable.

Aspectos claves para la Identificación de los Peligros

Para asegurar una identificación técnica y exhaustiva, la entidad seguirá este ciclo de gestión:

- **Definir el instrumento:** establecer y mantener una herramienta técnica (matriz) que permita registrar de forma sistemática la información para la identificación de peligros y valoración de los riesgos.
- **Clasificación de operaciones:** categorizar los procesos, actividades y tareas, incluyendo instalaciones, planta física, personal y procedimientos operativos.
- **Identificación de peligros:** determinar de forma específica quién, cuándo y cómo los trabajadores pueden resultar afectados por cada actividad laboral.
- **Análisis de controles existentes:** relacionar y evaluar las medidas que la organización ya tiene implementadas para reducir el impacto o la probabilidad de cada riesgo.
- **Construcción del plan de acción:** diseñar estrategias para mejorar los controles actuales o implementar nuevos, según la necesidad detectada en la valoración.
- **Validación de conveniencia:** re-valorar los riesgos proyectados tras la implementación de los controles propuestos para asegurar que el riesgo final sea asumible por la entidad.

Mantenimiento, Actualización y Trazabilidad

Para garantizar que la gestión no sea estática, se establecen las siguientes directrices:

- **Mantenimiento y actualización:** realizar un seguimiento continuo para asegurar que tanto los controles nuevos como los existentes sean efectivos y que la valoración del riesgo refleje la realidad actual de la entidad.

- **Documentación de trazabilidad:** registrar formalmente la ejecución de los planes de acción, incluyendo responsables, cronogramas y estados de avance. Este registro constituye la memoria institucional de la gestión en Seguridad y Salud en el Trabajo.

La secuencia operativa detallada anteriormente se sintetiza en el siguiente esquema, el cual representa la ruta crítica que debe seguir cada dependencia de la entidad para garantizar la integridad del sistema.

Ilustración 34. Identificación riesgos de SST

Fuente: OAP

2.5.1.2. Definir el Instrumento para Recolectar Información

Para garantizar que la identificación de peligros y la valoración de riesgos se realice de manera técnica y uniforme en toda la entidad, se establece el uso de una herramienta sistemática de registro. Este instrumento permite capturar la realidad operativa y transformarla en datos para la toma de decisiones, debiendo ser actualizado periódicamente o cada vez que las condiciones laborales sufran modificaciones significativas.

A continuación, se describen los campos mínimos para la gestión de riesgos de SST.

Tabla 19. Contenido del instrumento de gestión de riesgos

Contenido del Instrumento de Gestión de Riesgos	
Categoría	**Campos de Información**
Caracterización técnica	Proceso, Zona/Lugar, Actividades y Tareas.
Naturaleza de la labor	Identificación de si la tarea es rutinaria (Si/No).
Identificación del peligro	Descripción del peligro, clasificación técnica y efectos posibles en la salud/seguridad.
Controles existentes	Medidas actuales aplicadas en la **Fuente**, el **Medio** o el **Individuo**.
Evaluación del riesgo	Cálculo del Nivel de Deficiencia (ND), Nivel de Exposición (NE), Nivel de Probabilidad (NP), Nivel de Consecuencia (NC) y Nivel de Riesgo (NR) con su respectiva interpretación.
Valoración del riesgo	Determinación de la **Aceptabilidad del Riesgo** conforme a los criterios institucionales.
Criterios de control	Número de expuestos, Peor consecuencia y existencia de Requisitos Legales asociados.
Medidas de intervención	Plan de acción basado en la jerarquía de controles: **Eliminación, Sustitución, Controles de Ingeniería, Controles Administrativos y EPP.**

Fuente: OAP

2.5.1.3. Metodología para la Descripción y Clasificación de Peligros

La identificación de peligros no debe limitarse a una lista estática; requiere un análisis crítico de cada entorno laboral. Para orientar este proceso, los líderes de proceso y servidores responsables deberán aplicar un enfoque basado en cuestionamientos preventivos:

- **Detección del riesgo:** ¿Existe una fuente, situación o acto con potencial de generar daño a la integridad física o mental?
- **Identificación del sujeto:** ¿Quién (personal interno, contratistas, visitantes) o qué (infraestructura, equipos) puede sufrir el daño?
- **Mecánica del evento:** ¿Cómo puede ocurrir el daño? (Análisis de la secuencia de eventos).
- **Temporalidad:** ¿Cuándo puede ocurrir el daño? (Análisis de jornadas, tareas rutinarias o condiciones excepcionales).

Inventario Institucional de Peligros

Cada dependencia de la entidad tiene la obligación de desarrollar y mantener actualizada su propia Lista de Peligros. Este inventario debe ser específico y considerar:

- **Naturaleza de las actividades:** riesgos propios de la labor administrativa, técnica o de campo.
- **Entorno geográfico y físico:** las condiciones particulares de las sedes, oficinas o puntos de atención al ciudadano donde se realiza el trabajo.

Para asegurar la pertinencia del sistema, la entidad desarrollará una lista de peligros personalizada. Este catálogo debe construirse a partir del análisis del carácter de sus actividades misionales y administrativas, considerando las variables del entorno físico y geográfico de los centros de trabajo donde opera la institución.

2.5.2. Identificación del Riesgos Ambiental

Esta etapa inicial tiene como objetivo reconocer de manera sistemática los riesgos que deben ser gestionados. Bajo los lineamientos de la GTC 104, es imperativo aplicar un proceso estructurado, dado que cualquier riesgo potencial omitido en esta fase quedará fuera del análisis posterior. La identificación debe ser exhaustiva, abarcando tanto los riesgos bajo control directo de la entidad como aquellos externos.

2.5.2.1. Metodología de Identificación

La identificación se desarrolla en niveles que van desde lo estratégico hasta lo operativo. Un examen detallado debe considerar el impacto en:

- Ecosistemas naturales y medio ambiente general.
- Comunidades y pueblos circundantes.
- Continuidad del negocio y procesos de la organización.

2.5.2.2. Proceso de Análisis de Fuentes e Impactos

Para una identificación técnica, la entidad seguirá la ruta lógica de fuente-ruta-receptor:

- **Identificar las fuentes de riesgo:** reconocer peligros, aspectos ambientales (elementos de las actividades que interactúan con el ambiente) e incidentes potenciales.
- **Describir el ambiente circundante:** analizar el entorno donde la entidad opera.

- **Identificar los impactos ambientales potenciales:** determinar el cambio en el medio ambiente, ya sea adverso o beneficioso, resultado de las actividades de la entidad.

Tabla 20. Estructura de análisis de impacto

Fuente (Peligro/Aspecto)	Ruta (Evento/Mecanismo)	Barrera (Control)	Receptor (Afectado)	Impacto (Consecuencia)
Energía: Química, Eléctrica, Mecánica, Ruido, Radiación, etc.	Fallas en planta, incendios, dispersión atmosférica, escurrimiento hídrico.	Medidas físicas, administrativas o reglamentarias.	Seres humanos, sociedad, instalaciones, patrimonio natural.	Afectación a la sostenibilidad, economía, patrimonio cultural o natural.
Operativa: Maquinaria, procesos e inventario de materias primas.	Rutas biológicas (ingestión, cadena alimentaria), vectores.	Controles de proceso y limpieza.	Ecosistemas, aguas subterráneas y suelo.	Daño ambiental, sanciones legales o pérdida de imagen.

Fuente: OAP

2.5.2.3. Comunicación del Riesgo Ambiental

La comunicación debe ser proactiva y temprana, especialmente cuando las actividades institucionales generen interés público.

- **Planificación:** iniciar el diálogo con las partes interesadas (Stakeholders) desde la fase de contexto.
- **Implementación:** utilizar medios de consulta efectivos para asegurar que todos los involucrados estén informados según su nivel de impacto.
- **Monitoreo:** el plan de comunicación debe revisarse periódicamente para verificar si cumple con los objetivos del proceso de gestión del riesgo.

3. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA – SIGRIP

Teniendo en cuenta la expedición de la Ley 2195 de 2022, que hace obligatorio para las entidades públicas la “prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional. Se sugiere por la secretaria de

transparencia implementar un Programa de Transparencia y Ética Pública contar con un sistema de gestión que le permita prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), de manera integral.

Dicho lo anterior, la UIAF adopta el Sistema de gestión para la integridad pública – SIGRIP el cual se articula con el programa de transparencia y ética pública.

A continuación, se define la integridad pública como el compromiso de los servidores públicos de actuar con coherencia, ética y valores, priorizando siempre el interés general por encima de los intereses privados. Se considera la principal barrera contra la corrupción y un pilar fundamental para recuperar la confianza ciudadana en las instituciones.

3.1. Amenazas para la integridad pública

La integridad pública no ocurre en un mundo perfecto. En el día a día, los servidores públicos enfrentan presiones, tentaciones y situaciones difíciles que ponen a prueba su honestidad. Estas son las llamadas amenazas para la integridad, y conocerlas es fundamental para saber cómo reaccionar a tiempo y proteger el bienestar de todos.

- **Soborno:** es básicamente el uso de "premios" (plata, regalos o favores) para torcer el deber de un servidor público. Es un camino de doble vía: **Entrante:** cuando alguien de afuera intenta "comprar" al servidor. **Saliente:** cuando el servidor ofrece algo para conseguir beneficios para su entidad.
- **Fraude:** ocurre cuando se altera la realidad (con mentiras, datos incompletos o informes falsos) para sacar un provecho propio o ayudar a alguien más. No siempre es un plan maestro; a veces es un "error" hecho a propósito o una omisión descuidada que termina en beneficio ilegal.
- **Inadecuada gestión del conflicto de intereses:** un conflicto de intereses ocurre cuando un servidor público debe tomar una decisión, pero en medio de ella está su propio beneficio o el de su círculo cercano (familia, pareja o socios). Es ese momento donde el bien de todos se choca de frente con el bien personal.

Lo más importante que hay que saber es que tener un conflicto no es un delito, lo que está mal es no decirlo. Es normal que a veces nuestras relaciones personales se crucen con el trabajo. El problema no es que el conflicto aparezca, sino ocultarlo para intentar beneficiar a los suyos en lugar de servir a la ciudadanía.

- **Corrupción:** la corrupción es desviar el poder o los recursos que son de todos para llenar bolsillos privados. No es solo robar dinero; es cualquier acto que use el cargo público para obtener ventajas personales, familiares o políticas.

- **LA/FT/FP:** El Lavado de Activos, la Financiación del Terrorismo y la Proliferación de Armas (LA/FT/FP) comprometen la integridad pública al utilizar a las entidades estatales como instrumentos para legalizar recursos ilícitos o financiar actos violentos. Estas conductas, que pueden afectar a la institución incluso sin la participación directa de sus funcionarios, debilitan la capacidad del Estado para cumplir sus fines.

3.2. Sistema de gestión del riesgo

Una vez identificadas las amenazas que acechan la labor pública (como el soborno, el fraude o el lavado de activos), el paso lógico para la Entidad es pasar de la teoría a la acción. No basta con saber que los riesgos existen; es necesario gestionarlos a través de una estructura sólida: el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP).

Este sistema funciona como un engranaje central donde todo se conecta. Su importancia radica en que un fallo en la gestión, un descuido fiscal o una brecha en la seguridad de la información suelen tener la misma raíz: un conflicto de intereses mal manejado o un acto de corrupción. Por eso, el SIGRIP no trabaja de forma aislada, sino articulada bajo un mismo objetivo, el de asegurar que cada proceso sea íntegro.

Para que este sistema sea efectivo en nuestra operación diaria, se apoya en tres pilares fundamentales:

I. **Instrumentos de gestión:** herramientas claras para identificar dónde somos vulnerables. (política ALA/CFT/CFP, política antisoborno, política antifraude, procedimiento para la gestión de los conflictos de intereses, procedimiento para el reporte de operaciones

sospechosas, procedimiento para la operación del canal institucional de denuncias por corrupción y buzón ético.

II. **Conocimiento de contrapartes:** la debida diligencia para saber con quién contratamos y nos relacionamos (evitando ser usados por el crimen organizado).

III. **Función de cumplimiento: un** rol activo que vigila que la ley se cumpla en cada rincón de la organización.

En definitiva, el SIGRIP es la garantía de que la gestión institucional no solo sea eficiente, sino que sea ética y legal de principio a fin, cerrándole la puerta a cualquier conducta que comprometa los fines del Estado.

3.2.1. Soporte y Operación del SIGRIP

Para asegurar la operatividad del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), la UIAF garantiza la disponibilidad de recursos técnicos, humanos y tecnológicos especializados en inteligencia financiera. La entidad promueve atributos comportamentales basados en la reserva, la honestidad y la diligencia, integrados en su Código de Integridad. Asimismo, se implementa una estrategia de formación continua y planes de comunicación interna para sensibilizar a los servidores sobre la cultura del riesgo.

Finalmente, todas las etapas de identificación, tratamiento y monitoreo son documentadas y custodiadas, sirviendo como evidencia para los procesos de mejora y control institucional. Para dar cumplimiento a lo anterior, la entidad identifica y dispone de las siguientes capacidades:

- **Talento humano y habilidades especializadas:** equipo interdisciplinario con experiencia en ciencia de datos, derecho sancionatorio y análisis financiero predictivo, con énfasis en debida diligencia y gestión de reserva legal.
- **Soluciones de TI e infraestructura:** plataforma SIREL (Sistema de Reporte en Línea) y herramientas de analítica avanzada para el procesamiento de Big Data, bajo altos estándares de ciberseguridad.
- **Recursos financieros y organizacionales:** asignación de partidas presupuestales para el fortalecimiento de la infraestructura crítica y la suscripción a fuentes de información internacionales.

- **Material de referencia y experiencia:** capitalización de guías de tipologías, estándares del Grupo Egmont y manuales de procesos internos que documentan la experiencia histórica de la Unidad.

3.2.2. Idoneidad en la Administración del Sistema

La UIAF asegura que los servidores responsables de la Administración del Programa de Transparencia, quienes coordinan también el SIGRIP, cuenten con perfiles de idoneidad técnica alineados con sus funciones. La entidad garantiza que dicho personal acredite los requisitos de educación superior y experiencia profesional definidos en el Manual de Funciones, complementando su desempeño mediante el Plan Institucional de Capacitación en temas de integridad, ética y gestión pública.

3.2.3. Toma de Conciencia y Cultura de Integridad

La UIAF reconoce que la efectividad del SIGRIP depende del compromiso de todos los niveles de la organización. Para ello, la entidad establece como lineamiento la integración de acciones de sensibilización orientadas a la toma de conciencia en los siguientes aspectos:

- **Objetivos y alcance:** entender cómo el sistema protege la misión de la Unidad.
- **Elementos del SIGRIP:** conocer los componentes técnicos que integran la gestión del riesgo.
- **Beneficios institucionales:** valorar el sistema como una herramienta de transparencia y generación de confianza.
- **Implicaciones del incumplimiento:** claridad sobre las responsabilidades y consecuencias derivadas de no aplicar los requisitos del sistema.

Estas temáticas deberán ser incorporadas de manera progresiva en las estrategias de capacitación y comunicación interna, asegurando que la gestión del riesgo para la integridad se convierta en una práctica institucional transversal.

3.2.4. Lineamientos de Comunicación y Difusión de Resultados

La UIAF establece que la gestión de riesgos para la integridad debe ser transparente y conocida por toda la organización y sus partes interesadas. Para dar cumplimiento a este lineamiento,

la Administración del Sistema de Riesgos definirá los contenidos técnicos que deben comunicarse, integrándolos en la Acción de Comunicación del Programa de Transparencia y Ética Pública (PTEP) bajo los siguientes criterios:

- **Difusión de resultados:** se comunicarán periódicamente los avances en el tratamiento de los riesgos de integridad y los resultados del monitoreo de controles, asegurando que la Alta Dirección y los líderes de proceso cuenten con información para la toma de decisiones.
- **Actualizaciones del sistema:** cualquier modificación en la Política de Riesgos, en las metodologías de evaluación o en los elementos del SIGRIP, será informada de manera oportuna a través de los canales institucionales.
- **Reporte a Entes de Control:** los resultados consolidados y las evidencias de la operación del Sistema estarán disponibles para los organismos de control y vigilancia en los términos que la ley disponga, garantizando la transparencia institucional bajo los protocolos de reserva de la Unidad.
- **Canales y periodicidad:** la comunicación se realizará de forma semestral o anual, aprovechando los espacios de socialización definidos en la estrategia de comunicación institucional de la Unidad.

3.2.5. Gestión Documental y Control de la Información del SIGRIP

La UIAF garantiza que cada uno de los elementos y actividades que integran el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) se encuentren debidamente documentados, asegurando su trazabilidad y soporte institucional. Para ello, se establecen los siguientes lineamientos:

- **Integración al sistema de gestión:** una vez implementados, los documentos, matrices, actas y reportes del SIGRIP se incorporarán al Sistema de Gestión Institucional y a las Tablas de Retención Documental (TRD), cumpliendo con los estándares de gestión archivística de la entidad.
- **Creación y actualización:** la administración del SIGRIP será responsable de generar y actualizar la información documentada (políticas, manuales y mapas de riesgos), asegurando que reflejen la realidad operativa y los cambios en el contexto de la Unidad.

- **Clasificación y reserva de la información:** el tratamiento de los documentos del SIGRIP no será uniforme; cada producto (matriz, acta o informe) será sometido a un Índice de Información Clasificada y Reservada. La oficina responsable de la administración del riesgo, en coordinación con el Oficial de Cumplimiento o el área jurídica, determinará si el documento es Público (ej. la Política), Clasificado (datos personales) o Reservado (detalles técnicos de inteligencia financiera), aplicando las restricciones de acceso que dictan las Leyes 1712 de 2014 y 1621 de 2013.
- **Seguridad y acceso a la información:** se establecerán restricciones de acceso y protocolos de almacenamiento para que la documentación del SIGRIP esté protegida contra modificaciones no autorizadas, pérdida de datos o consultas por personal no facultado, garantizando la reserva de la inteligencia institucional.

3.2.6. Identificación y Valoración de Riesgos para la Integridad Pública

La UIAF adopta una visión de gestión integral, donde los riesgos para la integridad pública (Corrupción, LA/FT/FP) no se analizan de forma aislada, sino en conjunto con los riesgos de gestión, seguridad de la información y riesgos fiscales. El objetivo es asegurar que la entidad opere bajo un estándar ético que impida que sus instituciones sean utilizadas para dar apariencia de legalidad a activos ilícitos.

3.2.6.1. Identificación y Descripción del Riesgo

Para identificar los puntos donde la integridad de la Unidad puede verse comprometida, se aplicarán dos metodologías diferenciadas según la naturaleza del riesgo:

- **Riesgos de LA, FT y FP (Enfoque en Operaciones):** la identificación se centrará en los puntos de riesgo operativos. Estos son los momentos en el flujo de procesos donde existe un intercambio de recursos (bienes, servicios o pagos). **Criterio**: se analizará toda operación donde la entidad reciba o entregue un recurso, identificando si dicha transacción puede ser aprovechada para canalizar recursos hacia actividades delictivas o terroristas.
- **Riesgos de corrupción y sus manifestaciones (Enfoque en Actividades):** para los riesgos de soborno, fraude e inadecuada gestión del conflicto de intereses, el análisis será más amplio. **Criterio:** los puntos de riesgo no se limitan a transacciones de dinero; pueden ser cualquier

actividad dentro de un proceso. Se debe evaluar cada tarea para detectar posibles abusos de poder o decisiones direccionadas hacia beneficios particulares que afecten la transparencia.

3.2.6.2. Identificación de Áreas de Impacto y Materialización

La UIAF evaluará el impacto de los riesgos para la integridad pública considerando no solo la afectación económica, sino las dimensiones legales, reputacionales y de contagio.

Dimensiones del Impacto

- **Impacto legal:** surge ante el incumplimiento de normas o contratos, manifestándose desde que una contraparte es vinculada a procesos judiciales o administrativos.
- **Impacto por contagio:** posibilidad de afectación a la UIAF por acciones de entidades o individuos relacionados (partes interesadas), aunque no haya un vínculo directo en el evento.
- **Impacto reputacional:** ocurre cuando la Unidad se ve involucrada en denuncias o reportes que cuestionan su integridad o reserva, afectando la confianza ciudadana.
- **Impacto operativo:** situaciones donde la conducta contraria a la integridad interrumpe o degrada la calidad de los procesos de inteligencia y trámites (SIREL).

Materialización del Riesgo

Un riesgo se considera materializado cuando el evento identificado ocurre y genera un impacto negativo. En la UIAF, esto incluye:

- Afectación a la reputación, operación o cumplimiento normativo.
- Compromiso en la ejecución de los recursos públicos.
- Detección de operaciones sospechosas: En materia de LA/FT/FP, el riesgo se considera gestionable desde la tentativa, obligando al reporte inmediato sin necesidad de que se consume un delito penal.

3.2.7. Continuidad del Negocio y Respuesta Institucional

Ante la materialización de un riesgo, la respuesta de la UIAF se orientará a la Continuidad del Servicio. La Política de Riesgos debe asegurar que, a pesar del impacto, la operación normal de

la organización y sus objetivos misionales se mantengan vigentes, con independencia de las investigaciones que adelanten otras autoridades.

3.2.7.1. Factores de Riesgo y Segmentación (LA/FT/FP e Integridad)

La UIAF identifica los factores de riesgo como los elementos generadores del riesgo de Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas (LA/FT/FP). Estos factores se analizan de manera conjunta para caracterizar cada transacción u operación institucional.
Factores de riesgo mínimos: para todo análisis de riesgo en la Unidad, se considerarán al menos los siguientes cuatro factores:

- **Contrapartes:** Clientes, usuarios, proveedores o cualquier persona natural o jurídica con la que se establezca un vínculo.
- **Productos/Servicios:** bienes o servicios entregados o recibidos por la entidad.
- **Canales:** medios dispuestos por la UIAF para la realización de las operaciones (ej. plataformas digitales, SIREL, trámites presenciales).
- **Jurisdicciones:** ubicación geográfica donde se origina o ejecuta la operación.

Segmentación: la entidad aplicará la segmentación para agrupar estos factores en categorías con características similares.

- **Objetivo:** determinar los parámetros normales de comportamiento transaccional para cada grupo.
- **Señales de alerta:** cualquier operación que se salga de los límites de normalidad definidos en la segmentación será catalogada como operación inusual. Estas señales activarán el estudio por parte de la función de cumplimiento para determinar si procede un reporte a las autoridades competentes.

Obligaciones y recursos de soporte: para garantizar la efectividad de este análisis, la UIAF establece:

- **Gestión de recursos para el monitoreo:** la entidad ejecutará la debida diligencia sobre sus contrapartes y operaciones mediante el talento humano asignado a las funciones de contratación y cumplimiento. Para ello, se apoyará en las herramientas institucionales de

consulta y bases de datos disponibles, permitiendo la identificación de alertas o señales de inusualidad en los tiempos definidos por los procesos internos.

- **Indicadores:** la construcción de señales de alerta se basará en indicadores clave de riesgo que permitan detectar de manera temprana intentos de utilizar a la entidad para fines ilícitos.

3.2.8. Procedimiento de Debida Diligencia y Conocimiento de Contrapartes

El Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) exige que cada entidad implemente un documento de Debida Diligencia. Este instrumento busca identificar, analizar y evaluar los riesgos en las interacciones con contrapartes para tomar decisiones informadas y prevenir delitos como soborno, fraude, corrupción, lavado de activos y financiación del terrorismo.

Principios Rectores

- **Razonabilidad:** Los mecanismos deben ser cumplibles según los recursos de la entidad.
- **Proporcionalidad:** La intensidad de la debida diligencia dependerá del nivel de riesgo (Simplificada, Estándar o Ampliada).

Componentes del Proceso de Debida Diligencia: Para que el proceso sea efectivo, el documento debe cubrir cuatro etapas clave:

- **Preparación:** Definir objetivos, procesos y equipos responsables.
- **Recolección:** Consultar fuentes (estados financieros, listas restrictivas, visitas en sitio).
- **Análisis:** Evaluar inconsistencias frente a patrones normales del sector.
- **Informe:** Documentar hallazgos, viabilidad de la relación y medidas de mitigación.

Verificaciones Obligatorias: Se debe verificar la identidad y antecedentes de personas naturales, representantes legales, revisores fiscales y beneficiarios finales mediante:

- **Listas Nacionales:** Antecedentes penales, fiscales (SIBOR), disciplinarios (SIRI), medidas correctivas (RNMC) y deudores alimentarios (REDAM).
- **Listas Internacionales:** ONU, terroristas de EE. UU. y la Unión Europea.

- **Historial y Reputación:** Relaciones previas (2 años), programas de ética, prensa y fuentes de recursos.
- **PEPs:** Investigación profunda a Personas Expuestas Políticamente (hasta 2 años tras dejar el cargo).

Consecuencias y Toma de Decisiones: El conocimiento de la contraparte no genera inhabilidades legales automáticas, pero sí permite a la entidad tomar acciones preventivas como:

- **Ajustes contractuales:** Implementar controles adicionales o requerir aprobaciones superiores.
- **Monitoreo:** Seguimiento especial a operaciones inusuales.
- **Abstención:** En casos excepcionales, terminar o no iniciar la relación según la normativa.
- **Reporte:** Notificación obligatoria de operaciones sospechosas a la UIAF o Fiscalía.

Gestión de Información: La UIAF debe garantizar el archivo, custodia y confidencialidad de los datos personales y documentos obtenidos, aplicando la normativa vigente de tratamiento de datos.

3.2.9. Función de cumplimiento del SIGRIP

La UIAF asignará la Función de Cumplimiento a un servidor de nivel Directivo o Asesor, quien reportará directamente a la Alta Dirección. Este rol podrá ser asumido por el Administrador del Programa de Transparencia (PTEP).

Responsabilidades Clave

- **Operación:** velar por el funcionamiento del SIGRIP y apoyar a los líderes en la gestión de riesgos.
- **Reporte:** informar periódicamente a la Alta Dirección sobre resultados, operaciones inusuales y planes de mejora.
- **Debida diligencia:** definir los criterios para el conocimiento de contrapartes y el reporte de operaciones sospechosas ante las autoridades competentes.
- **Articulación:** coordinar capacitaciones internas y promover la adopción de correctivos.

Requisitos de integridad e independencia:

- **Perfil:** el responsable debe destacar por su probidad y ética, sin investigaciones vigentes y con declaraciones de bienes y conflictos de interés actualizadas.
- **Posición:** se ubicará en el segundo nivel jerárquico de la entidad para garantizar su autonomía frente a los procesos evaluados. Esta función no sustituye las facultades de Control Interno.
- **Notificación:** la identidad y contacto del responsable se informará y actualizará ante la Secretaría de Transparencia de la Presidencia.

3.2.10. Herramientas de Gestión para la Integridad Pública

La UIAF adopta un enfoque integral donde la Política de Riesgos se articula con herramientas específicas desarrolladas en el marco del Programa de Transparencia y Ética Pública (PTEP). Estas herramientas son de obligatorio cumplimiento y refuerzan la cultura de legalidad institucional.

Declaraciones de compromiso (Políticas de Prevención): la entidad formulará y mantendrá actualizadas políticas institucionales que manifiesten el compromiso de la Alta Dirección en:

- **LA/FT/FP:** prevención del lavado de activos y financiación del terrorismo y financiación de la proliferación de armas, obligando al cumplimiento normativo y a la debida diligencia de contrapartes.
- **Antisoborno y antifraude:** prohibición expresa de estas prácticas, tipificación de conductas y promoción de la denuncia segura (sin represalias) ante señales de alerta.

Procedimientos operativos de integridad: la UIAF establecerá procedimientos internos detallados para la gestión de eventos específicos:

- **Gestión de conflictos de intereses:** catálogo de situaciones reales, pasos para la declaración periódica y el trámite interno para su resolución.
- **Reporte de operaciones sospechosas:** criterios para identificar operaciones inusuales, pasos para que los líderes reporten a la Función de Cumplimiento, su posterior evaluación y el procedimiento de reporte ante la autoridad competente (incluyendo tentativas).

- **Canal institucional de denuncias y buzón ético:** medios de recepción, pasos para la evaluación técnica de denuncias por corrupción y trámite de conclusión de las mismas.

Integración institucional: todas estas herramientas, junto con el Mapa de Riesgos y el Documento de Debida Diligencia, forman parte integral del PTEP.

3.2.11. Monitoreo, Evaluación y Mejora Continua del SIGRIP

La UIAF garantiza la efectividad del SIGRIP mediante un proceso permanente de seguimiento y auditoría, estructurado bajo el modelo de líneas de defensa para asegurar la integridad de su operación.

Monitoreo (Primera línea de defensa): los líderes de proceso y sus equipos son los responsables directos del seguimiento cotidiano de los riesgos.

- **Obligación:** identificar cambios en el contexto y verificar la operatividad de los controles asignados.
- **Reporte:** generar y remitir informes trimestrales al Administrador del SIGRIP sobre el estado de la gestión de riesgos en su área.

Evaluación de la gestión (Segunda línea de defensa): corresponde al Administrador del SIGRIP (Función de cumplimiento) realizar la evaluación objetiva del sistema.

- **Alcance:** medir el cumplimiento de los objetivos del sistema mediante indicadores de gestión y el análisis de los reportes de la primera línea.
- **Periodicidad:** se realizará una evaluación consolidada anual que será presentada a la Alta Dirección, incluyendo resultados de debida diligencia y efectividad de controles.

Auditoría independiente (Tercera línea de defensa): la Oficina de Control Interno e Inspección realizará auditorías periódicas al SIGRIP con un enfoque basado en riesgos.

- **Objetivo:** determinar de forma independiente la conformidad y eficacia del sistema y sus controles individuales.

- **Criterios:** la auditoría se ejecutará conforme al Plan Anual de Auditoría, generando hallazgos que alimenten los planes de mejoramiento institucional.

Mejora continua (Línea estratégica): la Alta Dirección es la responsable de la revisión integral del SIGRIP para asegurar su evolución.

- **Acciones:** basándose en los insumos del monitoreo, la evaluación y la auditoría, la dirección ordenará los ajustes necesarios a la Política de Riesgos.
- **Compromiso:** implementar planes de mejoramiento para subsanar no conformidades y fortalecer preventivamente el sistema ante nuevas amenazas a la integridad.

Nivel de aceptación: se determinan como resultado de la valoración de la probabilidad de ocurrencia del riesgo y de la magnitud del impacto al momento de evaluar su materialización.

Los riesgos de gestión inherentes ubicados en la zona de riesgos baja pueden ser aceptados, por tal razón, no es necesario establecer controles.

Los riesgos de corrupción son los únicos que son inaceptables en todo sentido, por tanto, deben tener controles permanentes de seguimiento.

Ilustración 35. Nivel de aceptación del riesgo

Tipos de Riesgo	Zona de Riesgo Residual	Estrategia de tratamiento
	Baja	Seguimiento SEMESTRAL
	Moderada	Seguimiento TRIMESTRAL
	Alta	Seguimiento MENSUAL
	Extrema	Seguimiento MENSUAL

Fuente: OAP

Tratamiento del riesgo: es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

Ilustración 36. Tratamiento del riesgo

Tipos de Riesgo	Zona de Riesgo Residual	Tratamiento	Estrategia de tratamiento
	Baja	Se aceptan	Seguimiento SEMESTRAL
	Moderada	Se mitigan	Seguimiento TRIMESTRAL
	Alta	Se mitigan	Seguimiento MENSUAL
	Extrema	Se mitigan	Seguimiento MENSUAL

Fuente: OAP

4. SEGUIMIENTO, MONITOREO Y REVISIÓN EN EL MARCO DEL ESQUEMA DE LÍNEAS DEL MODELO ESTÁNDAR DE CONTROL INTERNO MECI

La UIAF articula el seguimiento de sus riesgos con la Dimensión 7 del MIPG, asignando niveles de autoridad y responsabilidad en la aplicación de controles. Para garantizar que la gestión del riesgo sea una herramienta estratégica y no solo operativa, se establecen mecanismos de medición basados en indicadores que permiten validar el cumplimiento de metas y detectar desviaciones en la integridad institucional.

Tipologías de indicadores para el seguimiento: la entidad define dos categorías de indicadores para monitorear la salud del sistema de gestión de riesgos:

Tabla 21. Tipología de indicadores

	Propósito	Aplicación
Indicadores Clave de Desempeño (KPI - Key Performance Indicators)	Miden el cumplimiento de los objetivos estratégicos, procesos y proyectos misionales de la UIAF.	Permiten verificar si la planeación institucional se está ejecutando según lo previsto y facilitan la introducción de ajustes a los planes de acción.
Indicadores Clave de Riesgo (KRI - Key Risk Indicators)	Funcionan como señales de alerta temprana que indican cambios en el perfil de riesgo o la posible materialización de una amenaza.	Son la base para la toma de decisiones informadas de la Alta Dirección, permitiendo actuar antes de que un riesgo afecte la misión o la reputación de la Unidad.

Fuente: OAP

Articulación con la plataforma estratégica: el diseño de estos indicadores no es aislado; parte de la Misión, Visión y Valores de la UIAF. Los KPI miden "qué tanto estamos logrando", mientras que los KRI miden "qué tanto peligro corremos de no lograrlo".

Esta estructura asegura que el monitoreo realizado por la Primera Línea (Líderes de Proceso) y la evaluación de la Segunda Línea (Administrador del SIGRIP) cuente con datos objetivos para establecer la efectividad de los controles y asegurar la continuidad del servicio.

4.1. Alcance de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI)

La gestión estratégica moderna exige una visión dual que equilibre la ejecución con la seguridad operativa. En este contexto, la articulación entre los KPI y los KRI es fundamental: mientras los primeros se centran en la eficacia y la consecución de logros, los segundos actúan como radares que detectan amenazas potenciales. Aunque operan bajo lógicas distintas, su integración permite una toma de decisiones informada, combinando la medición del éxito con la capacidad de anticipación ante la incertidumbre.

A continuación, se resumen sus principales alcances y diferencias:

Tabla 22. Alcance de indicadores

Característica	KPI (Desempeño)	KRI (Riesgo)
Misión	Medir el avance hacia las metas establecidas.	Detectar señales tempranas de exposición al riesgo.
Perspectiva	Histórica: evalúa resultados de programas y proyectos.	Predictiva: identifica eventos que podrían impactar el futuro.
Gestión	Optimiza recursos y mejora la planificación operativa.	Mitiga impactos y facilita el escalamiento de alertas.
Resultado	Determina qué tan bien se están logrando los objetivos.	Determina qué tan probable es que un riesgo nos afecte.

Fuente: OAP

4.2. Lineamientos generales para el establecimiento de Indicadores Clave de Riesgo (KRI)

Dada la naturaleza misional de la UIAF, la entidad opera bajo una premisa de apetito de riesgo nulo. Esto implica que los KRI no se diseñan para gestionar niveles de aceptación, sino para

garantizar la integridad absoluta de los procesos de inteligencia financiera. Cualquier desviación captada por un KRI se considera una vulnerabilidad crítica que requiere intervención inmediata.

4.2.1. Interpretación de los KRI frente a la Tolerancia Cero

Bajo el modelo de la UIAF, la relación entre el cálculo del indicador y el control institucional se rige por la detección temprana de tendencias negativas:

- **Valor dentro de la normalidad:** indica que la operación se mantiene estrictamente bajo los parámetros legales y de seguridad definidos.
- **Aproximación al umbral de alerta:** se interpreta como una señal de advertencia técnica. Revela que el riesgo está aumentando y podría materializarse si no se corrigen las causas raíz de inmediato.
- **Exceso del umbral:** representa el incumplimiento del mandato institucional. Al no haber apetito de riesgo, cualquier valor que supere el umbral exige acciones correctivas urgentes y el escalamiento al Comité Institucional de Coordinación de Control Interno para retornar a la zona de seguridad.

4.2.2. Requisitos para la Construcción de KRI en la UIAF

Para asegurar que los indicadores sean efectivos en un entorno de alta sensibilidad, su construcción debe seguir estos lineamientos:

- **Identificación de amenazas:** se deben mapear riesgos mediante el análisis de causas raíz y bases históricas de eventos (Mesas de ayuda, PQRD, Oficina Jurídica, Líneas de denuncia). Si ocurre un incidente no identificado previamente, este debe integrarse de forma prioritaria al sistema.
- **Ficha técnica del indicador:** todo KRI debe estar formalizado con: Nombre, descripción, fórmula, fuente confiable (bases de datos o auditorías), frecuencia de monitoreo y los umbrales de alerta aprobados por la Alta Dirección.

- **Responsabilidad y supervisión:** se deben designar responsables para el cálculo y reporte, asegurando que la información sea veraz para una toma de decisiones con certeza y confiabilidad.

Ejemplos de aplicación por procesos: con el fin de operacionalizar los lineamientos anteriores, se presentan a continuación ejemplos de cómo se estructuran los KRI en diferentes áreas, relacionando el proceso, el indicador y su métrica de control:

Tabla 23. Ejemplo de indicadores y su aplicación por procesos

Proceso Asociado	Indicador Clave de Riesgo (KRI)	Métrica de Medición
Tecnologías de la Información (TIC)	Tiempo de interrupción de aplicativos críticos en el mes.	Número de horas de indisponibilidad de aplicativos críticos.
Gestión Financiera	Reportes emitidos al regulador fuera del tiempo establecido.	Número de reportes mensuales remitidos fuera de términos.
Atención al Usuario	Reclamos por incumplimiento a términos de ley o reiteraciones.	% de solicitudes mensuales fuera de términos / % solicitudes reiteradas.
Administrativo y Financiera	Errores en transacciones y su impacto en la gestión presupuestal.	Volumen de transacciones al mes sobre la capacidad disponible.
Talento Humano	Rotación de personal crítico.	% de nuevos empleados que abandonan el puesto en los primeros 6 meses.

Fuente: OAP

Responsables y reporte: para asegurar la efectividad de estos indicadores, la entidad define responsables específicos encargados de:

- **Cálculo y monitoreo:** líderes de proceso y sus equipos técnicos.
- **Evaluación y reporte:** los resultados deben ser presentados ante la Alta Dirección y el Comité Institucional de Coordinación de Control Interno, garantizando que cualquier desviación del umbral de "apetito nulo" active de inmediato planes de contingencia.

Atributos y limitaciones estratégicas: para que el KRI sea una herramienta de inteligencia preventiva, debe cumplir con:

- **Capacidad predictiva:** debe anticipar el problema antes de que afecte la misión de la entidad.

- **Confiabilidad de la fuente:** si los datos están desactualizados o son errados, el KRI pierde su efectividad, aumentando la exposición al riesgo.
- **Complementariedad:** el KRI no sustituye el análisis de contexto; se requiere conocimiento profundo del entorno de inteligencia financiera para interpretar sus resultados.

4.2.3. Comunicación y Reporte de KRI en el Marco del Esquema de Líneas de Aseguramiento

En concordancia con el Esquema de Líneas de Aseguramiento (Dimensión 7 de MIPG), la gestión de los KRI requiere un trabajo conjunto para generar alertas tempranas que fortalezcan la prevención. Dado que la UIAF opera con un apetito de riesgo nulo, este esquema garantiza que cada nivel de la entidad contribuya a evitar la materialización de amenazas. A continuación, se detalla la asignación de roles y responsabilidades.

4.2.4. Consideraciones Finales para la Implementación

- **Sinergia KPI-KRI:** el Comité de Gestión y Desempeño Institucional debe realizar el análisis articulado de ambas métricas. El éxito del desempeño (KPI) es directamente proporcional a la gestión efectiva de las alertas de riesgo (KRI).
- **Cultura de reporte:** al ser una entidad de inteligencia, la veracidad y oportunidad de los datos reportados en el sistema institucional son la base para que la Alta Dirección tome decisiones con certeza y confiabilidad.
- **Acción preventiva:** si un KRI identifica una tendencia fuera de lo esperado, la 1ª línea tiene la obligación de intervenir preventivamente, sin esperar a que el riesgo se materialice.

5. HISTORIAL DE CAMBIOS DEL DOCUMENTO

Versión	Motivo del Cambio	Descripción del Cambio	Fecha del Cambio
1	Versión inicial	Elaboración del Anexo Metodología para la Gestión Integral de Riesgos Unidad de Información y Análisis Financiero – UIAF.	20 de marzo de 2026