Política

Administración del riesgo

Unidad de Proyección Normativa y Estudios de Regulación Financiera

Contenido

1. Declaración de la política 6
2. Objetivos 6
2.1. Objetivo general 6
2.2. Objetivos específicos 7
3. Ámbito de aplicación 7
4. Términos y definiciones 8
5. Roles y responsabilidades 15
6. Metodología para la administración del riesgo 21
6.1. Contexto estratégico 22
6.2. Etapa de identificación 23
6.2.1. Nombre del riesgo 25
6.2.2. Descripción del riesgo 25
6.2.3. Aspectos y orientaciones para la descripción de los riesgos fiscales 26
6.2.4. Responsables del riesgo identificado 27
6.2.5. Factores generadores de riesgo 27
6.2.6. Causas 34
6.2.7. Clasificación de las causas 34
6.2.8. Consecuencias 34
6.2.9. Asociación estratégica, organizacional y por proceso 34
6.2.10. Incidencia jurídica del riesgo 35
6.2.11. Fuentes de identificación del riesgo 35
6.2.12. Tipos de riesgo 36
6.2.13. Productos y/o servicios que pueden afectarse con la materialización del riesgo 37
6.2.14. Recursos necesarios para la gestión del riesgo 37
6.2.15. Incidencia directa en el usuario externo 38
6.2.16. Aspectos validadores de los riesgos para la integridad pública 38
6.3. Etapa de análisis 39
6.3.1. Clasificación del riesgo 39
6.3.2. Evaluación del riesgo 41
6.4. Etapa de valoración de riesgos 43
6.4.1. Descripción cualitativa de controles 43
6.4.2. Evaluar los controles 48
6.5. Etapa de manejo de los riesgos 52
6.5.1. Determinación de la opción de manejo 52
6.5.2. Definición de acciones de contingencia 53
6.5.3. Apetito del riesgo 53
6.5.4. Definición del semáforo del riesgo 55
6.5.5. Acciones para el manejo de los riesgos 55
6.6. Etapa de monitoreo de los riesgos 56
6.7. Creación, modificación o eliminación de riesgos 58
6.8. Mapa de riesgos 59

7. Alineación con los valores del manual de integridad y buen gobierno.... 60
8. Comunicación 61
9. Mecanismo de monitoreo, control y evaluación 61
10. Documento referente 61
11. Datos de elaboración y control de cambios..... 61
12. Anexo 5. Riesgos de seguridad de la información digital 66

Tabla de ilustraciones

Ilustración 1. Ubicación de videotutoriales en el SMGI 4
Ilustración 2. Aspectos importantes sobre el alcance de la política 8
Ilustración 3. Roles y responsabilidades frente a la administración del riesgo ... 15
Ilustración 4. Etapas para la administración del riesgo 21
Ilustración 5. Aspectos importantes sobre el desarrollo conceptual y metodológico – Operación de la política 22
Ilustración 6. Resultados del Contexto Estratégico 23
Ilustración 7. Orientaciones para validar la adecuada definición del nombre del riesgo 25
Ilustración 8. Descripción de los riesgos de tipo fiscal 27
Ilustración 9. Escala de calificación para la probabilidad 40
Ilustración 10. Escala de calificación para el impacto 40
Ilustración 11. Impacto inherente del riesgo fiscal 41
Ilustración 12. Matriz de evaluación del riesgo 42
Ilustración 13. Zonas de riesgo 42
Ilustración 14. Resultados de la etapa de análisis 42
Ilustración 15. Aspectos mínimos para formulación y descripción de los controles 43
Ilustración 16. Aspectos importantes en la identificación de controles 46
Ilustración 17. Clases de controles 47
Ilustración 18. Escala afectada según el tipo de control 47
Ilustración 19. Cálculo para la evaluación del riesgo residual 51
Ilustración 20. Resultados de la etapa de valoración 52
Ilustración 21. Conceptos relacionados con el apetito del riego 54
Ilustración 22. Resultados de la etapa de manejo 56
Ilustración 23. Roles para el monitoreo y evaluación de los riesgos 57
Ilustración 24. Resultados de la etapa de monitoreo 57
Ilustración 25. Aval de solicitudes de creación, modificación o eliminación de riesgos 59

Anexos

Los siguientes anexos se encuentran disponibles en video tutoriales que se pueden consultar por el enlace asociado o mediante la opción de tutoriales disponible en la página principal del SMGI.

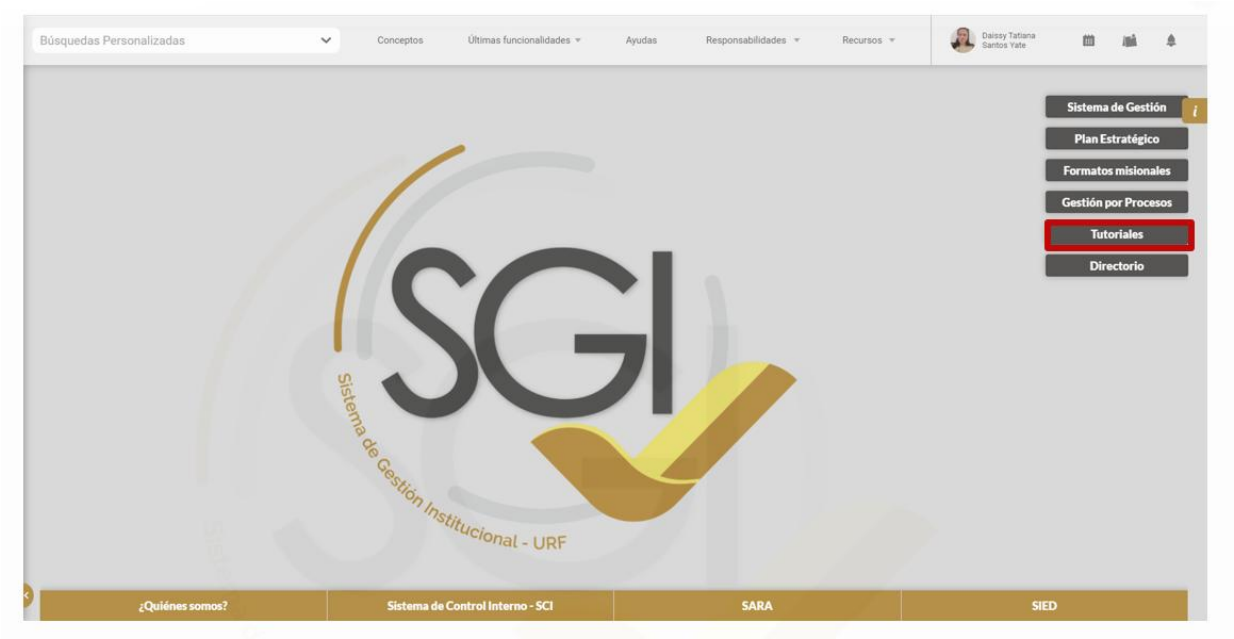


Ilustración 1. Ubicación de videotutoriales en el SMGI

- **Anexo 1.** Instrucciones para diligenciar las etapas de gestión del riesgo en el Sistema de Monitoreo de la Gestión Institucional – SMGI.
- **Anexo 2.** Instrucciones para diligenciar el reporte del monitoreo en el Sistema de Monitoreo de la Gestión Institucional – SMGI.
- **Anexo 3.** Instrucciones para el reporte de materialización de riesgos en el Sistema de Monitoreo de la Gestión Institucional – SMGI.
- **Anexo 4.** Instrucciones para solicitar la devolución de una etapa del riesgo en el Sistema de Monitoreo de la Gestión Institucional – SMGI.

La presente versión de la política de administración del riesgo de la Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF, fue puesta en consideración del Comité Institucional de Coordinación de Control Interno, en la sesión del 20 de abril de 2026, de acuerdo con lo establecido en el literal g) del artículo 2.2.21.1.6 del Decreto 648 de 2017 y del artículo cuarto de la Resolución No. 016 de 2021; surtido este paso y con el aval del Comité, fue aprobada por la Representante Legal de la Unidad, Diana Larisa Caruso López, Directora General encargada de la URF.

1. Declaración de la política

Mediante la expedición del Decreto 1499 de 2017, se estableció el Sistema de Gestión y su marco operativo de referencia; el Modelo Integrado de Planeación y Gestión. En este modelo, uno de los elementos transversales es la administración del riesgo, el cual define un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso, de tal forma que permita a las Unidades minimizar pérdidas y maximizar oportunidades.

La UAE - Unidad de Proyección Normativa y Estudios de Regulación Financiera - URF, entendiendo la importancia de una adecuada gestión de los eventos que tendrán impactos sobre los objetivos institucionales, se ha comprometido con la implementación de los procesos para el adecuado tratamiento, manejo, y seguimiento a los riesgos, buscando fortalecer la gestión institucional.

De acuerdo con lo anterior, la política que se desarrolla en este documento establece los elementos para realizar una adecuada administración de riesgos, favoreciendo la mejora continua y la toma de decisiones.

2. Objetivos

2.1. Objetivo general

Establecer los lineamientos estratégicos y operativos que orienten la identificación, análisis, valoración, manejo, monitoreo y comunicación de los riesgos en la Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF, mediante la definición y aplicación de parámetros de referencia conceptuales y metodológicos coherentes con el Modelo Integrado de Planeación y Gestión (MIPG) y las mejores prácticas internacionales de gestión del riesgo, incluyendo el marco COSO-ERM, con el fin de fortalecer la toma de decisiones informadas, anticipar eventos que puedan afectar el cumplimiento del objeto institucional y asegurar una gestión pública íntegra, eficiente, transparente y orientada a resultados.

Asimismo, esta política busca promover una cultura organizacional basada en la integridad, la prevención y la responsabilidad, fortalecer la gobernanza institucional y contribuir a la generación de valor público y a la confianza ciudadana mediante una gestión proactiva y sistemática de los riesgos que puedan afectar la misión de la entidad.

2.2. Objetivos específicos

- Establecer la metodología que permita la adecuada administración de riesgos en la URF.

- Establecer roles y responsabilidades frente a la administración del riesgo que comprometan a todos los servidores de la Unidad, con su adecuado tratamiento y prevención.

- Establecer, a partir de la administración de riesgos, una base confiable para la toma de decisiones en la gestión institucional.

- Socializar en todos los niveles de la Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF, la política de administración del riesgo y concientizar sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión institucional.

3. Ámbito de aplicación

La Política de Administración del Riesgo aplica a todos los procesos, procedimientos y actividades que desarrolla la Unidad para el cumplimiento de su misión y de los objetivos institucionales. Su implementación es obligatoria para todos los servidores, contratistas y equipos de trabajo; quienes deberán incorporar sus lineamientos en la planeación, ejecución, seguimiento y mejora de la gestión.

Asimismo, la política establece la metodología institucional para la identificación, análisis, valoración, tratamiento, monitoreo y comunicación de los siguientes tipos de riesgo:

- Riesgo estratégico
- Riesgos generales de la gestión
- Riesgos para la integridad pública
- Riesgo fiscal
- Riesgos de seguridad de la información digital
- Riesgos ambientales
- Riesgos de seguridad y salud en el trabajo

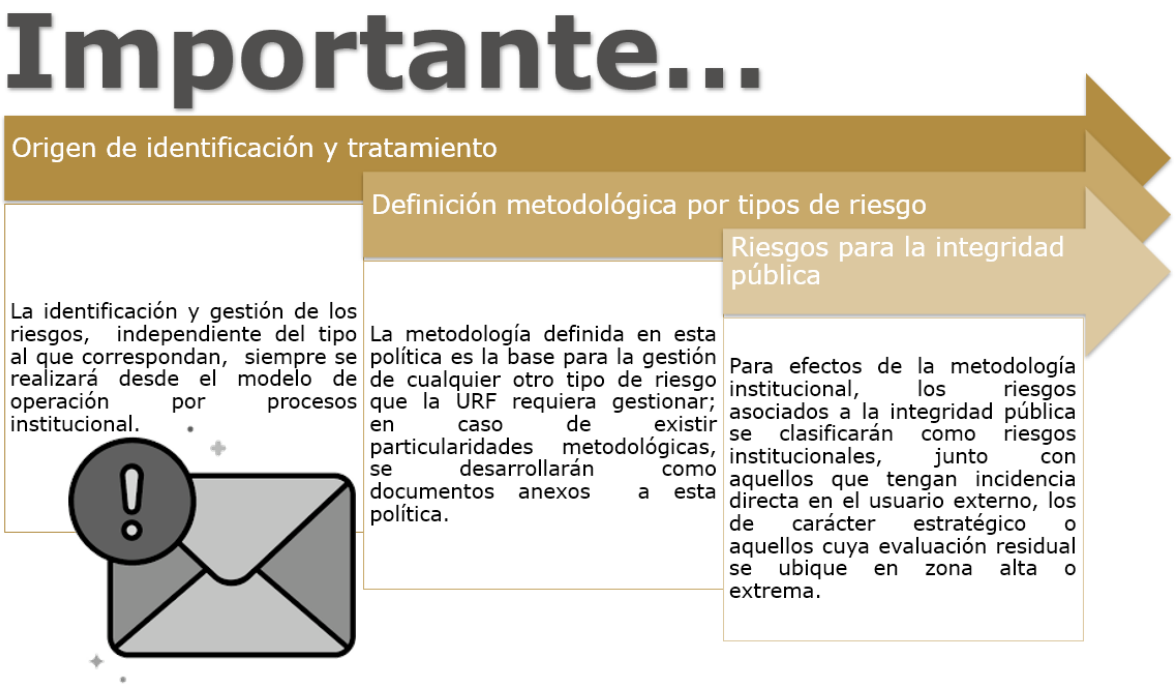


Ilustración 2. Aspectos importantes sobre el alcance de la política

4. Términos y definiciones

Para la implementación y operación de la política de administración del riesgo de la URF, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** son las que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar, compartir), en la etapa de manejo, están orientadas a fortalecer los controles identificados. Es requisito formular acciones cuando se han identificado fallas en los controles después de realizar su calificación en la etapa de valoración.

- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

- **Amenaza:** situación externa que no controla la Unidad y que puede afectar su operación.

- **Análisis del riesgo:** etapa de administración de los riesgos donde se establece la probabilidad de ocurrencia y el impacto del riesgo, antes de determinar los controles (análisis del riesgo inherente), y posterior a la definición de controles para prevenir la ocurrencia del riesgo (análisis del riesgo residual).

- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **Causa:** medios, circunstancias y/o agentes que generan riesgos.

- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata).

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **Compartir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsorcing, seguros, sitios alternos. Los riesgos para la integridad pública se pueden compartir, pero no se puede transferir su responsabilidad.

- **Conflicto de interés:** Se presenta cuando el interés general, propio de la función pública, entra en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011)

- **Consecuencia:** son los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la Unidad, sus grupos de valor y demás partes interesadas. Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.

- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia y/o el impacto del riesgo.

- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo; estos controles tienen costos implícitos.

- **Control detectivo:** control accionado durante la ejecución del proceso; estos controles detectan el riesgo, pero generan reprocesos.

- **Control preventivo:** control 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.

- **Contingencia:** acciones inmediatas identificadas para hacer frente a la materialización del riesgo.

- **Corrupción:** uso del poder para desviar la gestión de lo público hacia el beneficio privado.

- **Debilidad:** situación interna que la Unidad puede controlar y que puede afectar su operación.

- **Evaluación del riesgo:** resultado del cruce cuantitativo de la calificación de impacto y probabilidad, para establecer la zona donde se ubicará el riesgo.

- **Evitar el riesgo:** opción de manejo donde se deben determinar acciones para continuar disminuyendo tanto probabilidad como el impacto, mediante el fortalecimiento de controles, optimización de procesos y el diseño de nuevos controles.

- **Fraude:** errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025)

- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

- **Gestión del riesgo:** proceso efectuado por la alta dirección y por todos los servidores públicos y contratistas para proporcionar un aseguramiento razonable con respecto al logro de los objetivos.

- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que administran o manejan recursos o fondos públicos, desarrollando actividades económicas, jurídicas o tecnológicas orientadas a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos. Asimismo, comprende a quienes realizan la recaudación, manejo e inversión de las rentas públicas, en cumplimiento de los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que la modifique o sustituya). **Ejemplo**: entre otros, representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

- **Identificación del riesgo:** etapa de administración del riesgo donde se definen los riesgos con sus causas, agentes generadores asociados a las causas, consecuencias, definición de productos y/o servicios que pueden afectarse con la materialización del riesgo, situaciones de deño antijurídico y clasificación.

- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- **Mapa de riesgos:** organización sistemática que muestra el desarrollo de las etapas de la administración del riesgo.

- **Materialización del riesgo:** ocurrencia del riesgo identificado; cuando un riesgo se materializa, se debe registrar el reporte de materialización en el SMGI. En los casos de materialización de los riesgos para la integridad pública, se debe notificar a las autoridades competentes sobre los hechos presentados.

- **Monitorear:** observar, analizar, verificar y evaluar los riesgos identificados, determinando el adecuado desarrollo de cada una de las etapas de administración y el nivel de cumplimiento y efectividad de los controles y acciones definidas.

- **Observaciones o desviaciones del control:** acciones que deben tomarse, una vez se aplica el control y se evidencia algún incumplimiento en el proceso controlado; la actividad no debería continuarse hasta que se subsane la situación; si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Ej. El sistema SAP, cada vez que se va realizar un pago, valida que el proveedor

al cual se le va girar el pago, no está reportado en listas restrictivas, comparando el número de identificación tributaria (NIT) o cédula, con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo. En caso de encontrar coincidencias, el sistema no permite realizar el pago.

- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar o compartir el riesgo residual).

- **Política de administración del riesgo:** conjunto de lineamientos, directrices definidas y adoptadas para la gestión del riesgo en la Unidad. La política es la declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Proceso:** conjunto de operaciones secuenciales que realiza permanentemente la Unidad para generar productos/servicios a sus usuarios internos y externos a partir de unos insumos determinados.

- **Producto y/o servicio:** cualquier bien material o servicio final que se genera con la operación de un proceso institucional, orientado a satisfacer la necesidad de un grupo de valor interno o externo.

- **Punto de Riesgo**: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

- **Recurso público:** Para efectos de los riesgos fiscales, se entenderá como recurso público los dineros comprometidos y ejecutados en el ejercicio de la función pública.

- **Reducir el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados.

- **Riesgo:** evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

- **Riesgo de gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos de los procesos o sobre su operación.

- **Riesgo inherente:** es aquel al que se enfrenta una Unidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo institucional:** son los riesgos que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen alguna de las siguientes características:

  - Los clasificados con tipo estratégico.
  - Los riesgos que después de la evaluación residual se ubican en zona alta o extrema.
  - Los riesgos que tengan incidencia directa en el usuario o destinatario final externo.
  - Los riesgos para la integridad pública.

- **Riesgo para la integridad**: Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de la Unidad que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar controles para su administración.

- **Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP:** esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad

pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos.

- **SMGI:** Sistema de Monitoreo de la Gestión Institucional – SMGI; Herramienta oficial para la documentación y administración de los riesgos mediante el módulo de "Gestión del riesgo".

- **Soborno:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar. (A partir de ISO37001:2025)

- **Soborno entrante:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la Unidad.

- **Soborno saliente:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la Unidad.

- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir y si es necesario, las acciones a desarrollar para el fortalecimiento de controles.

5. Roles y responsabilidades

El éxito en la administración del riesgo depende de la decidida participación de los directivos y servidores públicos; por esta razón, es preciso identificar los actores que intervienen, de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión, a partir de la estructuración de las líneas de defensa:

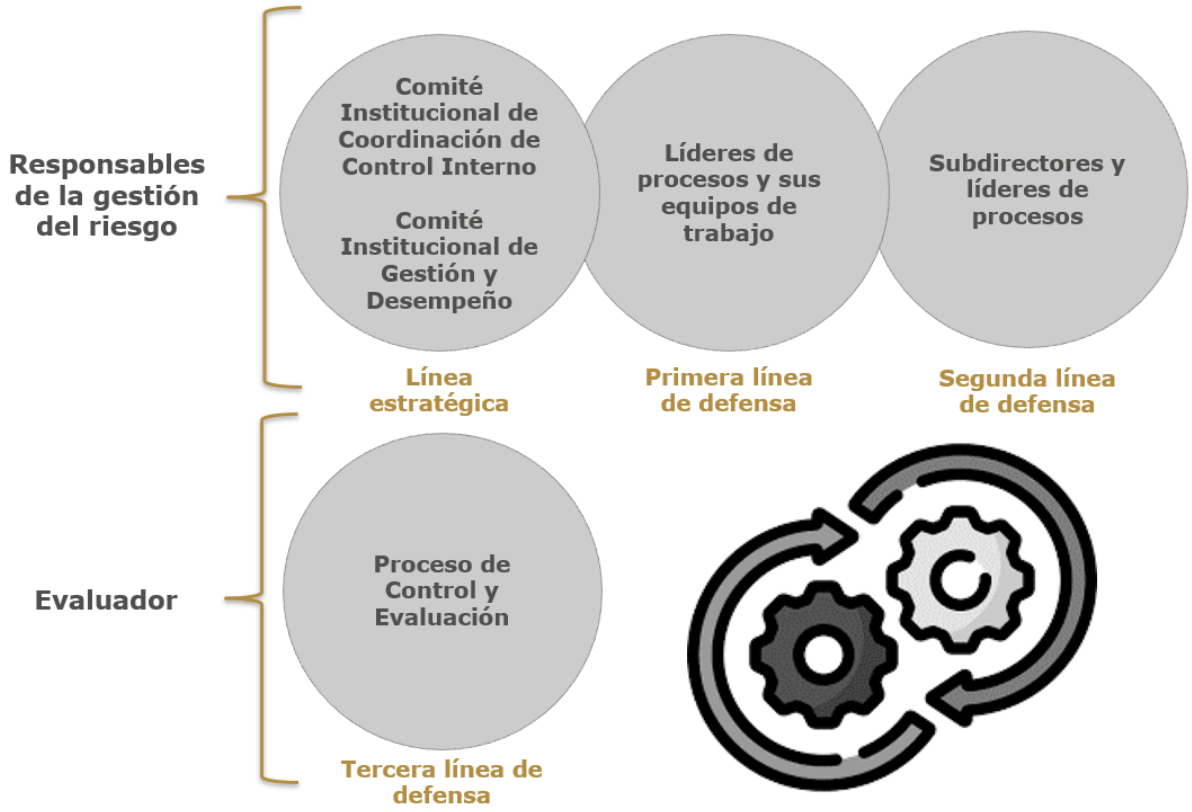


Ilustración 3. Roles y responsabilidades frente a la administración del riesgo

Línea de defensa	Responsabilidades	Integrantes
Línea estratégica	• Aprobar la política de administración del y evaluar su aplicación. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. • Retroalimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo.	Comité Institucional de Coordinación de Control Interno
	• Asegurar la implementación y articulación de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo en diferentes ámbitos institucionales. • Generar recomendaciones de mejora a la política de administración del riesgo para su inclusión y aprobación en el Comité Institucional de Coordinación de Control Interno. • Realizar seguimiento y análisis periódico a los riesgos institucionales y proponer mejoras a su estructura.	Comité Institucional de Gestión y Desempeño

Línea de defensa	Responsabilidades	Integrantes
Primera línea de defensa	• Identificar, analizar, evaluar y valorar los diferentes tipos de riesgos en la Unidad con sus equipos de trabajo y actualizarlos cuando se requiera. • Cada líder debe asegurar que, en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que esta información y lineamientos llegue a cada servidor público de su equipo de trabajo. • Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la Unidad y proponer mejoras a la gestión del riesgo en su proceso y reportar en el Sistema de Monitoreo de la Gestión Institucional los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Los líderes de proceso y coordinadores deben supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Informar al proceso de Direccionamiento y Planeación sobre los riesgos materializados en los procesos. En caso de la materialización de un riesgo no identificado, este debe ser incluido en el mapa de riesgo del proceso correspondiente.	Líderes de procesos y equipos de trabajo (Servidores públicos)

Línea de defensa	Responsabilidades	Integrantes
	• Establecer y aplicar las acciones de mejora requeridas frente al mapa de riesgos correspondiente, una vez se genera el reporte de materialización del riesgo.	
Segunda línea de defensa	• Realizar una evaluación continua de las actividades de control ejecutadas por la primera línea de defensa. Esto implica que las funciones de la segunda línea de defensa incluyen mantener informada a la Alta Dirección (con la posibilidad de que algunos integrantes formen parte de ella) y generar información clave para la toma de decisiones, en tiempos distintos a los utilizados por la tercera línea de defensa para sus seguimientos y evaluaciones.	Subdirectores y líderes de procesos
	• Generar la metodología para la administración del riesgo en la Unidad y la presentarla para aprobación del Comité Institucional de Coordinación de Control Interno y del Director de la Unidad. Adicionalmente, coordinar, liderar, capacitar y asesorar en su aplicación. • Asesorar a la línea estratégica en el análisis del contexto interno y externo, para una adecuada definición de la política de administración del riesgo. • Identificar cambios en el entorno (interno o externo) que afecten el apetito del riesgo en la entidad, para su análisis en el CICCI y se adelanten los ajustes que correspondan a este aparte dentro de la presente política.	Proceso de Direccionamiento y Planeación

Línea de defensa	Responsabilidades	Integrantes
	• Consolidar el mapa de riesgos institucional, con un enfoque para el análisis de los riesgos de mayor criticidad frente al logro de los objetivos y presentarlo en la última sesión ordinaria de cada vigencia del Comité Institucional de Gestión y Desempeño para su análisis y toma de decisiones correspondiente. • Informar a la 1ª línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado para que sea identificado e incluido en el mapa de riesgo del proceso correspondiente. • Verificar el cumplimiento normativo en materia de integridad pública, supervisar la gestión de los riesgos de integridad, apoyar la evaluación de efectividad de los controles y emitir recomendaciones a la alta dirección. Para este tema, el proceso de Direccionamiento y Planeación debe contar con independencia técnica y acceso a la información necesaria para el ejercicio de esta función de cumplimiento.	
Segunda línea de defensa	• Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de la Información en la Unidad. • Asesorar a los líderes de proceso en la identificación de los riegos de seguridad de la información digital. • Supervisar la respuesta a incidentes sobre violaciones de la seguridad, informando a la Línea Estratégica sobre sus consecuencias y acciones implementadas. • Generar informes semestrales sobre fugas de información y los medios externos identificados.	Proceso de Gestión de la Información - Oficial de seguridad de la información

Línea de defensa	Responsabilidades	Integrantes
	• Proponer a la Línea estratégica medidas y mecanismos para mejorar la gestión de seguridad de la información.	
Segunda línea de defensa	• Es responsable de administrar y manejar los recursos públicos garantizando su uso adecuado; identificar, analizar y valorar los riesgos fiscales; implementar y fortalecer controles preventivos; custodiar bienes y rentas públicas; reportar información de manera oportuna y transparente; apoyar el control fiscal interno; y actuar con integridad para prevenir cualquier daño patrimonial al Estado.	Gestor Financiero
Tercera línea de defensa Proceso de Control y Evaluación	• Llevar a cabo la evaluación independiente de los riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional de Coordinación de Control Interno. • Generar recomendaciones y/o alertas con alcance preventivo a la línea estratégica, a fin de incorporar acciones inmediatas a los temas críticos identificados. • Asesorar y acompañar a toda la Alta Dirección en la incorporación de estrategias y metodologías para la gestión de riesgo, acorde con las actualizaciones en materia de riesgos para la integridad pública, fiscales y otros que se definan en normas nacionales. En cumplimiento del principio de la independencia, los servidores públicos del proceso de Control y Evaluación no participan en la gestión institucional,	Proceso control y evaluación

Línea de defensa	Responsabilidades	Integrantes
	mediante autorizaciones o refrendaciones.	

6. Metodología para la administración del riesgo

La metodología que se presenta a continuación es integral y aplica para cualquier tipo de riesgo que la Unidad deba gestionar; sin embargo, cuando se identifiquen particularidades metodológicas para la administración de algún tipo de riesgo, es indispensable que previamente se realice el desarrollo técnico y metodológico correspondiente y se formalice mediante anexo a la presente política.

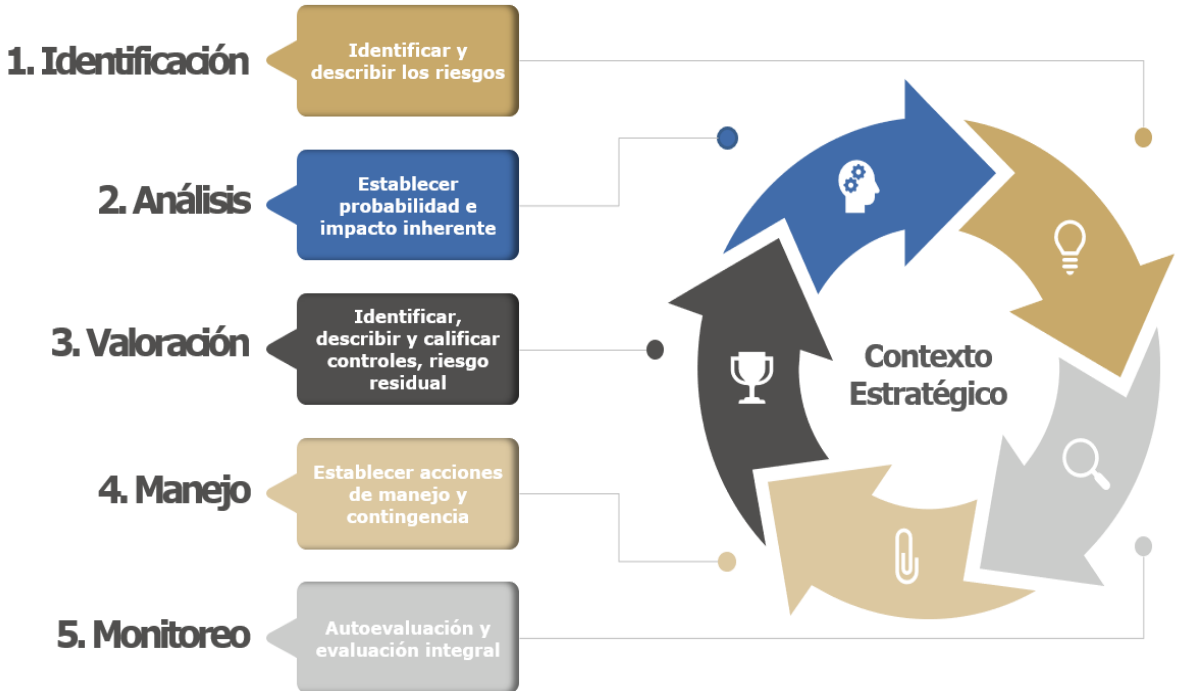


Ilustración 4. Etapas para la administración del riesgo

Ilustración 5. Aspectos importantes sobre el desarrollo conceptual y metodológico – Operación de la política

6.1. Contexto estratégico

Hace referencia a las condiciones internas y del entorno, que pueden generar oportunidades o afectar negativamente el cumplimiento de la misión y objetivos de la Unidad. Definir el contexto estratégico contribuye al control de la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgo y actuar oportunamente para su prevención o mitigación.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo.

Por lo tanto, el diseño del contexto se fundamenta en la identificación de los agentes internos (debilidades) y/ o externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

El Contexto es la base para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones del entorno de la Unidad, tanto de carácter social, económico, cultural, de orden público, político, legal y/o cambios tecnológicos, entre otros.

El análisis del contexto estratégico de la Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF se revisará, como máximo, cada cuatro años, teniendo en cuenta los cambios de gobierno. Este ejercicio será liderado por el proceso de Direccionamiento y Planeación y se desarrollará de manera articulada con la construcción del plan estratégico y los planes de acción. Su propósito es identificar, con la participación de los líderes de proceso y sus equipos de trabajo, los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos de gestión de los procesos y de la Entidad.

Con la identificación del contexto estratégico de la Unidad se obtiene:

Factores internos y externos , como insumo para la identificación, porque a partir de su análisis, se determinan las CAUSAS del riesgo; estos agentes se articulan en la metodología mediante la primera etapa, denominada identificación.

Ilustración 6. Resultados del Contexto Estratégico

6.2. Etapa de identificación

La identificación del riesgo en la URF debe realizarse de manera sistemática, considerando los elementos estratégicos, operativos y de valor público asociados a cada proceso. Para ello, se adoptan las siguientes orientaciones:

- **Asociar cada riesgo con los objetivos del proceso**: La identificación debe partir del análisis de los objetivos del proceso y de los eventos que puedan afectar su cumplimiento. Deben considerarse "aquellos eventos que podrían afectar de forma previsible el logro de los objetivos del proceso.

- **Analizar la estructura del proceso y sus actividades clave**: Se deben revisar las actividades esenciales del proceso, su secuencia y su interacción dentro del ciclo del proceso, identificando en qué puntos pueden presentarse fallas, interrupciones o desviaciones.

- **Considerar la cadena de valor público**: La identificación debe contemplar los atributos de los insumos, actividades, productos, resultados e impactos que conforman la cadena de valor, evaluando cómo un evento puede afectar la eficiencia, eficacia o calidad del servicio público.

- **Identificar los eventos que puedan afectar productos, servicios o resultados**: Se deben analizar los atributos técnicos, operativos y de calidad de los bienes o servicios generados por el proceso, y determinar qué eventos podrían alterarlos o impedir su entrega.

- **Analizar interdependencias entre procesos**: La identificación debe incluir los efectos que un evento puede generar en otros procesos de la entidad, especialmente cuando existe una relación directa en la cadena de valor o en la prestación del servicio.

- **Incorporar el conocimiento experto**: La identificación debe apoyarse en entrevistas, talleres y análisis con líderes de proceso y servidores expertos, quienes aportan conocimiento técnico sobre los riesgos inherentes a la operación.

- **Considerar el contexto institucional**: La identificación debe tener en cuenta la naturaleza, funciones, estructura organizacional, recursos, grupos de valor y particularidades de la URF, reconociendo que los riesgos varían según el ámbito organizacional.

Una vez identificados los riesgos, se deben establecer los siguientes aspectos:

- Nombre del riesgo
- Descripción del riesgo
- Responsables de la gestión del riesgo identificado
- Factores generadores de riesgo (Externos y/o internos)
- Causas (Raíz e inmediatas)
- Consecuencias
- Asociación estratégica, organizacional y por proceso
- Incidencia jurídica del riesgo
- Fuentes de identificación del riesgo
- Tipos de riesgo
- Productos y/o servicios que pueden afectarse con la materialización del riesgo
- Recursos necesarios para la gestión del riesgo
- Incidencia del riesgo en el usuario externo
- En los riesgos para la integridad pública, se incorporará un aspecto adicional relacionado con los validadores definidos para esta tipología.

A continuación, se detallan las orientaciones conceptuales para cada uno de los aspectos mencionados:

6.2.1. Nombre del riesgo

La identificación del nombre del riesgo no se puede realizar de manera fragmentada; debe existir una relación total entre las causas identificadas, el riesgo y las consecuencias que podrían presentarse producto de la materialización.

Adicionalmente, es importante considerar los aspectos que se presentan a continuación para validar que el nombre del riesgo haya quedado bien definido:

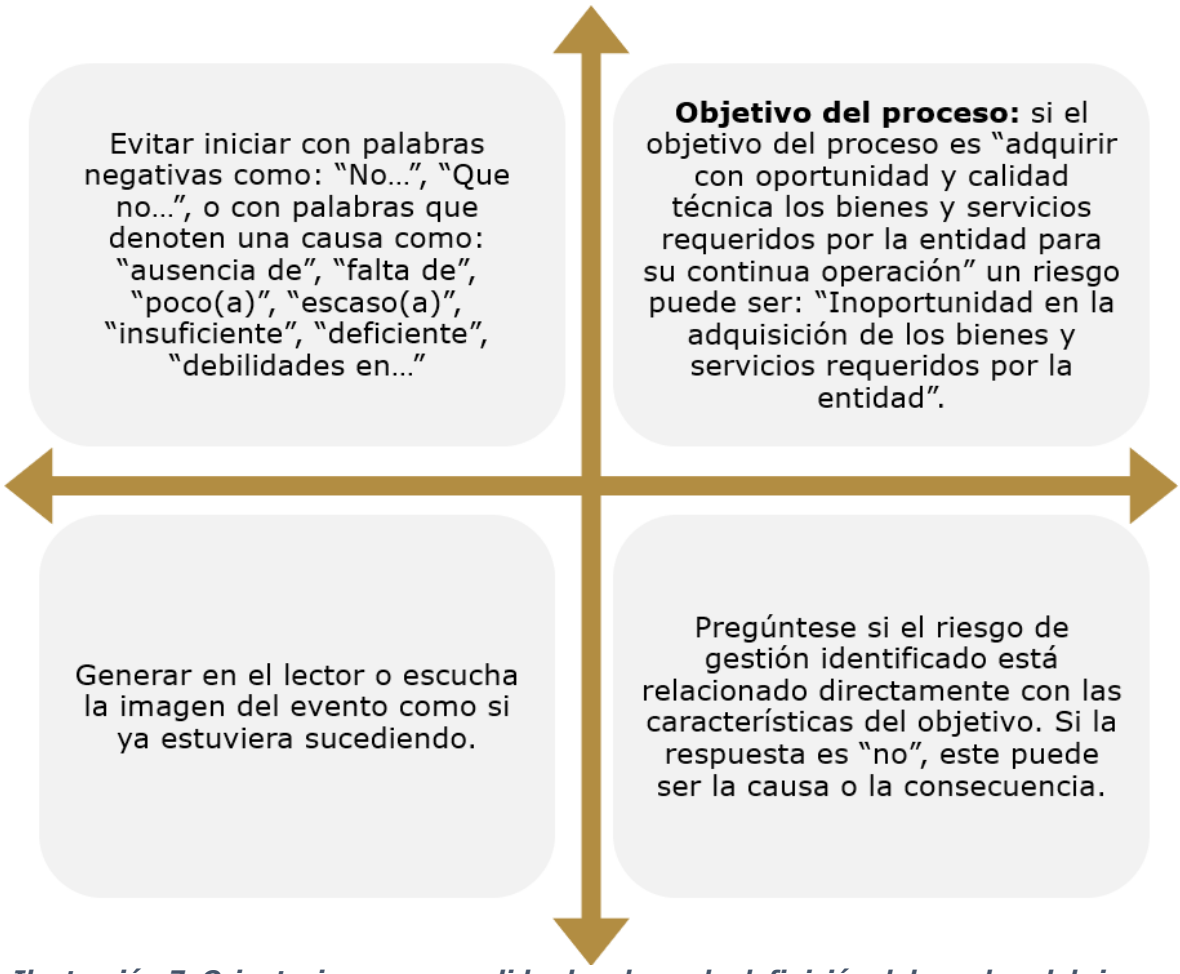


Ilustración 7. Orientaciones para validar la adecuada definición del nombre del riesgo

6.2.2. Descripción del riesgo

El campo "Descripción" permitirá establecer la relación entre tres aspectos de la identificación del riesgo, que facilitan su comprensión:

- Posibilidad de afectación: la posibilidad de afectación está determinada por los tipos de impacto que pueda generar la materialización del riesgo (Económica o reputacional), dependiendo del riesgo que se esté identificando, se define cual genera un mayor nivel de afectación y este será la primera parte de la descripción del riesgo. Ejemplo: Posibilidad de afectación reputacional

- Riesgo: retoma el nombre del riesgo definido en el numeral 6.2.1 y lo acompaña del conector "Por". Ejemplo: por el Incumplimiento de la planeación institucional.

- Debido a: una vez se identifiquen las causas del riesgo, se clasifican en causas raíz e inmediatas; las raíces se llevan a la descripción del riesgo, iniciando con debido a. ejemplo: debido a la subestimación en cuanto a tiempos y recursos necesarios para desarrollar las actividades planificadas.

Finalmente, la descripción del riesgo debe quedar estructurada de la siguiente manera:

Posibilidad de afectación reputacional por el Incumplimiento de la planeación institucional debido a la subestimación en cuanto a tiempos y recursos necesarios para desarrollar las actividades planificadas.

6.2.3. Aspectos y orientaciones para la descripción de los riesgos fiscales

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.

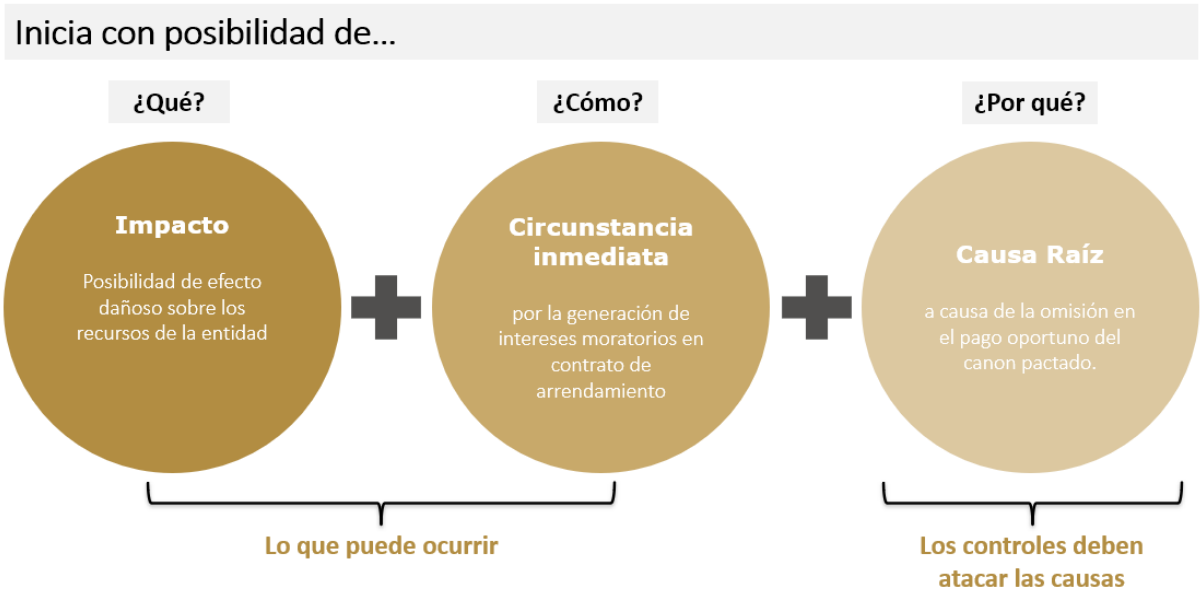


Ilustración 8. Descripción de los riesgos de tipo fiscal

6.2.4. Responsables del riesgo identificado

En esta etapa se determinan dos responsabilidades frente al riesgo identificado, denominadas de la siguiente manera:

- **Responsable:** es el encargado de liderar la identificación y gestión adecuada del riesgo, desde el modelo de operación por procesos institucional.
- **Gestor:** es el encargado de registrar los resultados del comportamiento del riesgo a partir de las autoevaluaciones realizadas en el proceso y la operación de los controles asociados.

6.2.5. Factores generadores de riesgo

Los factores generadores de riesgo son el resultado del análisis del contexto estratégico, por lo tanto, son el insumo para determinar las causas del riesgo; por esta razón, cada una de las causas del riesgo identificado, se deben asociar a un agente externo o interno de riesgo, según corresponda.

A continuación, se presentan los agentes generadores de riesgo internos y externos definidos a partir de los insumos de la planeación estratégica y de la revisión anual a partir de la estructuración del plan de acción:

Nombre del factor	Descripción	Situaciones asociadas
URF_EXT_01_Económicos y financieros	Asignación de recursos económicos suficientes para funcionamiento e inversión, independientemente la fuente de recursos.	Falta de disponibilidad de recursos para la operación institucional en cuanto a: • Provisión de cargos • Cumplimiento compromisos • Ejecución proyectos de inversión • Desarrollo de estudios e investigación
URF_EXT_02_Político y decisiones de gobierno	Actuaciones políticas nacionales o internacionales que generan cambios en el entorno institucional.	• Decisiones políticas que pueden afectar la operación institucional • cambios de gobierno • asignación de responsabilidades en PND
URF_EXT_03_Legal y reglamentario	Normatividad externa aplicable a la Unidad, así como los lineamientos del MIPG que resultan pertinentes para su operación institucional.	• Cambios en la legislación nacional o internacional • Cambios o nuevos lineamientos por parte de los líderes de políticas de gestión y desempeño institucional • Lineamientos externos desactualizados o con requerimientos que no corresponden con las particularidades de la Unidad
URF_EXT_04_Interacción y relación con partes interesadas y grupos de valor	Condiciones de interacción y relación con los usuarios, grupos de valor, proveedores y demás partes interesadas de la Unidad.	• Eventos relacionados con transacciones y operaciones realizadas • Baja participación de los usuarios y grupos de valor en los procesos participativos que adelanta la Unidad • Desconocimiento de la gestión institucional o pérdida de credibilidad por parte de los usuarios y partes interesadas hacia la Unidad

Nombre del factor	Descripción	Situaciones asociadas
		• Dependencia del Ministerio de Hacienda y Crédito Público en el marco de la colaboración Interinstitucional, de acuerdo con decreto 1658 de 2016 • Incumplimiento de proveedores en sus obligaciones con la Unidad, en las diferentes etapas del proceso de contratación • Coordinación interinstitucional en el marco de sus funciones o ejecución de convenios interadministrativos • Retrasos o reprocesos en revisión de proyectos normativos por parte de la Secretaría General del MHCP
URF_EXT_05_Social	Condiciones del entorno social relacionadas con situaciones de orden público, dinámicas comunitarias y comportamientos anómalos que puedan afectar la operación institucional o la seguridad de los servidores.	• Alteración en el orden público que dificulten la operación • Hurtos • Actuaciones o presiones indebidas de particulares para influir en la gestión de la Unidad (Soborno, Corrupción, conflicto de intereses)
URF_EXT_06_Tecnológico	Cambios y avances tecnológicos de la cuarta revolución industrial que pueden afectar la operación de la Unidad.	• Evoluciones tecnologías • Modificación de plataformas tecnológicas • Interrupciones en las redes de comunicación, fallas en las plataformas tecnológicas y aplicativos externos • Vulnerabilidad en los sistemas de seguridad de la información • Cambios tecnológicos que generen obsolescencia de los sistemas y modelos con que cuenta la Unidad mediante el convenio con el Ministerio de Hacienda

Nombre del factor	Descripción	Situaciones asociadas
URF_EXT_07_Ambiental	Eventos naturales o acciones humanas que afectan el ambiente y pueden impactar la infraestructura donde opera la Unidad, generalmente de manera inesperada o imprevisible.	**Eventos naturales:** • Incendios forestales o estructurales. • Inundaciones. • Terremotos. • Deslizamientos o derrumbes. • Tormentas, vendavales o granizadas. **Acciones humanas que generan afectación ambiental:** • Contaminación del aire, agua o suelo. • Vertimientos o derrames de sustancias peligrosas. • Manejo inadecuado de residuos. • Obras civiles o intervenciones externas que afecten la infraestructura. • Daños intencionales o vandalismo que comprometan el entorno físico.
URF_INT_01_Estructura Organizacional	Situaciones relacionadas con la, estructura organizacional, funciones y responsabilidades	• Cambios en la estructura y funcionamiento de las dependencias • Cambios en el modelo de operación de la Unidad • Definición de niveles de responsabilidad y autoridad • Novedades en planta de personal • Novedades administración de personal • Disponibilidad de personal para desarrollo de funciones • Liderazgo de Alta Dirección en la sostenibilidad del el Sistema de Gestión Institucional

Nombre del factor	Descripción	Situaciones asociadas
URF_INT_02_ Competencias e Integridad del Talento Humano	Capacidad operativa y comportamiento íntegro de los servidores de la Unidad en el ejercicio de sus funciones y responsabilidades.	• Deficiente capacidad operativa y/o conocimiento técnico para el desarrollo de funciones • Desconocimiento del marco normativo • Desarrollo de funciones sin acatar el manual de integridad • Actos de corrupción y/o acciones que afectan la integridad pública • Extralimitación de funciones • Baja disposición para participar en actividades de capacitación, sensibilización que se programan en la Unidad • Resistencia al cambio
URF_INT_03_S eguridad y salud en el trabajo	Condiciones internas de trabajo, incluyendo aspectos físicos, de seguridad, emocionales y psicosociales; que pueden afectar la protección, el bienestar y la salud física, mental y social de los servidores, así como su motivación y desempeño.	**Condiciones físicas y del entorno de trabajo** • Espacio físico insuficiente o inadecuado • Instalaciones en mal estado o con deficiencias • Temperaturas extremas o inadecuadas **Condiciones organizacionales** • Organización inadecuada del trabajo • Carga mental elevada. • Estabilidad laboral limitada o incierta • Políticas de ascenso poco claras, inexistentes o no basadas en criterios de mérito • Remuneración laboral percibida como insuficiente o inequitativa **Condiciones psicosociales y relacionales** • Conflictos en los equipos de trabajo • Debilidad en las relaciones interpersonales • Acoso laboral (moral, sexual o por discriminación)

Nombre del factor	Descripción	Situaciones asociadas
URF_INT_04_Gestión y administración de procesos	Condiciones asociadas con la operación, gestión y mejora de los procesos institucionales	• Operación inadecuada de los modelos de gestión, • Incumplimiento actividades del proceso • Registro deficiente de la gestión del proceso en el SMGI relacionada con los elementos transversales • Deficiente autorregulación del proceso • Deficiente divulgación de lineamientos internos • Lineamientos inadecuados • Entrega deficiente o inoportuna de insumos a otros procesos • Fallas en la interrelación y coordinación entre procesos
URF_INT_05_Mecanismos de Control	Condiciones relacionadas con la suficiencia, oportunidad y efectividad de los mecanismos de seguimiento, control y toma de decisiones institucionales, que pueden afectar la adecuada revisión, aprobación y supervisión de los procesos.	• Insuficientes e inadecuados mecanismos de seguimiento y control • Demoras o retrasos en las actividades de revisión y aprobación por parte de los responsables asignados (líderes, líneas de defensa) • Operación, resultados y decisiones de los diferentes comités institucionales • Sobrestimación de mecanismos de control y seguimiento
URF_INT_06_Sistemas tecnológicos y seguridad de la información	Operación y disponibilidad de los sistemas de información de la Unidad, así como la seguridad de la información	• Desactualización o limitaciones en las herramientas tecnológicas utilizadas por la Unidad • Deficiente identificación y descripción de necesidades para el desarrollo o ajuste de soluciones tecnológicas • Dificultades en el acceso a los sistemas de información institucionales • Fallas en los aplicativos administrados por la URF que afectan su disponibilidad o funcionamiento • Fugas o exposición no autorizada de información institucional • Resistencia a la adopción y aplicación de cambios tecnológicos

Nombre del factor	Descripción	Situaciones asociadas
URF_INT_07_Información, Comunicación y Gestión del Conocimiento	Condiciones relacionadas con la calidad, disponibilidad y circulación de la información, la efectividad de la comunicación interna y la implementación de estrategias de gestión del conocimiento, que pueden afectar la coordinación entre procesos, la toma de decisiones y la generación de resultados institucionales.	• Información remitida a otros procesos con deficiencias en calidad, vigencia o pertinencia para la generación de resultados • Limitada disponibilidad o acceso oportuno a la información requerida por otros procesos • Fallas en la comunicación entre equipos de trabajo y niveles directivos • Debilidad en la implementación y seguimiento de las estrategias de comunicación organizacional Falencias o inexistencia de estrategias estructuradas de gestión del conocimiento, incluyendo la identificación, documentación, transferencia y preservación del conocimiento institucional

6.2.6. Causas

Las causas son los medios, circunstancias y/o agentes generadores de riesgos; la definición de las causas es de gran relevancia para lograr una adecuada administración del riesgo. Se debe garantizar la coherencia entre las causas y el riesgo identificado, teniendo en cuenta que los controles estarán orientados a la eliminación o mitigación de causas asociadas al riesgo.

"Una definición inadecuada de las causas, conlleva a un tratamiento incipiente y poco efectivo de los riesgos identificados por definición errada de los controles".

6.2.7. Clasificación de las causas

Una vez identificadas las causas del riesgo, se deben clasificar en:

- **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.

- **Causa raíz:** es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir una o más causas o subcausas que pueden ser analizadas.

6.2.8. Consecuencias

Son los efectos que se generan o pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la Unidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Se deben determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado.

6.2.9. Asociación estratégica, organizacional y por proceso

En la etapa de identificación es necesario asociar los objetivos e iniciativas estratégicas de la Unidad que se verían impactados tras la materialización del riesgo, los cuales hacen parte del Plan Estratégico Institucional – PEI, por lo tanto,

es importante orientar las intervenciones del riesgo a mitigar las posibles consecuencias que podrían afectar a estos objetivos.

Adicionalmente, en este punto se realiza la asociación del riesgo al proceso que corresponde y área organizativa de la Unidad.

6.2.10. Incidencia jurídica del riesgo

Determinar si el riesgo identificado, puede generar un daño con incidencia jurídica en caso de materializarse:

Riesgo	¿La materialización del riesgo puede generar un daño con incidencia jurídica?	Descripción del daño que se puede generar
R27. Inadecuada defensa judicial de la Unidad	Si	Fallos judiciales en contra de la Unidad

6.2.11. Fuentes de identificación del riesgo

Este aspecto, hace referencia a las situaciones, circunstancias o mecanismos que se tuvieron en cuenta al momento de identificar el riesgo; las fuentes identificadas son:

- Análisis de factores como presiones internas o externas que puedan derivar en actos que afecten la integridad pública
- Análisis de las funciones institucionales
- Análisis estratégico institucional
- Análisis normativo
- Autoevaluación de los procesos
- Detalle de la operación del proceso, incluido objetivo, alcance, actividades, productos, entre otros
- Evaluación de información proveniente de quejas y denuncias de las partes interesadas
- Evaluación de la información proveniente de quejas y denuncias de los servidores de la Unidad
- Nuevas funciones institucionales
- Resultados de los Informes de Control Interno
- Resultados del Comité Institucional de Coordinación de Control Interno
- Resultados del Comité Institucional de Gestión y Desempeño
- Retroalimentación de grupos de valor y partes interesadas

- Reuniones de revisión de procesos

Al momento de documentar el riesgo en el Sistema de Monitoreo de la Gestión Institucional – SMGI, se podrán identificar otro tipo de fuentes que no se hayan nombrado en la lista anterior.

6.2.12. Tipos de riesgo

Los riesgos que se identifiquen a partir de la gestión de los procesos pueden ser de diferentes tipos; a continuación, se presentan los inicialmente definidos por la Unidad:

- **Riesgo estratégico:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la Unidad.

- **Riesgos generales de la gestión:** Son aquellos eventos que pueden afectar el desarrollo normal de los procesos, funciones y actividades de la Unidad. Corresponden a riesgos de naturaleza operativa, propios del funcionamiento institucional, y se originan en la forma como la Entidad organiza, ejecuta y controla sus procesos, utiliza sus recursos y atiende a sus grupos de valor.

  Estos riesgos pueden variar según las características de cada proceso y del ámbito organizacional en el que se desarrollan, teniendo en cuenta la naturaleza y funciones de la Unidad, su estructura, los recursos disponibles, los productos y servicios que entrega y las particularidades de su operación.

  Por esta razón, los riesgos asociados a los procesos pueden diferir en número, complejidad y alcance, dependiendo de los objetivos del proceso, sus actividades clave y su contribución a la generación de valor público.

- **Riesgos para la integridad pública:** son aquellos eventos, acciones u omisiones que pueden comprometer el comportamiento ético, la transparencia y la rectitud en el ejercicio de la función pública, afectando la confianza ciudadana y el cumplimiento de los fines del Estado. Estos riesgos incluyen situaciones que pueden generar afectación o pérdida de recursos públicos, así como la ocurrencia de fraude, corrupción o inadecuada gestión de conflictos de interés, en cualquiera de las etapas de la gestión institucional. Su materialización puede distorsionar la toma de decisiones, vulnerar principios de igualdad y legalidad, y deteriorar la eficiencia, eficacia y credibilidad de la entidad.

- **Riesgo fiscal:** posibilidad de daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403 de 2020, art.6). Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

  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.

  Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

- **Riesgos de seguridad de la información digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales; así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

- **Riesgos ambientales:** posibilidad de que se produzca un daño o catástrofe en el medio ambiente debido a un fenómeno natural o a una acción humana.

- **Riesgos de seguridad y salud en el trabajo:** fuente, situación o acto con un potencial de producir un daño en términos de una lesión o enfermedad, daño a la propiedad, daño al medio ambiente o una combinación de éstos.

6.2.13. Productos y/o servicios que pueden afectarse con la materialización del riesgo

En la identificación del riesgo, también es necesario asociar los productos finales del proceso que se pueden ver afectados con la materialización del riesgo, por tal motivo, se deben definir los productos asociados teniendo en cuenta el proceso al cual pertenece el riesgo y la caracterización correspondiente.

6.2.14. Recursos necesarios para la gestión del riesgo

De acuerdo con la naturaleza del riesgo identificado y sus posibles controles, se deben definir los tipos de recursos necesarios para su gestión:

- Talento Humano
- Físicos
- Tecnológicos
- Financieros

6.2.15. Incidencia directa en el usuario externo

De acuerdo con la descripción que se realice del riesgo (Determinación del riesgo con las causas y consecuencias asociadas), se debe definir la incidencia de este frente a la prestación de servicios para el usuario externo.

Posterior a realizar el análisis de la posible incidencia del riesgo frente al usuario externo, se debe responder la siguiente pregunta con "SI o NO", según corresponda:

¿El impacto generado por la materialización del riesgo, tiene incidencia directa en los servicios prestados al usuario externo?

El anterior ejercicio se realiza para clasificar como riesgos institucionales aquellos que, en el caso de materializarse, tengan una incidencia en el usuario externo.

6.2.16. Aspectos validadores de los riesgos para la integridad pública

Con el fin de facilitar la identificación de los riesgos para la integridad pública y evitar confusiones con los riesgos de gestión, se verifica el cumplimiento de una serie de aspectos previamente definidos que permiten determinar si un evento corresponde a esta categoría. Los aspectos validadores son:

- **Afecta o puede afectar recursos públicos**: Existe posibilidad de pérdida, uso indebido, desviación, deterioro o apropiación de recursos públicos. Se compromete la correcta administración de bienes, información o fondos del Estado.

- **Implica fraude o manipulación deliberada:** Hay intención o posibilidad de engañar, ocultar, alterar información o manipular procesos para obtener un beneficio indebido. Se presentan señales de falsificación, suplantación, alteración de documentos o registros.

- **Está relacionado con actos de corrupción**: El evento involucra o puede involucrar soborno, cohecho, tráfico de influencias, abuso de funciones, favorecimiento indebido o concusión. Se identifica riesgo de decisiones tomadas para beneficiar intereses particulares.

- **Involucra conflicto de interés no gestionado:** El servidor o contratista tiene intereses personales, familiares, económicos o de otra naturaleza

que pueden interferir en el cumplimiento imparcial de sus funciones. No existe declaración, gestión o mitigación adecuada del conflicto.

- **Afecta la transparencia o la confianza pública**: El evento puede deteriorar la credibilidad institucional, la percepción de integridad o la confianza de los grupos de valor. Se compromete el acceso a información pública o la rendición de cuentas.

- **Distorsiona la toma de decisiones públicas**: El riesgo puede generar decisiones parciales, sesgadas o no fundamentadas, afectando la objetividad y el interés general. Se identifican presiones indebidas, influencias externas o interferencias no autorizadas.

- **Compromete el cumplimiento de normas éticas o de integridad:** El evento vulnera principios del servicio público como la imparcialidad. Se incumplen lineamientos del Manual de Integridad y Buen Gobierno de la URF.

En caso de que uno o varios de estos aspectos validadores se cumplan, el riesgo deberá clasificarse como un riesgo para la integridad pública.

6.3. Etapa de análisis

La etapa de análisis busca establecer la probabilidad de ocurrencia del riesgo y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información cuantitativa y cualitativa para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, Probabilidad e Impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida a partir de la determinación de la frecuencia de ocurrencia del riesgo; por Impacto, se entiende las consecuencias que puede ocasionar a la Unidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

6.3.1. Clasificación del riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización el riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

		Escala de probabilidad	
		Frecuencia de materialización	**Frecuencia de la actividad riesgosa**
20%	**Muy baja**	Nunca o no se ha presentado	La actividad que conlleva el riesgo, se ejecuta máximo dos veces por año.
40%	**Baja**	Al menos una vez en el último año	La actividad que conlleva el riesgo, se ejecuta de 3 a 24 veces por año.
60%	**Media**	Al menos una vez en los últimos 8 meses	La actividad que conlleva el riesgo, se ejecuta de 24 a 500 veces por año.
80%	**Alta**	Una vez en el últimos 4 meses	La actividad que conlleva el riesgo, se ejecuta mínimo 501 y máximo 5000 veces por año.
100%	**Muy alta**	Más de una vez en el últimos 4 meses	La actividad que conlleva el riesgo, se ejecuta más de 5001 veces por año.

Ilustración 9. Escala de calificación para la probabilidad

		Escala de impacto	
		Afectación Económica	**Afectación reputacional**
20%	**Leve**	Afectación menor o igual a 10 SMLMV	El riesgo afecta la imagen de alguna subdirección o proceso de la Unidad.
40%	**Menor**	Afectación entre 11 y 50 SMLMV	El riesgo afecta la imagen de la Unidad internamente, de conocimiento general a nivel interno y del consejo directivo.
60%	**Moderado**	Afectación entre 51 y 100 SMLMV	El riesgo afecta la imagen de la Unidad con algunos grupos de valor de relevancia frente al logro de los objetivos.
80%	**Mayor**	Afectación entre 101 y 500 SMLMV	El riesgo afecta la imagen de la Unidad con efecto publicitario sostenido a nivel del Sector Hacienda y de los grupos de valor.
100%	**Catastrófico**	Mayor a 500 SMLMV	El riesgo afecta la imagen de la Unidad a nivel nacional, con efecto publicitario sostenido a nivel país y de los grupos de valor.

Ilustración 10. Escala de calificación para el impacto

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se deberá tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel mayor e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel mayor.

Ilustración 11. Impacto inherente del riesgo fiscal

Cuando se desarrolla la etapa de análisis como consecuencia de la identificación inicial del riesgo, se debe utilizar la frecuencia de la actividad riesgosa asociada en la escala de probabilidad, estableciendo el número de veces que se realiza la actividad riesgosa en una vigencia; cuando el análisis se realiza como consecuencia de materialización del riesgo, se debe utilizar la frecuencia de materialización.

6.3.2. Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente. La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas; esta evaluación se realiza de manera automática por el SMGI.

Probabilidad						
	Muy alta	A	A	A	A	E
	Alta	M	M	A	A	E
	Media	M	M	M	A	E
	Baja	B	M	M	A	E
	Muy baja	B	B	M	A	E
		Leve	Menor	Moderado	Mayor	Catastrófico
		Impacto				

Ilustración 12. Matriz de evaluación del riesgo

Color	Zona de riesgo
B	Baja
M	Moderada
A	Alta
E	Extrema

Ilustración 13. Zonas de riesgo

Con el desarrollo de la etapa de análisis se obtiene:

Calificación y evaluación del riesgo inherente (Corresponde a la determinación de la probabilidad, el impacto y el cruce de estas dos variables antes de contemplar posibles controles asociados al riesgo).

Ilustración 14. Resultados de la etapa de análisis

6.4. Etapa de valoración de riesgos

Es la etapa de valoración del riesgo mediante la cual se realiza la descripción detallada y calificación de los controles asociados al riesgo; se debe realizar en los siguientes pasos:

- **Paso 1:** Identificar y describir cualitativamente los controles y el detalle de sus características.
- **Paso 2:** Evaluar los controles a partir de la información documentada sobre sus características.

De acuerdo con la calificación de cada control, se determinará la evaluación del riesgo residual y la opción de manejo correspondiente.

6.4.1. Descripción cualitativa de controles

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la Unidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan los aspectos mínimos que se deben tener al momento de formular o describir los controles:

Ilustración 15. Aspectos mínimos para formulación y descripción de los controles

- **Nombre:** El nombre del control debe describir de manera explícita la acción que se ejecuta para prevenir o mitigar el riesgo. Debe formularse utilizando verbos de acción fuertes que indiquen claramente qué se hace, cómo se hace o qué se verifica. Ejemplos de verbos recomendados: verificar, validar, conciliar, comparar, revisar, cotejar, detectar. Ejemplo de buena práctica: "Revisar y tabular mensualmente las encuestas de satisfacción de usuarios".

- **Descripción:** Definir de manera detallada cómo se ejecuta el control. Ejemplo: Para un control denominado validar el cumplimiento de los bienes a recibir, la descripción es: El profesional de almacén revisa las características de los bienes a recibir de acuerdo con la orden del pedido y las características definidas en el contrato, diligenciando el formato de recepción de bienes**.**

- **Propósito:** Determinar para qué se realiza el control; ejemplo: Para un control denominado validar el cumplimiento de los bienes a recibir, el propósito es determinar si los bienes recibidos cumplen con las características definidas en el contrato de acuerdo con las necesidades establecidas.

- **Alcance:** determinar con qué acciones inicia y finaliza la operación del control.

- **Documentación:** Se debe indicar el documento del proceso que describe el control. Ejemplo: en el procedimiento de administración de bienes y servicios. No es una opción válida para este campo indicar de forma genérica que se encuentra en los documentos del proceso.

- **Responsable:** Persona asignada para ejecutar el control; la persona asignada, debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas (Riesgos para la Integridad Pública). Ejemplo: El coordinador de operaciones.

    - Cuando un control se hace de manera manual (ejecutado por personas) es importante establecer el cargo responsable de su realización; cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es

importante establecer como responsable de ejecutar el control al sistema o aplicación.

- **Línea de defensa del responsable:** registre la línea de defensa a la cual corresponde el responsable de operar el control.

- **Periodicidad:** El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Hay controles que no tienen una periodicidad específica como, por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores solo se ejecutan cuando se contratan proveedores. La periodicidad debe quedar redactada de tal forma que indique: que cada vez que se desarrolla la actividad se ejecuta el control.

- **Fuentes de información para la ejecución del control**: La ejecución del control debe sustentarse en el uso de fuentes de información confiables, que permitan verificar de manera objetiva su funcionamiento. Para ello, se deberán emplear:

  - Fuentes internas: formatos, registros, documentos o sistemas formales generados por la Unidad.
  - Fuentes externas: información verificable proveniente de terceros, tales como extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP o bases de datos oficiales.
  - Fuentes mixtas: combinación de datos provenientes de fuentes internas y externas que permitan validar la adecuada aplicación del control.

- **Observaciones o desviaciones:** El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Ejemplo: En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación.

- **Evidencias de aplicación:** El control debe dejar evidencia de su ejecución. Esta evidencia permite validar la información por parte de un tercero y

llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos. Ejemplo: Como evidencia: la respectiva lista de chequeo diligenciada con la información de la carpeta del cliente y correos solicitando la información faltante en los casos que aplique.

- **Divulgación de resultados con la alta dirección:** Cuando los resultados de aplicación de los controles se informan de manera directa a la alta dirección, se debe describir el mecanismo o espacio utilizado para realizar este ejercicio.

Ilustración 16. Aspectos importantes en la identificación de controles

Una vez se hayan identificado y descrito todos los controles, se debe determinar la clase del control; que puede ser preventivo, detectivo o correctivo como se presenta a continuación:

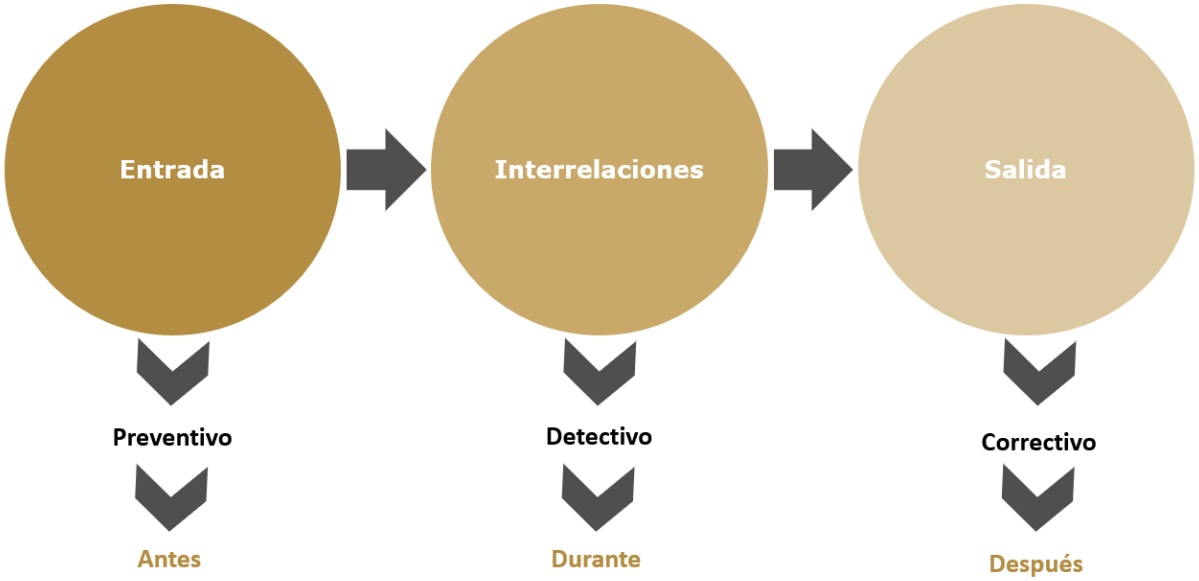


Ilustración 17. Clases de controles

Una vez se determina si el control descrito es preventivo, detectivo o correctivo, se debe determinar qué escala (probabilidad o impacto) se afecta con la aplicación del control, teniendo en cuenta las siguientes indicaciones:

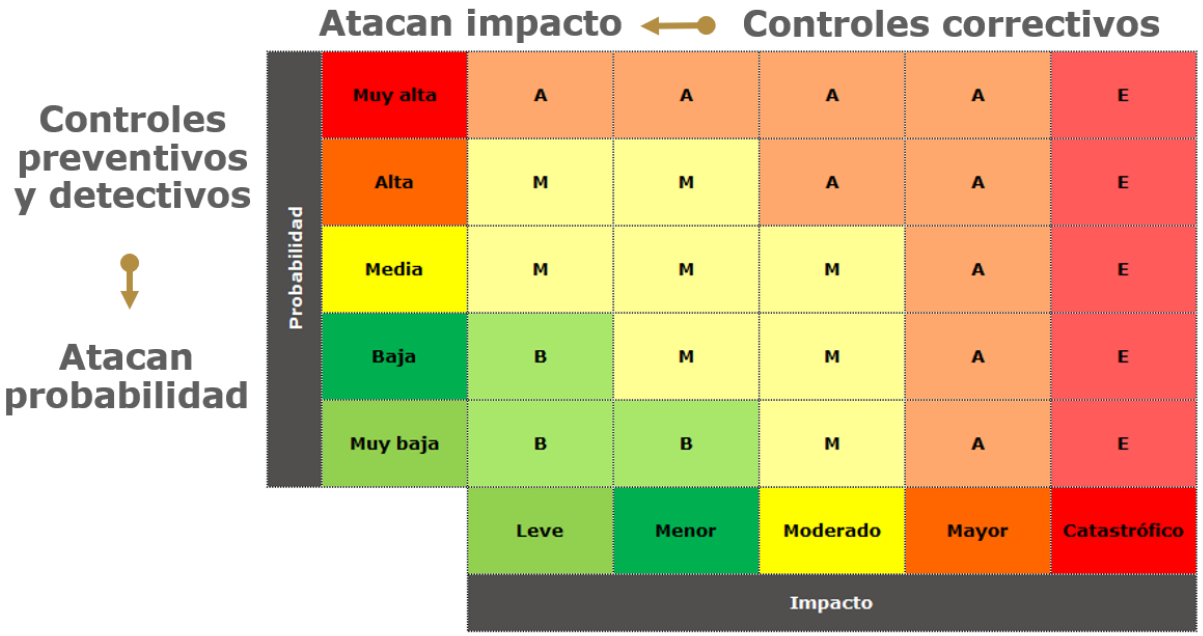


Ilustración 18. Escala afectada según el tipo de control

6.4.2. Evaluar los controles

De acuerdo con la información documentada en el paso anterior, relacionada con los aspectos que debe tener cada control y según los datos de su operación, se evaluaran los controles a partir de las siguientes preguntas:

La máxima calificación que puede obtener un control será de 50 puntos; este resultado definirá la evaluación del riesgo residual de acuerdo con la siguiente operación matemática que debe aplicarse por cada control:

Tipo de atributo	Peso total criterio	Nombre del criterio	Opciones del criterio	Descripción opciones del criterio	Peso por opción del criterio
Atributos de Eficiencia	15	Propósito de control (Tipo)	Prevenir y detectar	El control identificado se puede clasificar como preventivo y detectivo	15
			Prevenir	Va hacia las causas del riesgo, aseguran el resultado final esperado.	15
			Detectar	Detecta que algo ocurre y devuelve el proceso a los controles preventivos; se pueden generar reprocesos.	10
			Corregir	Permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	5
	10	Implementación	Automático	El control es una o varias actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	10

Tipo de atributo	Peso total criterio	Nombre del criterio	Opciones del criterio	Descripción opciones del criterio	Peso por opción del criterio
			Manual	El control es ejecutado por una persona.	7
Atributos de Formalización	5	Documentación	Documentado	El control está documentado en el proceso, ya sea en manuales, procedimientos o cualquier otro tipo documental.	5
			Sin Documentar	El control se ejecuta pero no se encuentran documentado en el proceso.	0
	5	Responsabilidad	Asignada	Existe un responsable asignado para la ejecución del control y esta responsabilidad es coherente con sus funciones u obligaciones.	5
			Asignada sin asociación	Existe un responsable asignado para la ejecución del control; sin embargo, la responsabilidad no es coherente con sus funciones u obligaciones.	3
			No asignada	No existe un responsable asignado para la ejecución del control.	0
	4	Frecuencia	Continua	El control se ejecuta siempre que se realiza la actividad originadora del riesgo.	4

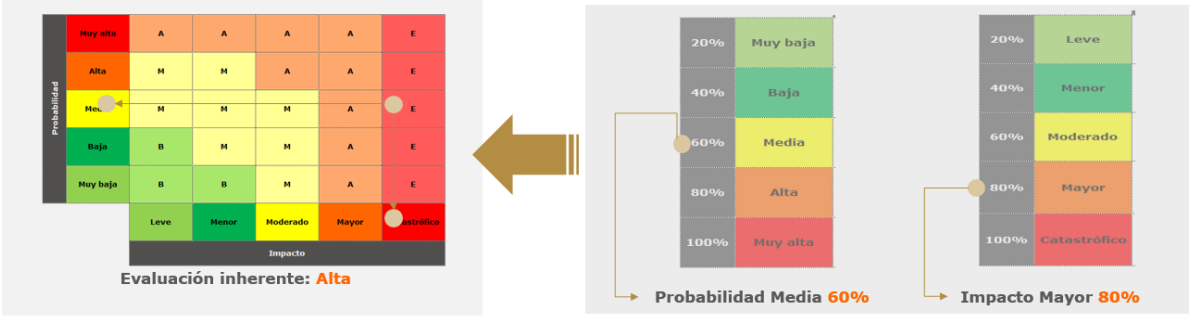
Tipo de atributo	Peso total criterio	Nombre del criterio	Opciones del criterio	Descripción opciones del criterio	Peso por opción del criterio
			Aleatoria	El control se ejecuta de manera esporadica o aleatoria.	2
	4	Observaciones o desviaciones	Gestionadas	Se encuentran definidas, se investigan y resuelven oportunamente.	4
			No gestionadas	No están definidas, por lo tanto, a la fecha no se investigan ni resuelven.	0
	3	Comunicación de resultados	Divulgados	Como parte del control, se comunican los resultados a la alta dirección para tomar medidas y hacer seguimiento a su operación.	3
			No divulgados	No se comunican los resultados de aplicación del control.	2
	4	Evidencia	Con Registro	Existe evidencia o rastro disponible actualmente, que permita validar la ejecución del control con un registro manual o electrónico.	4
			Sin Registro	No existe evidencia que permita validar la ejecución del control.	0

Al seleccionar la respuesta para cada pregunta, se asigna automáticamente una calificación cuantitativa según los pesos definidos en la matriz. Esta calificación determina el nivel de efectividad del control y permite calcular el promedio del conjunto de controles asociados al riesgo. El resultado final establece la ubicación del riesgo residual dentro de la matriz de evaluación.

Evaluación residual → **R. Residual = R. Inherente – (R.I. * Control)**

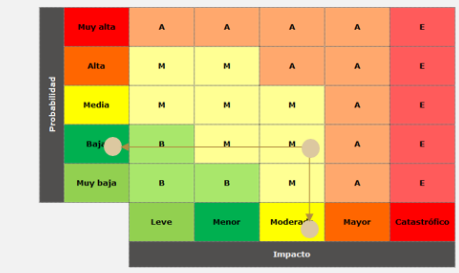
El Riesgo Inherente tiene dos valores, uno de probabilidad y otro de Impacto.

Ejemplo: Divulgar información inoportuna, confusa y poco confiable



Controles definidos para el riego

Nombre del control	Calificación *	Ataca	Fórmula para determinar la evaluación residual R. Residual = R. Inherente – (R.I. * Control)
• Revisar y aprobar la información antes de la publicación.	40	Probabilidad	(Probabilidad inherente) **60%** * (Calificación del control que afecta probabilidad) **40%** = (Resultado de la operación matemática) **24** **60% - 24% = 36% (Probabilidad residual)**
• Activar el plan de contingencia con Dirección de tecnología del MHCP.	35	Impacto	(Impacto inherente) **80%** * (Calificación del control que afecta impacto) **35%** = (Resultado de la operación matemática) **28** **80% - 28% = 52% (Impacto residual)**



Evaluación residual: Moderada

Los controles mitigan el riesgo de forma **acumulativa**, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Ilustración 19. Cálculo para la evaluación del riesgo residual

En ningún caso, se aceptará que un riesgo solo tenga asociados controles de tipo correctivo o solo un control (Preventivo o detectivo), con una calificación igual o inferior a 32 puntos.

Con el desarrollo de la etapa de valoración se obtiene:

Identificación, descripción y calificación de controles que permiten la determinación y ubicación del **riesgo residual** (Residual hace referencia la evaluación del riesgo después de calificar el estado de los controles asociados al riesgo).

Ilustración 20. Resultados de la etapa de valoración

6.5. Etapa de manejo de los riesgos

En esta etapa se determinarán los siguientes aspectos:

- Determinación de opción de manejo
- Definición de acciones de contingencia
- Definición del semáforo del riesgo
- Definición de acciones asociadas

6.5.1. Determinación de la opción de manejo

Después de la definición de la ubicación del riesgo residual, se debe asociar la opción de manejo; la descripción de estas opciones responde al apetito del riesgo aceptado por la Unidad:

Opción de manejo	Descripción
Asumir	Se acepta la pérdida residual probable si el riesgo se materializa.
Reducir el riesgo	Determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados; La formulación de acciones adicionales a los controles es necesaria cuando el nivel de probabilidad residual supera el nivel de "Muy baja".
Evitar el riesgo	Determina la formulación de acciones para continuar disminuyendo tanto probabilidad como el impacto, mediante el fortalecimiento de controles, optimización de procesos y el diseño de nuevos controles. La formulación de acciones adicionales a los controles es necesaria cuando el nivel de probabilidad residual supera el nivel de "Muy baja".

Opción de manejo	Descripción
Compartir el riesgo	Determina compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsorcing, seguros, sitios alternos. Los riesgos para la integridad pública se pueden compartir, pero no se puede transferir su responsabilidad. La formulación de acciones adicionales a los controles es necesaria cuando el nivel de probabilidad residual supera el nivel de "Muy baja".

Estas opciones se determinan teniendo en cuenta la ubicación del riesgo residual.

La opción de asumir el riesgo solo es válida cuando la evaluación residual se ubica en zona de riesgo baja o cuando la probabilidad se ubica en el menor nivel posible.

6.5.2. Definición de acciones de contingencia

La definición de acciones de contingencia aplica para todos los riesgos, independiente de su evaluación residual o de los controles existentes y consiste en la definición de **acciones inmediatas** a desarrollar en el caso de materialización del riesgo; estas acciones son la respuesta inicial a la materialización del riesgo y se enfocan en las correcciones que se deben desarrollar de acuerdo con las consecuencias definidas.

6.5.3. Apetito del riesgo

Teniendo en cuenta que dentro de la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación se desarrolla conceptualmente este tema para contar con mayores elementos de juicio para su análisis e implementación en los riesgos definidos en la Unidad:

Nivel de riesgo: Valor resultante de combinar la probabilidad de ocurrencia de un evento potencialmente adverso y la magnitud del impacto que dicho evento generaría sobre la capacidad institucional para alcanzar sus objetivos.

Apetito del riesgo: Nivel de riesgo que la entidad está dispuesta a aceptar en coherencia con sus objetivos estratégicos, su marco normativo y las directrices de la Alta Dirección y del Gobierno. Este puede variar según el tipo de riesgo que se gestione.

Tolerancia al riesgo: Límite máximo de desviación permitido respecto al apetito de riesgo definido, dentro del cual la gestión institucional se considera aceptable.

Capacidad de riesgo: Umbral superior del nivel de riesgo que la entidad puede soportar antes de comprometer gravemente la consecución de sus objetivos estratégicos.

Gráficamente, estos conceptos interactúan de la siguiente manera:

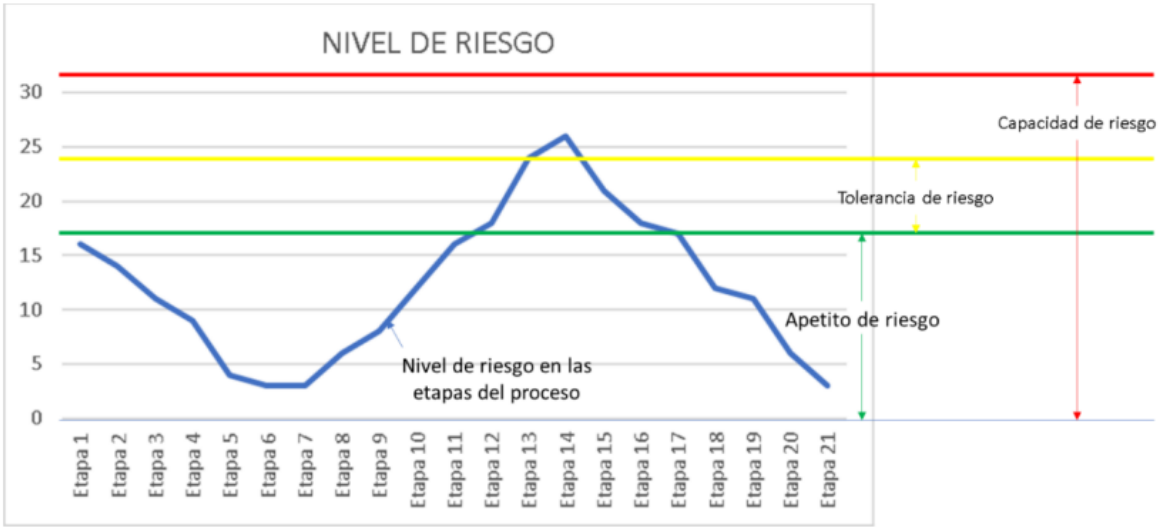


Ilustración 21. Conceptos relacionados con el apetito del riego

Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

En la fase de manejo de riesgos, cada responsable debe realizar un análisis contextualizado de las condiciones del riesgo identificado, considerando factores como la naturaleza del proceso, la criticidad de los objetivos afectados y las posibles consecuencias institucionales. Con base en dicho análisis, deberá establecer el **nivel de apetito de riesgo**, entendiendo este como el umbral de exposición que la Unidad considera aceptable en función de su capacidad de respuesta, marco normativo, objetivos estratégicos y directrices de la Alta Dirección.

Este nivel debe ser registrado de manera clara y argumentada en el campo dispuesto para tal fin en el módulo correspondiente del SMGI. Su adecuada formulación es **determinante para identificar cuándo se supera el umbral aceptable** y, por tanto, cuándo se requiere activar los mecanismos de reporte por materialización del riesgo. Además, este valor permite diferenciar entre una desviación esperada y un incidente que exige intervención correctiva inmediata.

Este enfoque refuerza la trazabilidad y consistencia de la gestión de riesgos y facilita el trabajo articulado entre las líneas de defensa, el comité institucional y los procesos responsables, asegurando que las decisiones estén basadas en criterios previamente definidos y no en interpretaciones reactivas o discrecionales.

La documentación de esta información se realiza en el siguiente espacio dispuesto en el Sistema de Monitoreo de la Gestión Institucional – SMGI:

- **Apetito del riesgo**: De acuerdo con la información estimada en el campo de actividad riesgosa, defina el número de veces que la entidad puede asumir la ocurrencia del riesgo para determinar el nivel de tolerancia o apetito del riesgo sin que esto implique una afectación mayor a la gestión institucional. Se recomienda estimar un nivel de tolerancia superior al 90%

6.5.4. Definición del semáforo del riesgo

Esta opción permite definir la opción mediante el cual la herramienta SMGI presentará los riesgos y su semáforo; las opciones disponibles en el sistema son:

- Sobre el estado y documentación oportuna de las acciones que se asocien para el manejo del riesgo.
- Sobre el estado y reporte que se realice de los indicadores que se asocien al riesgo.
- Sobre el cumplimiento de las fechas de monitoreo establecidas en la Unidad para que cada responsable.
- A partir de la evaluación residual del riesgo.

De acuerdo con los lineamientos institucionales, el semáforo de todos los riesgos se debe calcular con la opción de cumplimiento de las fechas de monitoreo.

6.5.5. Acciones para el manejo de los riesgos

La URF, en la determinación de la política de administración del riesgo, define que no se aceptan los riesgos si estos presentan fallas en los controles asociados (Calificación del control igual o inferior a 32 puntos); por esta razón, cuando se identifiquen controles con esta condición, se deben asociar acciones de manera obligatoria; las acciones deben estar orientadas al mejoramiento y fortalecimiento de los controles identificados; estas acciones se registrarán en el sistema como acciones de tipo preventivo.

Con el desarrollo de la etapa de manejo se obtiene:

Definición de los **niveles de aceptación del riesgo**, mediante la formulación de **acciones** para el fortalecimiento de los controles y formulación de acciones de **contingencia**.

Ilustración 22. Resultados de la etapa de manejo

6.6. Etapa de monitoreo de los riesgos

Esta etapa permite el seguimiento periódico a la gestión de los riesgos mediante el monitoreo a la operación adecuada de los controles; cada cuatro meses (Durante abril, agosto y diciembre), los responsables deben realizar seguimiento al estado, pertinencia y calificación de los controles, la vigencia de la información registrada en cada una de las etapas del riesgo, posibles situaciones de materialización y citar las evidencias de aplicación de los controles, mediante el reporte de información relacionada con:

- **Descripción de aplicación del control:** descripción de la operación para cada control durante el periodo, de acuerdo con los cortes de monitoreo establecidos.

- **Nombre de las evidencias:** se deben describir los soportes que evidencien la operación del control durante el periodo o citar la URL donde se encuentran ubicadas.

- **Soportes del control:** se deben adjuntar o asociar mediante la opción de conceptos los soportes que evidencien la operación del control durante el periodo.

- **Responsable de la ejecución del control**: registrar el cargo del servidor, rol o instancia que ejecutó el control durante el periodo.

- **Periodo de monitoreo:** de la lista desplegable, seleccionar el periodo al que corresponde el reporte de monitoreo.

- **Materialización del riesgo durante el periodo**: de la lista desplegable, indicar si el riesgo se materializó o no durante el periodo.

- **¿Se solicitó a direccionamiento y planeación actualizar la evaluación inherente del riesgo?:** Este campo aplica únicamente si la respuesta a la pregunta anterior fue afirmativa. Debe marcarse "Sí" cuando se haya reportado la materialización del riesgo y se hayan llevado a cabo sesiones de trabajo con Direccionamiento y Planeación orientadas a la actualización de la evaluación residual.

A partir de la información registrada por los responsables en el monitoreo, el proceso de Direccionamiento y Planeación realizará seguimiento al estado de gestión de este elemento transversal del Sistema de Gestión Institucional. Posteriormente, el proceso de Control y Evaluación, de acuerdo con los ciclos establecidos en el plan de auditoría, realizará la evaluación independiente de los riesgos identificados y gestionados en la Unidad.

Ilustración 23. Roles para el monitoreo y evaluación de los riesgos

Con el desarrollo de la etapa de monitoreo se obtiene:

Autoevaluación, seguimiento y evaluación independiente de la gestión del riesgo.
El proceso de Control y Evaluación también podrá pronunciarse sobre el desarrollo metodológico para la administración del riesgo establecido en la política.

Ilustración 24. Resultados de la etapa de monitoreo

6.7. Creación, modificación o eliminación de riesgos

Cuando el proceso requiera crear un nuevo riesgo, hacer ajustes en la información documentada, o eliminar un riesgo existente, se deberá registrar la solicitud correspondiente en el SMGI, mediante el módulo de mejoras, flujo Trámite de solicitudes.

Tipo de solicitud	Descripción	Tiempos de gestión
Crear riesgos	Registrar la solicitud con la justificación correspondiente en el flujo Trámite de solicitudes.	Los tiempos de gestión para dar respuesta a esta solicitud, se encuentran estandarizados en el flujo. **Nota:** se debe tener en cuenta que para crear riesgos es importante generar mesas de trabajo con el fin de registrar la información de cada etapa. Estas reuniones y el cierre de la solicitud dependerán de la programación que se realice de las mesas de trabajo. Para este caso, el proceso de direccionamiento y planeación realizará asesoría y acompañamiento.
Ajustar la información del riesgo	Mediante la opción disponible en el módulo de riesgos, registrar la solicitud con la justificación correspondiente.	De acuerdo con la justificación, el proceso de Direccionamiento y Planeación tendrá cinco días hábiles para verificar cada caso y aprobar la devolución a la etapa del riesgo, según la solicitud. Una vez aprobada la devolución de la etapa, el responsable tendrá diez días hábiles para registrar los ajustes en la información de las etapas del riesgo. Para este caso, el proceso de direccionamiento y planeación realizará asesoría y acompañamiento.
Eliminar riesgos	Mediante la opción disponible en el módulo de riesgos, registrar la solicitud con la justificación correspondiente.	Una vez registrada la solicitud debidamente justificada; el proceso de Direccionamiento y Planeación tendrá cinco días hábiles para inactivar el riesgo en el SMGI o pronunciarse al respecto.

Ilustración 25. Aval de solicitudes de creación, modificación o eliminación de riesgos

Para los casos dónde se necesite ampliar la información de los cambios con los solicitantes, el proceso de direccionamiento y planeación citará a las reuniones correspondientes.

6.8. Mapa de riesgos

El mapa de riesgos estará disponible para la consulta de todos los servidores, en el SMGI. Los líderes de procesos y sus equipos de trabajo deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y vigente. Cualquier ajuste que se deba realizar de esta información, debe ser tramitada con el proceso de Direccionamiento y Planeación.

Será el proceso de Direccionamiento y Planeación, el responsable de la publicación del mapa en la página web de la Unidad; esta publicación se realizará cada vez que se realicen ajustes a la información registrada por los procesos, o máximo cada cuatro meses, durante abril, agosto y diciembre de cada vigencia; la publicación se realizará en datos abiertos (Archivo de Excel) para facilitar la consulta por las partes interesadas.

7. Alineación con los valores del manual de integridad y buen gobierno

La Política de Administración del Riesgo de la URF se fundamenta en los principios y valores definidos en el Manual de Integridad y Buen Gobierno, los cuales orientan la conducta de los servidores y constituyen el marco ético para la gestión preventiva de riesgos. En coherencia con este manual, la gestión del riesgo se desarrolla bajo los siguientes lineamientos:

- **Honestidad:** La identificación, análisis, valoración y tratamiento de los riesgos se realiza con veracidad, transparencia y rectitud, garantizando que la información utilizada sea completa, confiable y oportuna.

- **Respeto:** La gestión del riesgo se desarrolla reconociendo la dignidad de todas las personas, promoviendo el diálogo técnico y la participación de los equipos de trabajo, y evitando cualquier forma de discriminación o trato inequitativo.

- **Compromiso:** Los servidores asumen la gestión del riesgo como una responsabilidad inherente a su rol, aportando activamente a la identificación de riesgos, la implementación de controles y la mejora continua.

- **Diligencia:** La administración del riesgo se ejecuta con oportunidad, rigor técnico y eficiencia, asegurando el uso adecuado de los recursos públicos y la calidad de los análisis y productos generados.

- **Justicia:** Las decisiones relacionadas con la valoración y tratamiento de riesgos se adoptan con imparcialidad, objetividad y equidad, basadas en evidencia y criterios técnicos.

- **Responsabilidad:** La gestión del riesgo incorpora el deber de rendición de cuentas, el uso adecuado de los bienes públicos y la obligación de prevenir cualquier daño patrimonial o afectación al interés general.

- **Servicio:** La administración del riesgo se orienta a fortalecer la calidad del servicio público, anticipando eventos que puedan afectar el cumplimiento misional y la satisfacción de los grupos de valor.

En consecuencia, la gestión del riesgo en la URF se concibe no solo como un ejercicio técnico, sino como una práctica ética que refleja los valores institucionales y orienta la conducta de los servidores hacia la protección del interés general. La aplicación de esta política exige que cada etapa del proceso, desde la identificación

hasta el monitoreo del riesgo, se ejecute con integridad, transparencia y responsabilidad, garantizando que las decisiones adoptadas fortalezcan la confianza pública, prevengan afectaciones al patrimonio del Estado y contribuyan al cumplimiento de los objetivos institucionales.

8. Comunicación

El mecanismo institucional utilizado para la divulgación de la política es el Sistema de Monitoreo de la Gestión Institucional -SMGI.

9. Mecanismo de monitoreo, control y evaluación

El mecanismo institucional utilizado para monitorear periódicamente el cumplimiento de los lineamientos establecidos en la política de gestión del riesgo es la Estrategia de Seguimiento y Evaluación del Desempeño Institucional - ESEDI, la cual permite fortalecer y hacer seguimiento a la aplicación y operación de los elementos transversales del Sistema de Gestión Institucional (planes, documentos, riesgos, indicadores, mejoras) en cada uno de los procesos definido en el modelo operación.

10. Documento referente

Tipo	Nombre
Caracterización	Caracterización del proceso de Direccionamiento y Planeación.

11. Datos de elaboración y control de cambios

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
2019-05-09	1.0	No aplica	Creación del documento.
2020-06-08	2.0	URF_TS-078	Ajuste de acuerdo con los lineamientos del Departamento Administrativo de la Función Pública y parametrización del SMGI.

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
2021-03-26	3.0	URF_TS-275	Ajuste de la política en aspectos relacionados con: - Escalas de probabilidad e impacto - Tipos de controles y criterios para la calificación de controles Ajuste de anexos para orientar en el manejo del módulo de riesgos en el SMGI.
2022-10-12	4.0	TS_0139	- Actualización del documento en el formato vigente para documentar políticas - Identificación de ajuste en la declaración principal (Página 3) - Inclusión de la tipología de riesgo fiscal - Ajuste en la definición de mapa de riesgos de corrupción - Cambio del logo del SMGI - Ajuste en las directrices para la descripción del riesgo (Numeral 6.2.2) - Inclusión de ajustes en los factores de riesgo, de acuerdo con la última actualización del contexto estratégico - Inclusión del numeral 6.26 de clasificación de las causas entre raíz e inmediata Inclusión del alcance en el numeral 6.4.1 de descripción cualitativa de los controles
2023-05-02	5.0	TS-0254	- Actualización del contexto estratégico - Ajuste en la definición de riesgo fiscal Ajuste en el numeral 6.2.2 - Descripción del riesgo, relacionado con la afectación económica de los riesgos de tipo fiscal.
2024-08-02	6.0	TS-0579	- Actualización del contexto estratégico - Ajuste de roles y responsabilidades - Ajuste del documento de acuerdo con la identidad visual vigente
2025-04-29	7.0	TS-0687	- Actualización del contexto estratégico - Actualización del documento al formato de política vigente

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
			- Actualización de la información relacionada con el apetito del riesgo - Actualización de la información relacionada con los campos dispuestos para reportar el monitoreo periódico del riesgo. - Inclusión del anexo de los riesgos de seguridad de la información digital - Actualización de la tabla de ilustraciones
2026-04-20	8.0	TS-1162	- **Incorporación de riesgos para la integridad pública:** Esta versión incorpora el tipo de riesgo para la integridad pública dentro del ámbito de aplicación, junto con su definición, alcance y los aspectos validadores que permiten clasificarlos. - **Incorporación de la función de cumplimiento**: Se introduce la función de cumplimiento como responsabilidad del proceso de Direccionamiento y Planeación, asignándole tareas como verificar el cumplimiento normativo en integridad pública, supervisar la gestión de riesgos de integridad, apoyar la evaluación de controles y emitir recomendaciones a la alta dirección. Esta función se incorpora como parte de la segunda línea de defensa y se establece la necesidad de contar con independencia técnica y acceso a la información para su adecuado ejercicio. - **Fortalecimiento de la metodología para riesgos fiscales**: La política incorpora un apartado específico con orientaciones para la descripción de los riesgos fiscales, incluyendo elementos como el objeto fiscal afectado, el evento generador, las causas, las consecuencias y los puntos críticos de riesgo. También se incluye una figura explicativa y definiciones actualizadas como gestor fiscal, punto de riesgo fiscal y recurso público.

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
			- **Actualización de términos y definiciones:** Se actualizan y amplían definiciones para armonizarlas con la Guía DAFP V7 y normas recientes, incluyendo conceptos como riesgo para la integridad, soborno entrante y saliente, fraude según ISO 37001:2025, materialización del riesgo en casos de integridad y punto de riesgo fiscal. - **Ajustes en roles y responsabilidades**: La tabla de líneas de defensa se actualiza para reflejar nuevas responsabilidades y fortalecer la gobernanza del riesgo. Se refuerza el rol de la línea estratégica en el análisis del contexto y el apetito del riesgo; se incorpora la obligación de reportar materializaciones en la primera línea; se formaliza la función de cumplimiento en la segunda línea; se fortalece el rol del Gestor Fiscal; y se ajustan las responsabilidades del proceso de Gestión de la Información en seguridad digital. La tercera línea refuerza su enfoque preventivo en auditoría interna. - **Ampliación del ámbito de aplicación**: La política amplía su alcance para ajustar las tipologías de riesgo, entre ellas los riesgos para la integridad pública, el riesgo fiscal, los riesgos de seguridad de la información digital, los riesgos ambientales y los riesgos de seguridad y salud en el trabajo. - **Ajustes en la metodología de controles:** Se actualizan los criterios para nombrar controles, promoviendo el uso de verbos de acción fuertes y descripciones claras. Se ajusta la estructura para describir controles, se actualiza la metodología de valoración y se incorpora la relación entre el tipo de control y su efecto en la matriz de riesgo residual.

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
			- **Actualización del contexto estratégico del riesgo:** de acuerdo con la información registrada en el levantamiento del plan de acción y las orientaciones de la guía de riesgos de la Función Pública. - **Actualización del anexo de riesgos de seguridad de la información digital.**

Elaboración, revisión y aprobación	
Elaboración	
Nombre:	Daissy Tatiana Santos Yate
Cargo:	Asesor
Revisión	
Nombre:	Acta No. 02 de 2026
Cargo:	Comité Institucional de Coordinación de Control Interno
Aprobación	
Nombre:	Diana Larisa Caruso López
Cargo:	Directora General encargada

12. Anexo 5. Riesgos de seguridad de la información digital

Contenido

1. Ámbito de aplicación 2
2. Términos y definiciones 2
3. Articulación etapas para la administración de riesgos 3
4. Articulación entre administración de riesgos de seguridad de la información con la Política de administración del riesgo 3
4.1. Etapa identificación del riesgo 4
4.1.1. Determinar la criticidad de los activos de información 8
4.1.2. Identificación de amenazas y vulnerabilidades 9
4.1.3. Variables adicionales de identificación 10
4.2. Etapa de análisis 11
4.3. Etapa de Valoración 11
4.3.1. Valoración de los controles existentes 11
4.4. Etapa de manejo 12
4.5. Fase de monitoreo 12
4.5.1. Registro y reporte de incidentes de seguridad de la información 12
4.5.2. Reporte de la gestión del riesgo de seguridad de la información 12
4.5.3. Reporte de la gestión del riesgo de seguridad de la información a autoridades especiales 13
5. Documento referente 13
6. Datos de elaboración y control de cambios 13

1. Ámbito de aplicación

Los riesgos de seguridad de la información digital aplican para todos los activos de información de la Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF, en lo relacionado con su integridad, confidencialidad y disponibilidad. Estos hacen parte del mapa de riesgos institucional, como se indica en el numeral 6.8 de la Política.

2. Términos y definiciones

A continuación, se definen los términos fundamentales empleados en el desarrollo de este documento, complementando las definiciones presentadas en el numeral 4 de la política de administración de riesgos, para establecer un marco de referencia común y asegurar la uniformidad en la interpretación.

- **Activos de información digital:** son cualquier tipo de información digital o recurso relacionado con la gestión de la información que tiene valor para la entidad y que deben protegerse en cuánto a su integridad, disponibilidad y confidencialidad. Son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios web, redes, información física o digital, personal, ubicación, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para funcionar en el entorno digital.

- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **Confidencialidad:** propiedad de la información que la hace no disponible.

- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.

- **Integridad:** propiedad de exactitud y completitud.

- **Riesgo de seguridad de la información digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales; así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

3. Articulación etapas para la administración de riesgos

Las etapas generales del proceso de gestión de riesgos se aplican transversalmente a distintas categorías, como los riesgos de gestión, contra la integridad pública y seguridad de la información. Sin embargo, las particularidades propias de cada tipología pueden requerir la adopción de herramientas o procedimientos adicionales, principalmente en las fases de identificación y análisis.

En lo que respecta a los riesgos de seguridad de la información digital, a continuación, se detallan los elementos específicos que deben ser contemplados de manera complementaria y coordinada en cada fase del proceso.

Etapa	Aspecto particular para riesgos de seguridad de la información
Identificación del riesgo	Se complementa con: la identificación de activos críticos que son la base para analizar amenazas y vulnerabilidades (asociado con el ítem de los factores de riesgos, causas)
Análisis	Se complementa con resultados de la identificación de activos críticos. El impacto del riesgo se afecta con la criticidad del activo.
Valoración	Se aplican los mismos lineamentos de la política de administración de riesgos
Manejo	Se aplican los mismos lineamentos de la política de administración de riesgos
Monitoreo	Se complementa con el registro y reporte de incidentes de seguridad de la información

Tabla 1. Articulación con las etapas de administración del riesgo

4. Articulación entre administración de riesgos de seguridad de la información con la Política de administración del riesgo

La gestión de riesgos de seguridad de la información debe integrarse con la política general de administración del riesgo. A continuación, se explica cómo se relacionan ambas en cada fase del proceso.

4.1. Etapa identificación del riesgo

En el marco del convenio interadministrativo 002 de 2016 suscrito entre la Unidad Administrativa Especial URF y el Ministerio de Hacienda y Crédito Público (MHCP), y en concordancia con lo dispuesto en el artículo 8 del decreto 1658 de 2016 relativo a la colaboración interinstitucional, el MHCP presta apoyo administrativo a la URF en áreas de recursos humanos, gestión documental, comunicaciones y tecnología.

En consecuencia, resulta necesario determinar la autoridad competente sobre cada tipo de activo de información de la URF, con el fin de identificar los riesgos de seguridad de la información digital. Los activos de información cuya propiedad recae en el MHCP no podrán ser gestionados directamente por la URF por carecer de la competencia legal para tal efecto. A continuación, se presenta la identificación de la autoridad de gestión para cada tipo de activo.

Tipo	Descripción	Gobierno
Información	Es un conjunto organizado de datos procesados que constituyen un mensaje y poseen significado para la Entidad.	**URF** Es producida por la Unidad. Es propiedad de la Unidad.
Software (sw)	Activo informático lógico. Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.	**MHCP** El software utilizado por la Unidad para su funcionamiento es de propiedad del Ministerio. Con relación al aplicativo SARA la Unidad realizó una inversión de parametrización particular para la URF pero el licenciamiento sigue siendo del Ministerio. El Sistema de Monitoreo de la Gestión Institucional – SMGI es de propiedad de la URF y

Tipo	Descripción	Gobierno
		el soporte es realizado por un proveedor externo.
Hardware	Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la Entidad. El hardware Se refiere a las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.	**MHCP** **URF**
Servicios	Servicio brindado por parte del Ministerio de Hacienda y Crédito Público para el apoyo de las actividades de los procesos. Los servicios en este caso se refieren al soporte técnico especializado brindado a la URF, como por ejemplo el servicio de soporte tecnológico de la Dirección de Tecnologías del Ministerio de Hacienda y Crédito Público. Servicios como el soporte de equipos y redes, soporte a servicios de office 365, Servicios WEB, intranet, portales organizacionales, aplicaciones, internet, entre otros.	**MHCP** Son propiedad el Ministerio
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, como la propiedad intelectual, las relaciones con clientes y proveedores, el conocimiento y las habilidades de los servidores y el software y los programas desarrollados internamente o adquiridos.	**URF**
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red	**MHCP** Son propiedad el Ministerio

Tipo	Descripción	Gobierno
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información.	**URF** En general el personal es vinculado por la Unidad **MHCP** Los procesos de apoyo para gestión de la información y TI (mesa de ayuda) se desarrollan con personal del Ministerio.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la entidad, así como, los sistemas de información y comunicaciones.	**MHCP** Son propiedad el Ministerio
Infraestructura crítica cibernética nacional	Se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.	**No Aplica para la URF**

Tabla 2. Identificación de la autoridad de gestión por tipo de activo.

Una vez asignado el gobierno de cada activo, se debe identificar qué activos de información serán gestionados. El primer paso es crear un inventario de estos activos siguiendo los procedimientos indicados en la siguiente figura:

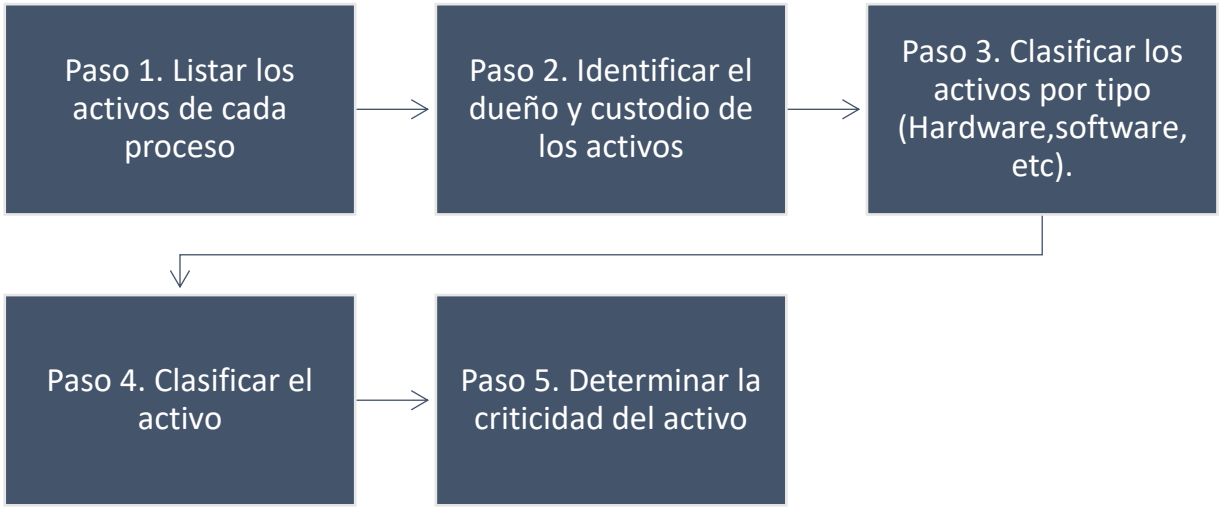


Figura 1. Pasos para la identificación de los activos. Elaboración propia.

En la identificación de activos se deben listar cada uno de los activos de la Entidad por parte de cada líder de proceso, registrando los siguientes datos:

- **Proceso:** proceso institucional al que pertenece el activo de información.
- **Tipo:** tipo de activo de información (Información y datos, sistemas de información y aplicaciones de software, Hardware, soporte para almacenamiento de información, servicios, recursos humanos, instalaciones, redes.
- **Oficina:** área, dependencia o proceso que está identificando el activo de información.
- **Serie documental:** cuando se trate de un activo documental.
- **Subserie documental:** cuando se trate de un activo documental.
- **Nombre:** nombre completo del activo de información.
- **Descripción:** descripción resumida para identificar el activo.
- **Nombre del responsable de producción de la información:** responsable de producir el activo.
- **Fecha de generación de la información:** fecha en la que el activo fue incluido en el inventario.
- **Soporte de registro:** físico, digital.
- **Medio de conservación:** medio en el cual se conserva el activo.
- **Formato:** identifica la forma, tamaño o modo en el que se presenta la información.

- **Idioma:** idioma, lengua o dialecto del activo.

Posteriormente, es necesario clasificar el activo de acuerdo con la propiedad correspondiente (Disponibilidad, integridad y confidencialidad) y proceder con la determinación de criticidad de cada activo, como se presenta a continuación.

4.1.1.Determinar la criticidad de los activos de información

Un activo de información digital es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización. En el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios web, redes, información digital, personal, ubicación, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la Unidad para su funcionamiento.

Como se explicó en el numeral anterior, la identificación de activos debe ser realizada por los líderes de proceso. Posteriormente, es necesario establecer la criticidad del activo, con base en la siguiente escala para los atributos de confidencialidad, integridad y disponibilidad:

Escala valoración activo por aspecto							
Confidencialidad Ley 1712 de 2014			**Integridad**			**Disponibilidad**	
1	Información pública		**1**	Se requiere un bajo grado de exactitud y completitud de la información		**1**	El activo tiene que estar disponible durante el horario laboral entre semana
2	Información clasificada		**2**	Se requiere un mediano grado de exactitud y completitud de la información		**2**	El activo tiene que estar disponible durante el horario laboral entre semana y los sábados
3	Información reservada		**3**	Se requiere un alto grado de exactitud y completitud de la información		**3**	El activo tiene que estar disponible tiempo completo, todos los días y a toda hora 24/7

Escala valoración activo por aspecto	
Escalas de criticidad	
Suma de calificación dada para cada criterio entre 3 a 4	**Bajo**
Resultado calificación entre 5 a 7	**Medio**
Resultado calificación entre 8 a 9	**Alto**

Figura 2. Valoración criticidad de los activos. Elaboración propia.

Posterior a la calificación de cada atributo en los activos de acuerdo con la escala anterior, se suman los puntajes obtenidos para priorizar la intervención de los activos que obtengan un puntaje superior a 7. En consecuencia, se procede con la identificación de riesgos, amenazas, vulnerabilidad y causas inherentes a la seguridad digital.

4.1.2.Identificación de amenazas y vulnerabilidades

Después de la identificación y valoración de los activos de información, se debe asociar el grupo de activos o activos específicos de cada proceso y analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Las amenazas pueden provenir de forma deliberada, fortuita, a través del ambiente o pueden ser dirigidas por el hombre, como guía se consulta la ISO 27000.

La presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza **puede** no requerir la implementación de un control.

Los riesgos inherentes que se podrán identificar corresponden a:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Después de la identificación y análisis de los activos de información, se debe asociar el grupo de activos o activos específicos de cada proceso y analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Las amenazas pueden provenir de forma deliberada, fortuita, a través del ambiente o pueden ser dirigidas por el hombre.

El listado de amenazas y vulnerabilidades pueden consultarse en la guía para la gestión integral del riesgo en entidades públicas, en su versión 7, expedida por el

DAFP. Cada activo de información se puede ver inmerso en uno o varios de los riesgos definidos en dicho documento.

4.1.3.Variables adicionales de identificación

A continuación, se presentan las variables adicionales de identificación para los riesgos de seguridad de la información digital, los cuales integran con las variables de la política general de administración de riesgos:

- **Factor de amenaza de riesgo:** corresponde a las amenazas de deliberadas, fortuitas o ambientales provenientes del entorno. Se debe diligenciar de acuerdo con las amenazas listadas en la guía para la gestión integral del riesgo en entidades públicas, en su versión 7, expedida por el Departamento Administrativo de la Función Pública.
- **Factor de vulnerabilidad del riesgo:** son vulnerabilidades (internas) que pueden detonar la amenaza. Se debe diligenciar de acuerdo con las amenazas listadas en la guía para la gestión integral del riesgo en entidades públicas, en su versión 7, expedida por el Departamento Administrativo de la Función Pública.

- **Causas:** se refiere a nexos causales (causa efecto) propios de la entidad, que impactan al riesgo. Para diligenciar este campo es necesario identificar las causas institucionales propias, adaptándolas a las amenazas, vulnerabilidades y controles listados en la guía para la gestión integral del riesgo en entidades públicas, en su versión 7, expedida por el Departamento Administrativo de la Función Pública.
- **Origen:** el origen puede ser deliberado, fortuito o ambiental, como se explicó en la amenaza del riesgo.

- **Activos críticos:** son cualquier tipo de información digital o recurso relacionado con la gestión de la información que tiene valor para la entidad y que deben protegerse en cuánto a su integridad, disponibilidad y confidencialidad. Es necesario diligenciar este campo de acuerdo con los activos críticos identificados previamente.

- **Nivel de autenticación digital:** se refiere al nivel de confianza en el proceso de autenticación digital que un sistema otorga a un usuario al validar su identidad para acceder a un servicio o recurso digital. Los niveles de confianza se diligencian de acuerdo con la siguiente tabla:

Nivel	Nivel de confianza para la autenticación digital
Bajo	Ofrece un nivel de confianza mínimo en el proceso de autenticación digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es mínimo.
Medio	Ofrece cierto nivel de confianza en el proceso de autenticación digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es moderado.
Alto	Ofrece una gran confianza en el proceso de autenticación digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo alto.
Muy alto	Ofrece más confianza en el proceso de autenticación digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo extremo.

Tabla 3. Niveles de autenticación digital.

4.2. Etapa de análisis

La etapa de análisis de riesgos de seguridad de la información digital se realiza de la misma manera descrita en la política general de administración del riesgo de la Unidad. El análisis se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización el riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. El resultado de los activos críticos influye en el análisis de impacto del riesgo.

4.3. Etapa de Valoración

4.3.1. Valoración de los controles existentes

Una vez identificados y valorados los riesgos inherentes, se procede con la identificación y evaluación de los controles existentes. Los controles estándar definidos se encuentran listados en la guía para la gestión integral del riesgo en entidades públicas, en su versión 7, expedida por el Departamento Administrativo de la Función Pública; sin embargo, también la Entidad puede crear controles adicionales a los listados en el anexo A de la norma ISO 27001:2022 de acuerdo con sus necesidades.

Una vez asociados y valorados los controles, se adapta la descripción de estos, de acuerdo con las condiciones especiales de operación institucional y se debe realizar un plan de implementación de controles, de conformidad con la guía en referencia.

4.4. Etapa de manejo

Para el manejo se aplican las opciones de manejo indicadas en la política de administración de riesgos.

4.5. Fase de monitoreo

Además de lo contemplado en la etapa de monitoreo, se elaboran los siguientes reportes complementarios:

4.5.1.Registro y reporte de incidentes de seguridad de la información

El proceso de gestión de la información debe contar con el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar. El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y con esta información, adoptar nuevos controles. En caso de en encontrar nuevas amenazas o vulnerabilidades, es necesario ajustar los riesgos existentes para adecuarlos a la realidad institucional.

4.5.2.Reporte de la gestión del riesgo de seguridad de la información

El oficial de seguridad de la información, perteneciente al proceso de gestión de la información, debe reportar a la línea estratégica de forma periódica la siguiente información:

- Matriz de los riesgos identificados de seguridad de la información.
- Listado de activos críticos.
- Reporte de criticidad.
- Plan de tratamiento de riesgos.
- Reporte de evolución de riesgos y modificación del riesgo.
- Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de evaluación realizada.
- Impacto económico que podría presentarse frente a la materialización del riesgo.

4.5.3. Reporte de la gestión del riesgo de seguridad de la información a autoridades especiales

Una vez que la URF obtenga los resultados de la gestión de riesgos de seguridad digital, estos deben consolidarse y reportarse a las autoridades designadas por el Gobierno Nacional. Así se podrán identificar oportunidades para crear políticas públicas, fortalecer capacidades o asignar recursos que mejoren la seguridad de la información.

5. Documento referente

Tipo	Nombre
Política	Política de administración del riesgo

6. Datos de elaboración y control de cambios

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
2025-04-30	1.0	TS-0814	Elaboración del documento.
2026-04-20	2.0	TS-1162	Actualización general de la política, de conformidad con la nueva guía para la gestión integral del riesgo en entidades públicas, versión 7, expedida por el DAFP. Se incluyen lineamientos necesarios en la etapa de identificación del riesgo, relacionados con la identificación inicial de activos de información, para su posterior valoración. Además, se adicionan lineamientos en torno a la identificación de mínimo un riesgo independiente por cada atributo de seguridad de la información (Disponibilidad, integridad y confidencialidad), junto con controles estandarizados en la guía para la

			gestión integral del riesgo en entidades públicas, versión 7, expedida por el DAFP. Aunado a lo anterior, se define que, también la Entidad puede crear controles adicionales a los listados en el anexo A de la norma ISO 27001:2022 de acuerdo con sus necesidades, los cuales debe valorarse de conformidad con los criterios de la guía.

Elaboración, revisión y aprobación	
Elaboración	
Nombre:	Franklin González Sierra
Cargo:	Profesional especializado
Revisión	
Nombre:	Juan Stiven Rios Andrade
Cargo:	Asesor
Aprobación	
Nombre:	Comité Institucional de Coordinación de Control Interno
Acta No.	Acta No. 02 de 2026