Superintendencia de Notariado y Registro

Manual General de Gestión del Riesgo

Proceso: Sistema Integrado de Gestión

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código de Formato: SIG – FR – 003 Versión: 2 Fecha Aprobación: 18-Ago-2026

EQUIPO DIRECTIVO:

Joaquín José Méndez Llach
SUPERINTENDENTE DE NOTARIADO Y REGISTRO

Esther Cristina Gómez Melo
SECRETARÍA GENERAL

Nancy Rocío Álvarez Garzón
SUPERINTENDENCIA DELEGADA PARA EL REGISTRO (E)

Cristina María López Vergara
SUPERINTENDENCIA DELEGADA PARA EL NOTARIADO

Yoly Beatriz Illidge Pimienta
SUPERINTENDENCIA DELEGADA PARA LA PROTECCIÓN, RESTITUCIÓN Y FORMALIZACIÓN DE TIERRAS

Consuelo Perdomo Jimenez(E)
DIRECCIÓN TÉCNICA DE REGISTRO

Yolanda Rodríguez Roldán
DIRECCIÓN ADMINISTRATIVA Y FINANCIERA (E)

Carlos Andrés Flórez Sarmiento
DIRECCIÓN DE TALENTO HUMANO (E)

Maikol Alfredo Grandett Gastelbondo
DIRECCIÓN DE CONTRATACIÓN

Adriana Consuelo Jiménez
DIRECCIÓN DE VIGILANCIA Y CONTROL NOTARIAL (E)

Julián Javier Santos de Ávila
DIRECCIÓN DE ADMINISTRACIÓN NOTARIAL (E)

Sandra Patricia Ruiz Moreno
OFICINA ASESORA DE PLANEACIÓN (E)

Yury Lizeth Quintero Calvache
OFICINA ASESORA JURÍDICA (E)

Esther Cristina Gómez Melo
OFICINA DE CONTROL INTERNO DISCIPLINARIO (E)

Jorge Arcecio Cañaveral Rojas

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN (OTI)

Mónica Amatista Jiménez Barros
OFICINA DE CONTROL INTERNO DE GESTIÓN

Leonardo Torres Galán
OFICINA DE ATENCIÓN AL CIUDADANO (E)

María Claudia Araque Araque
SUBDIRECCIÓN DE APOYO JURÍDICO REGISTRAL

Octubre / 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN 8

2. OBJETIVO 8

3. ALCANCE 8

4. ARTICULACIÓN MIPG CON RIESGOS 9

5. METODOLOGÍA PARA LA GESTIÓN DE LOS RIESGOS EN LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO 9

5.1 Establecimiento del Contexto: 10

5.2 Identificación del Riesgo 10

5.3 Análisis de los Objetivos Estratégicos y de los Procesos 11

5.4 Identificación de los Puntos de Riesgo 11

5.5 Identificación de Áreas de Impacto 12

5.6 Identificación de Áreas de Factores de Riesgo 12

5.7 Descripción de los Riesgos 14

5.8 Categoría de los Riesgos 15

5.9 Identificación de los Riesgos Fiscales. 15

5.10 Identificación de los Riesgos Fiscales - Control Interno Contable en el marco de la gestión del riesgo fiscal 18

5.11 Identificación y Descripción de Riesgos para la Integridad Pública 19

5.12 Identificación de Riesgos de Lavado de Activos y Financiación del Terrorismo 20

5.13 Identificación de Riesgos de Seguridad de la Información 21

5.14 Gestión de Activos de seguridad de la Información 21

5.15 Identificación de activos de información. 21

5.16 Clasificación de activos de información 24
5.17 Valoración de criticidad del activo de información 25
5.18 Identificación de Vulnerabilidades de Seguridad de la Información 25
5.19 Valoración del Riesgo 28
5.20 Determinación del Nivel de Probabilidad del Riesgo 28
5.21 Determinación del Nivel de Impacto del Riesgo 28
5.22 Determinación del Riesgo Inherente. 29
5.23 Diseño y Evaluación de Controles 30
5.24 Tipos de Control 30
5.25 Redacción de los Controles 31
5.26 Evaluación del Diseño de Controles. 32
5.27 Desplazamiento del Riesgo en el Mapa de Calor como Resultado de la Aplicación de Controles 34
5.28 Nivel de Riesgo Residual 34
6. TRATAMIENTO DEL RIESGO. 36
6.1 Tipos de Tratamiento al Riesgo 36
6.2 Plan de Tratamiento al Riesgo 37
6.3 Gestión de Eventos de Riesgo. 37
6.4 Riesgos en los Sistemas de Gestión 37
6.5 Mapa de Riesgos de la Entidad. 38
7. BIBLIOGRAFÍA 39
8. DOCUMENTOS ASOCIADOS 39
9. ANEXOS 39

TABLA DE FIGURAS

Figura 1. Pasos para la gestión del riesgo 9
Figura 2. Posibles puntos de impacto. 11
Figura 3. Estructura de redacción del riesgo 14
Figura 4. Estructura de redacción del riesgo de seguridad digital. 27
Figura 5. Estructura de redacción del riesgo de seguridad digital. 29
Figura 6. Desplazamientos de los riesgos en función de los controles 34
Figura 7. Riesgos Residual 34
Figura 8. Resultado riesgos residual 35

TABLA DE TABLAS

Tabla 1. Categorías de Riesgos 15
Tabla 2. Categorías de Riesgos 15
Tabla 3. Estructura redacción riesgos para la integridad excepto LA/FT/FP 20
Tabla 4. Estructura redacción riesgos LA/FT/FP 20
Tabla 5. Activos de Información 22
Tabla 6. Clasificación según ley 1581 De 2014 23
Tabla 7. Clasificación según ley 1712 de 2012 23
Tabla 8. Criterios de clasificación activos 24
Tabla 9. Niveles de valoración criterios de seguridad 24
Tabla 10. Criticidad de activos 25
Tabla 11. Vulnerabilidades Comunes de Seguridad de la Información 25

Tabla 12. Ejemplo de Vulnerabilidades Vs Amenazas.....26

Tabla 13. Ejemplo de Riesgo de Seguridad de la Información 27

Tabla 14. Tabla Niveles de Probabilidad.....28

Tabla 15. Tabla Niveles de Impacto 29

Tabla 16. Tabla Evaluación Diseño de Controles 32

Tabla 17. Ejemplo 1 Evaluación de Controles en el Diseño (Control Preventivo) 33

Tabla 18. Ejemplo 2 Evaluación de Controles en el Diseño (Control Detectivo): 33

1. INTRODUCCIÓN

Para la Superintendencia de Notariado y Registro (SNR) es de primordial importancia asegurar razonablemente el logro de los objetivos estratégicos, así como el de los objetivos de los procesos y de sus sistemas de gestión, para de esta manera cumplir con su misión de ejercer la inspección, vigilancia y control de sus vigilados, por tal motivo ha desarrollado una metodología adecuada a su condición de entidad pública, a las características de los procesos, a la normatividad aplicable y a la naturaleza de las actividades que desarrolla, que le permita identificar, analizar, evaluar y tratar efectivamente los riesgos de gestión del proceso, de corrupción, de seguridad de la información, de Lavado de Activos y Financiación del Terrorismo (LA/FT), fiscal, ambientales, de seguridad y salud en el trabajo.

Esta actualización sigue las orientaciones establecidas por la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 7 expedida por el DAFP e incorpora las orientaciones estratégicas de la alta dirección, articulando los objetivos estratégicos definidos y el modelo de operación de procesos con la planeación institucional.

2. OBJETIVO

El objetivo del presente manual es establecer y formalizar la metodología que será aplicada en la Superintendencia de Notariado y Registro para la administración de los riesgos de gestión, fiscales, de integridad (de corrupción, de fraude, de soborno, de conflictos de interés, de lavado de Activos y Financiación del Terrorismo (LA/FT/FP) y de seguridad de la información, en todas sus etapas tomando como base el análisis del contexto de la entidad. La metodología desarrollada en el presente manual define los detalles para llevar a cabo las actividades de identificación, análisis, evaluación, tratamiento, monitoreo y reporte de los riesgos de la Entidad. Con el desarrollo y documentación de esta metodología se da cumplimiento a lo establecido en la Política Integral de Gestión del Riesgo de la SNR.

3. ALCANCE

El presente Manual General de Gestión Integral del Riesgo, es de obligatoria aplicación para todos los procesos de la Entidad e incluye los aspectos metodológicos asociados con todos los tipos de riesgos a los que está expuesta la entidad.

La metodología definida en el presente manual NO es de obligatoria aplicación por parte de Modelo de Supervisión Enfocada en Riesgos MSER, pues la Oficina Asesora de Planeación no funge como segunda línea de defensa para los vigilados. No obstante, estos lineamientos metodológicos sirven como referencia para el MSER, al momento de desarrollar la metodología propuesta para la administración del riesgo de cara al vigilado.

4. ARTICULACIÓN MIPG CON RIESGOS

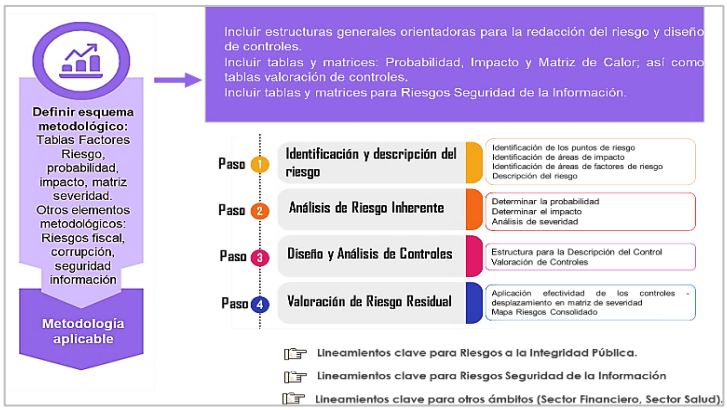
El Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de las Tecnologías de la Información y Comunicaciones desarrollaron la Guía para la Gestión Integral de Riesgos en Entidades Públicas en su versión 7 como una herramienta con un enfoque preventivo que permite a las entidades públicas establecer sus propias directrices para gestionar de manera efectiva sus riesgos de gestión, fiscales, de integridad (de corrupción, de fraude, de soborno, de conflictos de interés, de lavado de Activos y Financiación del Terrorismo (LA/FT/FP) y de seguridad de la información.

En este sentido el presente manual fija las bases metodológicas para la Superintendencia Notariado y Registro y de esta manera se garantice la articulación de la Entidad con las disposiciones que en materia de gestión del riesgo determina el Modelo Integrado de Planeación y Gestión en su manual operativo y lo establecido en la Guía para la Gestión Integral de Riesgos en Entidades Públicas en su versión 7.

5. METODOLOGÍA PARA LA GESTIÓN DE LOS RIESGOS EN LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO

A continuación, se presenta el esquema en donde se ilustran los pasos propuestos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas V7 para la gestión de los riesgos en entidades públicas:

Figura 1. Pasos para la gestión del riesgo



Fuente. Guía de gestión integral del riesgo en entidades públicas V7 DAFP.

5.1 Establecimiento del Contexto:

La Superintendencia de Notariado y Registro desarrollará el análisis del contexto interno y externo como base para la gestión integral del riesgo, considerando factores estratégicos, operacionales, tecnológicos, legales, territoriales, financieros, reputacionales y de integridad pública que puedan afectar el cumplimiento de los objetivos institucionales.

La metodología implementada por la SNR está diseñada para responder a las necesidades particulares de la Entidad y se adapta a las características propias de su estructura orgánica, los procesos y la naturaleza de las actividades que desarrolla para cumplir su misión.

La metodología para la gestión del riesgo está estructurada en la aplicación sistemática de etapas que van desde el establecimiento del contexto hasta las actividades de seguimiento y revisión e informe de los resultados de la gestión.

5.2 Identificación del Riesgo

La identificación de los riesgos consiste en encontrar, reconocer y describir los posibles eventos pueden afectar positiva o negativamente el logro de los objetivos de la entidad, sus procesos, planes o proyectos:

La identificación de los riesgos de gestión se realiza con base en el resultado del análisis de los elementos del contexto interno y externo que pueden tener impacto en el logro de los objetivos de la Entidad; a partir de este análisis se determinan los posibles eventos que pueden afectar negativa o positivamente los objetivos, se establecen sus causas y sus consecuencias potenciales.

En la SNR, la Oficina Asesora de Planeación realizará el acompañamiento metodológico en los ejercicios de identificación de los riesgos de gestión en todos los niveles. El ejercicio de identificación de los riesgos de gestión para los procesos se realiza por parte de los responsables de los procesos y sus equipos (primera línea de defensa) con base en la posible afectación a los objetivos de cada proceso. La primera línea de defensa corresponde a líderes de proceso y sus equipos; la segunda línea de defensa corresponde a las oficinas que tengan un rol asignado por tipologías de riesgo como está definido en la política integral de gestión de riesgos; y la tercera línea de defensa corresponde a la Oficina de Control Interno en ejercicio de evaluación independiente.

Para realizar una correcta identificación de los riesgos en la SNR es necesario llevar a cabo los siguientes pasos:

- Análisis de los Objetivos Estratégicos y de los Procesos.
- Identificación de los puntos de Riesgo.
- Identificación de las áreas de impacto.
- Identificación de las áreas de factores de riesgo.

- Identificación de puntos de riesgo fiscal.

5.3 Análisis de los Objetivos Estratégicos y de los Procesos

Los objetivos estratégicos son la base para la identificación de los riesgos estratégicos que corresponden a los eventos que pueden dificultar o impedir el logro de estos objetivos.

Antes de iniciar la identificación de los riesgos estratégicos, la entidad debe asegurarse a través de los ejercicios de Planeación Estratégica de la alineación de los objetivos estratégicos con la misión y la visión de la entidad, así como de su adecuada formulación, por lo que los objetivos estratégicos son un insumo del proceso de Direccionamiento Estratégico para el ejercicio de la identificación de los riesgos estratégicos.

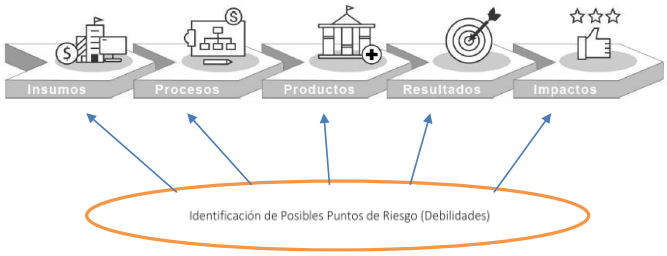
Los objetivos de los procesos establecen el propósito de cada proceso que debe estar alineado con los objetivos estratégicos y por ende con la visión y misión de la entidad. La identificación de los riesgos de los procesos se realiza con base en los posibles eventos que pueden afectar el cumplimiento de los objetivos asociados a estos procesos.

5.4 Identificación de los Puntos de Riesgo

Los puntos de los puntos de riesgo son las actividades dentro del flujo de procesos en donde se pueden presentar eventos de riesgo que pueden afectar el cumplimiento de los objetivos de los procesos.

La identificación de los puntos de riesgo se realiza sobre la cadena de valor del proceso, por lo que la realización de este paso en la SNR se debe realizar con base en los documentos de caracterización de los procesos, en dónde se pueden identificar puntos de riesgo en las entradas, las actividades, las salidas o en los recursos del proceso. Estos puntos de riesgos pueden definirse como debilidades del proceso dentro de un ejercicio de análisis interno, el cual puede sustentarse a partir de un estudio de capacidades del proceso y determinarse como estas debilidades pueden afectar los resultados de los procesos o a los usuarios de estos resultados.

Figura 2. Posibles puntos de impacto.



Fuente. Guía de gestión integral del riesgo en entidades públicas V7 DAFP.

5.5 Identificación de Áreas de Impacto

Las áreas de impacto corresponden a los efectos o consecuencias de la materialización de un evento de riesgo, de acuerdo con lo establecido por la Guía para la Administración del Riesgo y el Diseño de Controles Eficaces versión 7, para las entidades públicas las únicas consecuencias que aplican son las de tipo reputacional y económico (o presupuestal), por lo que al momento de realizar la valoración del riesgo se deben considerar estos dos tipos de afectaciones para determinar los niveles de criticidad del riesgo.

5.6 Identificación de Áreas de Factores de Riesgo

Los factores de riesgo corresponden a las fuentes generadores de los riesgos y factores de, las cuales pueden presentarse como causas de materialización de eventos de riesgos. De acuerdo con la Guía para la Gestión Integral del Riesgos en Entidades Públicas versión 7.

Las fuentes generadoras de riesgos en las entidades públicas pueden ser:

Procesos: Eventos relacionados con errores o fallas en la ejecución de las actividades de los procesos.



Talento Humano: Eventos asociados al desempeño del personal o a sus comportamientos incluyen factores asociados a la seguridad y salud en el trabajo y a actos intencionales frente a situaciones de corrupción



Tecnología: Eventos relacionados con la infraestructura tecnológica de la entidad.



Infraestructura: Eventos relacionados con la infraestructura física de la entidad.



Factores Externos: Son situaciones externas que pueden afectar a la entidad.

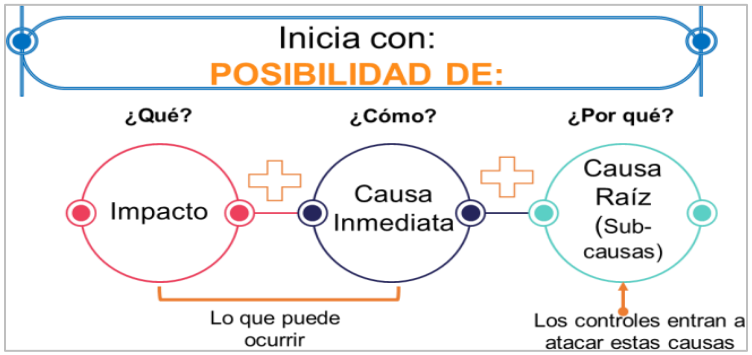


Nota: Durante los ejercicios de análisis y monitoreo que realiza la Entidad a su contexto, se pueden identificar factores o fuentes generadoras de riesgos que no estén incluidas en el listado anterior y las cuales también pueden ser tomadas para la identificación y análisis de los riesgos en la SNR.

5.7 Descripción de los Riesgos

Consiste en detallar las características del riesgo para determinar la información necesaria de manera que se pueda comprender el riesgo por parte del líder del proceso como por otras personas de la entidad o externas a la misma. Por lo anterior la estructura para la descripción de los riesgos en la Entidad es la siguiente:

Figura 3. Estructura de redacción del riesgo



Fuente. Guía de gestión integral del riesgo en entidades públicas V7 DAFP.

Se debe iniciar con las palabras" **Posibilidad de…",** posteriormente se redacta el **Impacto**, la **Causa Inmediata** y las **Causas Raíz.** A continuación, se presenta un ejemplo de redacción de un riesgo de gestión en la SNR:

Ejemplo Redacción Riesgo de Gestión en la SNR

Posibilidad de afectación reputacional por perdida de oportunidad en la atención a las solicitudes y necesidades de los grupos de interés internos y externos debido a debilidades en el seguimiento a los tiempos de las respuestas.

De acuerdo con lo anterior el riesgo puede desglosarse de la siguiente manera para facilitar su análisis:

Impacto: Son las consecuencias para la entidad resultantes de la materialización del riesgo y estas deben establecerse solamente a nivel de la afectación reputacional o presupuestal.

Causa Inmediata: Constituye el evento propio de riesgo que de materializarse puede afectar los objetivos del proceso, programa o proyecto en dónde se presenta o incluso podría llegar a afectar los objetivos institucionales generando los impactos reputacionales o presupuestales referenciados en el punto anterior.

Causa Raíz: Es la causa o causas básicas que en caso de no controlarse pueden originar la materialización del riesgo. Estas causas son las bases para el establecimiento de controles en la etapa de valoración.

5.8 Categoría de los Riesgos

La siguiente tabla muestra las categorías de riesgos propuestas la Guía para la Gestión Integral del Riesgos en Entidades Públicas versión 7 permiten la agrupación y consolidación de los diferentes tipos de riesgos de acuerdo con su naturaleza.

Tabla 1. Categorías de Riesgos

CATEGORIA DEL RIESGO	FACTOR DE RIESGO ASOCIADO	DESCRIPCIÓN
Ejecución y Administración de Procesos	Procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude Externo	Evento Externo	Pérdidas derivadas de actos de fraude por persona ajenas a la entidad
Fraude Interno	Talento Humano	Pérdida debido a actos de fraude, actos irregulares, comisión de hechos delictivos, abuso de confianza, aprobación indebida, incumplimiento de regulaciones legales o internas de la entidad, en dónde hay participación de servidores o funcionarios de la SNR.
Fallas Tecnológicas	Tecnología	Errores de hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones Laborales	Factores Varios	Pérdidas originadas de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, Productos y Prácticas Organizacionales	Factores Varios	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a estos.
Daños Activos Físicos	Infraestructura Evento Externos	Pérdida por daños o extravío de los activos físicos por desastres naturales u otros eventos.

Fuente. Guía de gestión integral del riesgo en entidades públicas V7 DAFP.

5.9 Identificación de los Riesgos Fiscales.

La identificación de riesgo fiscal se basa en el establecimiento de puntos de riesgos fiscales los cuales se pueden presentar en los diferentes procesos de la entidad y que corresponden a las actividades donde se gestionan o manejan recursos y bienes públicos y que por ende puedan generar eventos de pérdida o detrimento de estos.

A continuación, se presenta una tabla con los posibles puntos de riesgo fiscal en la Superintendencia de Notariado y Registro.

Tabla 2. Categorías de Riesgos

Referencia	Puntos de Riesgo Fiscal	Circunstancia Inmediata
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron
19	Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual

Referencia	Puntos de Riesgo Fiscal	Circunstancia Inmediata
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, fallas y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Fallas en la ejecución
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)

Referencia	Puntos de Riesgo Fiscal	Circunstancia Inmediata
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Fuente. Elaboración propia Oficina Asesora de Planeación.

Redacción del Riesgo Fiscal:

Para redactar un riesgo fiscal se debe tener en cuenta:

Iniciar con la oración: Posibilidad de, debido a que es un evento potencial

Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada.

5.10 Identificación de los Riesgos Fiscales - Control Interno Contable en el marco de la gestión del riesgo fiscal

En el marco de la Resolución 347 de 2025 de la Contaduría General de la Nación, la identificación de riesgos fiscales deberá incorporar el análisis del Control Interno Contable como fuente transversal de riesgos asociados a la generación, reconocimiento, medición, revelación y presentación de la información financiera institucional.

Para tal efecto, la Dirección Administrativa y Financiera, en articulación con la Oficina Asesora de Planeación y las áreas proveedoras de información contable, identificará los procesos, procedimientos, sistemas de información y dependencias que intervienen en la producción de hechos económicos susceptibles de afectar la razonabilidad de los estados financieros.

En este análisis se priorizarán especialmente:

- Los procesos relacionados con la gestión de ingresos institucionales,
- Las conciliaciones contables y financieras,
- La consistencia entre sistemas fuente de información,
- La oportunidad en el reporte de información financiera,
- La trazabilidad de soportes contables,
- La interoperabilidad entre sistemas administrativos y financieros

Como resultado de este ejercicio se deberán identificar riesgos contables potenciales, evaluar la efectividad de los controles existentes y definir acciones de fortalecimiento orientadas a prevenir diferencias contables, errores de reconocimiento, registros extemporáneos o inconsistencias en la información financiera reportada por la Entidad.

5.11 Identificación y Descripción de Riesgos para la Integridad Pública

De acuerdo con la Guía de Gestión Integral del Riesgo para entidades públicas v7 que establece que: “En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, las entidades deberán identificar y valorar los riesgos que pueden impactar el ejercicio íntegro de la función pública, incluidos los riesgos de LA/FT/FP. La Corrupción es la principal amenaza para la integridad, sin embargo, hay manifestaciones muy específicas de esta práctica que requieren ser identificadas y valoradas individualmente, como lo es el soborno, el fraude y la inadecuada gestión del conflicto de intereses. También, los riesgos por conductas que permiten o favorecen el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva, deben ser gestionados”. La SNR debe realizar la identificación y descripción de los riesgos para la integridad (corrupción, fraude, soborno, conflictos de interés y LA/FT/FP) de la misma manera que se hace para los riesgos de gestión, estableciendo el impacto, causa inmediata y causa raíz.

No obstante, y dadas las características especiales estos riesgos, la redacción de estos debe atender la estructura propuesta de acuerdo con cada tipo de riesgo para la integridad como se muestra en las siguientes tablas:

Tabla 3. Estructura redacción riesgos para la integridad excepto LA/FT/FP

Impacto	Causa Inmediata		Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	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 […]".	
	Soborno Saliente	Ofrecer, prometer o dar 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 […]"	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere 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	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	

Fuente. Elaboración propia Oficina Asesora de Planeación.

En el caso particular del riesgo LA/FT/FP, debe hacerse referencia particularmente a las actividades del flujo de procesos en que existe la vulnerabilidad o exposición al riesgo, como se explica en la siguiente tabla:

Tabla 4. Estructura redacción riesgos LA/FT/FP

Impacto	Causa Inmediata	Causa Raíz
Económico, Reputacional, Legal, Operativo o de Contagio	Usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva.	Descripción de la Operación o Transacción

Fuente. Elaboración propia Oficina Asesora de Planeación.

Los resultados de la identificación de los riesgos de corrupción se registran en la matriz de riesgos de corrupción de la entidad.

5.12 Identificación de Riesgos de Lavado de Activos y Financiación del Terrorismo

Teniendo en cuenta que los riesgos de LA/FT se les aplica el mismo tratamiento que a los riesgos de corrupción, la identificación del mismo se realiza de la misma manera que para los riesgos de corrupción teniendo en cuenta que, para que un riesgo sea considerado de LA/FT, implica aspectos éticos y de

comportamiento de personas que de manera intencional buscan a través de las actividades que desarrolla la SNR dar apariencia de legalidad de recursos económicos vinculados al lavado de activos o a la financiación del terrorismo o que busquen ocultar el origen ilícito de los fondos para presentarlos como legítimos.

5.13 Identificación de Riesgos de Seguridad de la Información

Para realizar la identificación de los riesgos de seguridad de la información es necesario primero realizar la identificación de los activos de seguridad de la información entendiendo por estos los elementos que utiliza la Entidad para funcionar en el entorno físico o digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, entre otros.

Después se procederá a valorar el activo determinando la importancia de los mismos en el logro de los objetivos de los procesos y de la Entidad y bajo este criterio se establece la criticidad y los controles adecuados para su protección.

Para cada activo evaluado como crítico se identificarán los riesgos de seguridad de la Información, estos pueden ser de tres tipos según al atributo de la seguridad de la Información que impacte:

a. Afectación de la Confidencialidad
b. Afectación de la Integridad
c. Afectación de la Disponibilidad

Posteriormente a la identificación de los riesgos de Seguridad de la Información para cada activo, se agrupan los activos por tipo de riesgo para realizar el análisis de las amenazas y vulnerabilidades que podrían causar su materialización.

5.14 Gestión de Activos de seguridad de la Información

La identificación y valoración de activos de información debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo un ejercicio orientado por el responsable de seguridad de la información de la Entidad con el acompañamiento de la Oficina Asesora de Planeación como segunda línea de defensa para la gestión del riesgo. Para realizar una gestión adecuada de activos, se debe realizar las siguientes actividades:

5.15 Identificación de activos de información.

Cada proceso de la entidad debe realizar identificación de sus activos de seguridad de la información, esta actividad es responsabilidad de la Primera Línea de Defensa, que corresponde a los Líderes de Proceso.

Para asegurar una identificación de activos de información de manera organizada y estandarizada, se emplearán los siguientes campos estándar para documentar cada activo. A continuación, se presenta una descripción detallada de cada uno de ellos:

- **Proceso:** Nombre del proceso al que pertenece el activo.
- **ID Activo:** Número consecutivo único que identifica al activo en el inventario.
- **Nombre del activo:** Identificación formal del activo de información.
- **Descripción:** Detalle que explica qué es el activo y su propósito.
- **Tipo de activo:** Los activos de información pueden ser clasificados en diferentes tipos de acuerdo con su naturaleza. En la siguiente tabla se presenta la clasificación de los tipos de activos de seguridad de la información.

Tabla 5. Activos de Información

TIPO DE ACTIVO	DESCRIPCIÓN
DATOS / INFORMACIÓN	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
SOFTWARE	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
HARDWARE	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
SERVICIOS	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
COMPONENTES DE RED	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
PERSONAS	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
INFRAESTRUCTURA	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la entidad

Fuente. Elaboración propia Oficina Asesora de Planeación.

- **Ubicación:** Dónde se encuentra el activo, ya sea físicamente o en el entorno virtual.
- **Propietario (responsable):** Parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente.
- **Custodio:** Parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. Pueden darse las siguientes opciones:

- Para sistemas de información o información consignada o respaldada en ellos, generalmente es la Oficina de Tecnología de la Información y las Comunicaciones.
- Para la información física, los custodios pueden ser los mismos funcionarios del proceso o el grupo de archivo o correspondencia, el custodio generalmente se define según donde reposa el activo original.

- Usuario: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.
- ¿Contiene Datos Personales/Sensibles?: Indicar si de acuerdo con la Ley 1581 de 2012 el activo contiene datos personales o sensibles.

Tabla 6. Clasificación según ley 1581 De 2014

¿CONTIENE DATOS PERSONALES/SENSIBLES?	DESCRIPCIÓN
SI	El activo de información maneja datos personales o sensibles. (Nombres, Cédulas, Números Telefónicos, Celulares, Etnia, Orientación Sexual, Género entre otros).
NO	El activo de información maneja otros tipos de datos, no relacionados con datos personales o datos sensibles.

Fuente. Elaboración propia Oficina Asesora de Planeación.

- **Clasificación de la información:** Indicar el activo de información que tipo de información maneja con base a los 3 tipos mencionados en la ley 1712 de 2014 (Información Pública, Información Clasificada o Información Reservada).

Tabla 7. Clasificación según ley 1712 de 2012

TIPO DE INFORMACIÓN	DESCRIPCIÓN
INFORMACIÓN RESERVADA	Información que es exceptuada de acceso por daño a intereses públicos, que en caso de ser conocida por terceros sin autorización puede conllevar a un impacto negativo de índole legal, operativo, de pérdida de imagen o económico. En este nivel se debe incluir la información de datos personales o sensibles de los ciudadanos.
INFORMACIÓN CLASIFICADA	Información que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias, o que su acceso por terceros sin autorización del propietario puede conllevar a un impacto negativo para los procesos de la entidad.
INFORMACIÓN PÚBLICA	La información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad sin que esto implique daños a terceros ni a las actividad y procesos de la entidad.

Fuente. Elaboración propia Oficina Asesora de Planeación.

5.16 Clasificación de activos de información

La clasificación de activos de información tiene como objetivo, asegurar que la información reciba los niveles de protección adecuados. Esto se basa en su valor y otras características específicas que requieren un manejo especial.

La clasificación de los activos se realizará en función de los tres criterios principales de la seguridad de la información: confidencialidad, integridad y disponibilidad. A continuación, se presenta una definición de cada criterio para tener en cuenta al clasificar los activos respecto a cada uno y sus escalas:

Tabla 8. Criterios de clasificación activos

CRITERIO	DESCRIPCIÓN
Confidencialidad	Define los roles, colaboradores, procesos o grupos de interés a los que la Superintendencia de Notariado y Registro permite el acceso al activo de información, y evalúa el impacto que tendría el incumplimiento de esta condición.
Integridad	Determina el efecto de la modificación no autorizada de los datos del activo de información, el impacto que tendría en los procesos donde está involucrado y las consecuencias para la Superintendencia de Notariado y Registro.
Disponibilidad	Determina el efecto que se produce en la Superintendencia de Notariado y Registro cuando el activo de información no está disponible cuando se necesita. Esto se establece según el tiempo que se puede esperar para que dicho activo esté accesible y pueda ser utilizado.

Fuente. Elaboración propia Oficina Asesora de Planeación.

Respecto a los tres criterios de seguridad de la información, se definirán tres escalas que permitan valorar el activo frente a sus impactos, para así lograr establecer un valor de criticidad específico para cada activo de información dentro del proceso. En este sentido se define el impacto para los diferentes criterios con respecto a los siguientes niveles:

Tabla 9. Niveles de valoración criterios de seguridad

VALOR	NIVEL	DESCRIPCIÓN
3	ALTA	La afectación del criterio conlleva un impacto negativo de índole legal o económica, retrasar sus funciones, detener la operación total de la entidad, y generar pérdidas de imagen severas a la entidad o entes externos.
2	MEDIA	La afectación del criterio puede conllevar un impacto negativo de índole legal o económica, retrasar funciones o detener parcialmente el proceso, o generar pérdida de imagen moderado de la entidad o entes externos.

VALOR	NIVEL	DESCRIPCIÓN
1	BAJA	La afectación del criterio conlleva un impacto no significativo o reducido, puede conllevar afectar la operación normal de la entidad o entes externos, sin implicaciones legales, económicas o de pérdida de imagen.

Fuente. Elaboración propia Oficina Asesora de Planeación.

5.17 Valoración de criticidad del activo de información

La valoración de los activos de información busca determinar la importancia o criticidad de cada activo dentro del proceso. La valoración se llevará a cabo sumando el valor del nivel definido para los criterios de confidencialidad, integridad y disponibilidad.

Tabla 10. Criticidad de activos

CRITICIDAD	ESCALA
ALTA	Si la sumatoria de las clasificaciones dadas para Confidencialidad, Integridad y Disponibilidad da un valor entre 7 y 9.
MEDIA	Si la sumatoria de las clasificaciones dadas para Confidencialidad, Integridad y Disponibilidad da un valor entre 4 y 6
BAJA	Si la sumatoria de las clasificaciones dadas para Confidencialidad, Integridad y Disponibilidad da un valor entre 1 y 3

Fuente. Elaboración propia Oficina Asesora de Planeación.

Los activos con grados de criticidad ALTA y MEDIA serán sujetos a un posterior análisis de riesgos de seguridad digital (o de la información).

5.18 Identificación de Vulnerabilidades de Seguridad de la Información

Las vulnerabilidades se entienden como las debilidades en los activos de seguridad de la Información o en su administración lo que incrementa el grado de exposición ante las posibles amenazas facilitando de esta manera la materialización de los riesgos.

Tabla 11. Vulnerabilidades Comunes de Seguridad de la Información

TIPO	VULNERABILIDADES
HARDWARE	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada

TIPO	VULNERABILIDADES
SOFTWARE	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
RED	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
PERSONAL	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
INFRAESTRUCTURA	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas

Fuente. Elaboración propia Oficina Asesora de Planeación.

Nota: 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**.**

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tabla 12. Ejemplo de Vulnerabilidades Vs Amenazas

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Almacenamiento de medios sin protección	Hurto de medios o documentos
SOFTWARE	Ausencia de parches de seguridad	Abuso de los derechos
RED	Líneas de comunicación sin protección	Escucha encubierta
INFORMACIÓN	Falta de controles de acceso físico	Hurto de información
PERSONAL	Falta de capacitación en las herramientas	Error en el uso
ORGANIZACIÓN	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente. Elaboración propia Oficina Asesora de Planeación.

A continuación, se presenta un ejemplo de Identificación de riesgos de seguridad de la información.

Tabla 13. Ejemplo de Riesgo de Seguridad de la Información

ACTIVO	RIESGO	DESCRIPCIÓN	TIPO	CAUSAS		CONSECUENCIAS
				Amenazas	Vulnerabilidades	
Base de datos de nómina	Pérdida de la integridad	Posibilidad de pérdida de la integridad por la falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada de la base de datos de nómina.	S.I.	Modificación no autorizada	Falta de políticas de Seguridad digital Ausencia de políticas de control de acceso Contraseñas sin protección Autenticación débil	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización de riesgos (legales, económicos, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.

Fuente. Elaboración propia Oficina Asesora de Planeación.

Los riesgos de seguridad de la información se basan en la afectación de tres principios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”.

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización; las cuales son denominadas como “causas” en la identificación de los riesgos de gestión y de corrupción.

Redacción de la descripción del riesgo de la Información

Se debe tener en cuenta una redacción adecuada de los riesgos de seguridad de la información. Con base al ejemplo anterior en la columna 3, la descripción del riesgo maneja la siguiente estructura, para que sea aplicada de manera uniforme en los procesos:

Figura 4. Estructura de redacción del riesgo de seguridad digital.



Fuente. Elaboración propia Oficina Asesora de Planeación.

5.19 Valoración del Riesgo

Esta etapa consiste en comprender la naturaleza y el nivel del riesgo, lo anterior permite conocer el perfil de riesgo de la SNR en términos de criticidad, así mismo permite establecer prioridades para intervenir los riesgos. Para tal fin es necesario determinar el nivel de riesgo el cual resulta de analizar el nivel de probabilidad de ocurrencia y el nivel de impacto o consecuencias de cada riesgo identificado, con el fin de estimar la zona de riesgo inicial o (RIESGO INHERENTE), lo cual indica que se trata del nivel de riesgo sin aplicación de controles.

5.20 Determinación del Nivel de Probabilidad del Riesgo

Consiste en evaluar de la manera más objetiva posible que tan expuesta esta la Entidad frente al riesgo que se está analizando. Para efectos del cálculo del nivel de probabilidad y para evitar la subjetividad en el ejercicio, el nivel de probabilidad se determinará considerando el número de veces que se realiza la actividad en dónde se presenta el riesgo durante un periodo de un año. De acuerdo con lo anterior em la siguiente tabla se presentan los criterios para determinar el nivel de probabilidad de los riesgos.

Tabla 14. Tabla Niveles de Probabilidad

Nivel de Probabilidad	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo dos veces al año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta de 501 a 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces al año	100%

Fuente. Elaboración propia Oficina Asesora de Planeación.

5.21 Determinación del Nivel de Impacto del Riesgo

Consiste en estimar de la manera más objetiva posible los efectos en caso de que el riesgo se materialice. Para determinar el nivel de impacto se deben considerar las consecuencias relacionadas para cada riesgo en la etapa de identificación las cuales están definidas en función de la afectación reputacional o presupuestal para que con base en ellas se establezca el nivel de afectación que representa la materialización del riesgo para la Entidad.

De acuerdo con lo anterior em la siguiente tabla se presentan los criterios para determinar el nivel de impacto de los riesgos.

Tabla 15. Tabla Niveles de Impacto

Nivel de Impacto	Afectación económica	Afectación Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de un área de la entidad
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente.
Moderado 60%	Entre 51 y 100 SMLMV	El riesgo afecta la imagen de la entidad externamente con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 101 y 500 SMLMV	El riesgo afecta la imagen de la entidad externamente con efecto publicitario negativo a nivel del sector trabajo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional con efecto publicitario negativo sostenido

Fuente. Elaboración propia Oficina Asesora de Planeación.

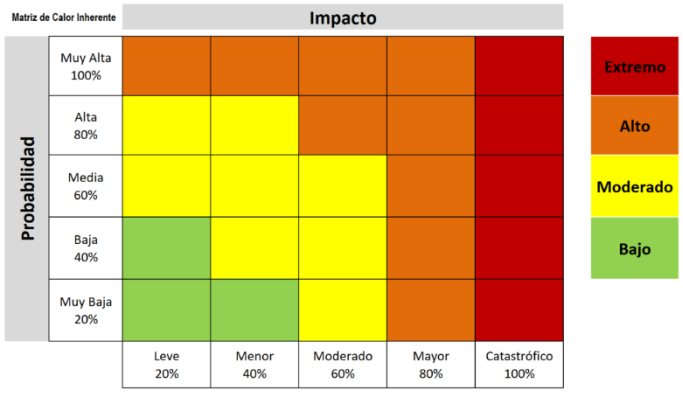
Nota: Con el propósito de minimizar el grado de subjetividad al momento de estimar los niveles de probabilidad e impacto en los ejercicios de análisis de riesgos, es necesario la utilización de fuentes de información confiables basadas en datos históricos, estadísticas de los procesos o el uso de bases confiables para la realización de proyecciones en caso de que sea necesario.

5.22 Determinación del Riesgo Inherente.

El nivel de riesgo inherente es el resultado de analizar el nivel de probabilidad y el nivel de impacto. El nivel de riesgo inherente permite ubicar la Zona de Riesgo Inherente para cada riesgo, es decir la ubicación del riesgo en el mapa de calor de riesgos de la entidad, antes de la aplicación de controles.

De esta manera se puede establecer cuales riesgos se pueden aceptar y cuales necesitan la implementación de controles u otras medidas de tratamiento para mitigarlos. A este ejercicio se le conoce como evaluación del riesgo que es la siguiente etapa en la gestión del riesgo en la SNR.

Figura 5. Estructura de redacción del riesgo de seguridad digital.



5.23 Diseño y Evaluación de Controles

Los controles hacen referencia a las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Los controles se estandarizan y despliegan a través de la información documentada de la entidad sin embargo un documento como una política, un manual o un procedimiento no son por sí solo un control.

Los controles por sí solos permiten prevenir la materialización del riesgo o mitigar los posibles impactos, por lo que actividades como sensibilizaciones, capacitaciones o acompañamientos no se consideran actividades de control.

Los controles están asociados a actividades como validaciones, verificaciones, seguimientos, chequeos, activación de planes de contingencia, activación planes de continuidad, ejecución de pólizas entre otros.

La identificación y aplicación de controles para la prevención y mitigación de los riesgos es responsabilidad de los líderes de los procesos en conjunto con sus equipos (primera línea de defensa, este ejercicio de identificación y diseño de controles debe estar acompañado desde la Oficina Asesora de Planeación (segunda línea de defensa).

Es responsabilidad de la tercera línea de defensa evaluar los controles en su efectividad.

5.24 Tipos de Control

Los controles se pueden clasificar mediante dos grandes criterios: de acuerdo con su propósito y de acuerdo con su forma de ejecución.

De acuerdo con su propósito, los controles se clasifican en tres tipos:

Los Controles Preventivos: Son los controles que están diseñados para evitar la materialización de un riesgo que pueda afectar el cumplimiento de los objetivos.

Los controles preventivos deben atacar las causas del riesgo, por lo que cada causa debe tener asociado al menos un control.

Los controles preventivos permiten disminuir el nivel de probabilidad del riesgo.

Ejemplo: La revisión que hace el supervisor del contrato para evitar que se presente un posible incumplimiento de las obligaciones contractuales por parte del contratista.

Los Controles Detectivos: Son los controles que están diseñados para detectar una posible materialización de un riesgo.

Al permitir la detección oportuna antes de la materialización de un riesgo, estos controles pueden evitar la materialización del mismo, pero generan reprocesos. Estos controles disminuyen la probabilidad del riesgo.

Ejemplo: Las conciliaciones que se realizan para detectar inconsistencias en la información contable o financiera antes de emitir informes financieros.

Los Controles Correctivos: Estos controles corresponden a acciones que se ejecutan después de que un riesgo se materializa.

Estos controles disminuyen el nivel de impacto de los riesgos.

Ejemplo: Las pólizas de cumplimiento que se aplican en los casos en los que se materializa el incumplimiento de un contrato y que busca mitigar el impacto económico del incumplimiento.

De acuerdo con forma de ejecución:

Los Controles Manuales: Estas actividades de control son ejecutadas directamente por los servidores de la entidad.

Ejemplo: La supervisión de la ejecución de un contrato por parte del respectivo supervisor del contrato.

Los Controles Automáticos: El control se aplica mediante un aplicativo o un sistema de información de manera automática.

Ejemplo: Conciliaciones contables automáticas realizadas por el aplicativo contable y que arroja errores que deben ser corregidos.

5.25 Redacción de los Controles

Responsable de ejecutar el Control: Se relaciona el cargo del servidor que realiza la actividad de control, en caso de que se trate de un control automático se identifica el sistema que ejecuta el control.

Acción: A través de los verbos apropiados se describe la actividad que se realiza para la ejecución del control.

Complemento: Se describe la información relevante que permita entender el propósito del control.

A continuación, se presenta un ejemplo de la redacción de un control bajo la estructura propuesta:

Ejemplo:

Riesgo:

Posibilidad de afectación reputacional por inoportunidad en la atención y respuesta a las PQRS debido a demoras en la clasificación, asignación y revisión de las mismas.

Control:

El profesional especializado, monitorea la oportuna asignación y respuesta de las PQRS a través de la matriz de control de PQRS y genera alertas tempranas a los responsables en caso de encontrar posibles demoras.

5.26 Evaluación del Diseño de Controles.

Los criterios para la evaluación del diseño de controles se han estructurado a través de una lista de verificación que permite validar si los controles que la entidad aplica son fuertes o débiles en diseño.

A su vez esta lista de verificación será tomada como base por la tercera línea de defensa para evaluar la efectividad de los controles en su aplicación por parte de la primera línea de defensa.

A continuación, se presenta el instrumento de validación establecido como lista de verificación de validación de controles en el diseño.

Tabla 16. Tabla Evaluación Diseño de Controles

Atributo	Tipo / característica	Descripción	Peso
Eficiencia	Preventivo	Atacan las causas, disminuye la probabilidad de materialización del riesgo	25%
Eficiencia	Detectivo	Detecta una posible materialización antes d que esta ocurra y devuelve el proceso, disminuye probabilidad	15%
Eficiencia	Correctivo	Permiten disminuir el impacto generado por la materialización de un riesgo	10%
Eficiencia	Automático	El control se aplica mediante un aplicativo o un sistema de información de manera automática.	25%
Eficiencia	Manual	Estas actividades de control son ejecutadas directamente por los servidores de la entidad. Por lo cual tiene implícito el error humano	15%
Informativo	Documentado	Las actividades de control están documentadas en procedimientos, manuales o cualquier otro documento propio del proceso	No aplica
Informativo	Sin Documentar	Las actividades de control se ejecutan, pero no están documentadas en ningún documento del proceso	No aplica
Informativo	Frecuencia Aleatoria	El control se aplica de manera aleatoria en la actividad que genera el riesgo	No aplica
Informativo	Frecuencia Continua	El control se aplica siempre que se ejecuta la actividad	No aplica
Informativo	Evidencia con registro	El control deja un registro que permite evidenciar su ejecución	No aplica

Atributo	Tipo / característica	Descripción	Peso
Informativo	Sin registro de evidencia	El control no deja registro de su ejecución	No aplica

Fuente. Elaboración propia Oficina Asesora de Planeación

Nota: Los atributos informativos le dan formalidad al control y permiten un mejor conocimiento de este, pero no influyen de manera directa en su efectividad.

Tabla 17. Ejemplo 1 Evaluación de Controles en el Diseño (Control Preventivo)

Control	Atributo	Característica	Peso
El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Propósito	Preventivo	25%
	Implementación	Manual	15%
	Documentación	Documentado	NA
	Frecuencia	Continua	NA
	Evidencia	Con Registro	NA
Total, Valoración del Control			40%

Fuente. Elaboración propia Oficina Asesora de Planeación

Tabla 18. Ejemplo 2 Evaluación de Controles en el Diseño (Control Detectivo):

Control	Atributo	Característica	Peso
El Director de Contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado, y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado.	Propósito	Detectivo	15%
	Implementación	Manual	15%
	Documentación	Documentado	NA
	Frecuencia	Continua	NA
	Evidencia	Con Registro	NA
Total, Valoración del Control			30%

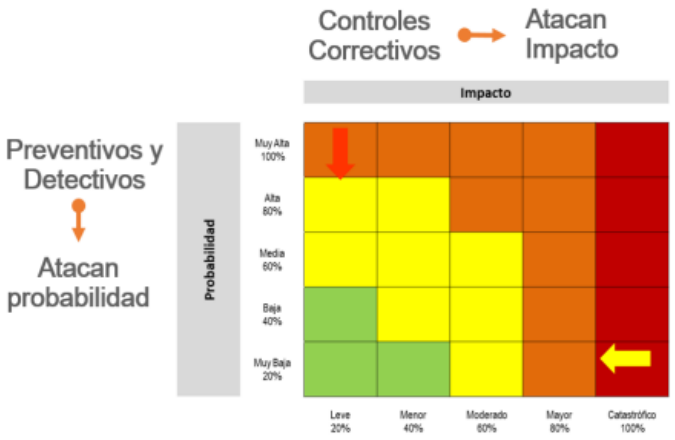
Fuente. Elaboración propia Oficina Asesora de Planeación

5.27 Desplazamiento del Riesgo en el Mapa de Calor como Resultado de la Aplicación de Controles

El peso (%) resultante de la evaluación del control en su diseño, es el que permitirá el desplazamiento del riesgo en el mapa de calor de las zonas de mayor severidad a zonas de calor menos severas de acuerdo con los criterios de evaluación del riesgo de la SNR.

El máximo peso que puede alcanzar un control es del 50% cuando se trata de un control de tipo preventivo y este se ejecuta de manera automática.

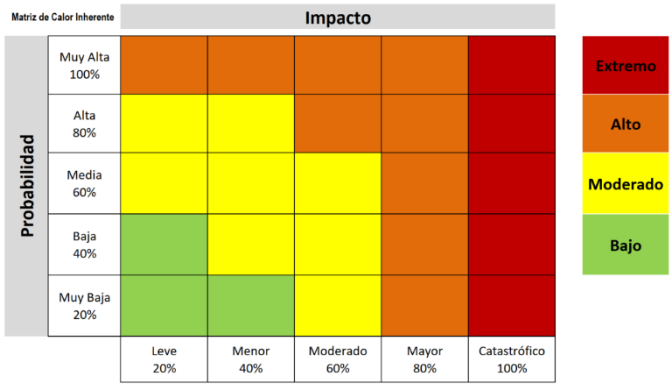
Figura 6. Desplazamientos de los riesgos en función de los controles



Fuente. Guía de gestión integral del riesgo en entidades públicas V7 DAFP

5.28 Nivel de Riesgo Residual

Figura 7. Riesgos Residual



Fuente. Guía de gestión integral del riesgo en entidades públicas V7 DAFP

Es el nivel de riesgo resultante después de la aplicación de controles una vez se evalúan los mismos con base en los atributos de eficiencia para cada control.

A partir de la evaluación de los controles preventivos y detectivos se disminuye la probabilidad del riesgo y a partir de los controles correctivos se disminuye su impacto.

Para la evaluación de los controles es importante tener en cuenta que los mismos mitigan los riesgos de manera acumulativa.

El nivel de riesgo residual resulta de restar el resultado de evaluación de los controles del nivel de riesgo inherente.

Figura 8. Resultado riesgos residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2º control				36%
	Valoración control 2 detectivo			30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual				25,2%
	Valoración de Impacto				
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual				80%

Fuente. Guía de gestión integral del riesgo en entidades públicas V7 DAFP.

La fórmula para el cálculo del riesgo residual es la siguiente:

R residual = R Inherente - (R Inherente *% eficiencia de los controles)

6. TRATAMIENTO DEL RIESGO.

Es la respuesta establecida por la primera línea de defensa (ver Política Integral de Gestión del Riesgo) para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

Esta respuesta corresponde a la decisión que se toma frente a un determinado nivel de riesgo. El análisis para la toma de las decisiones se realiza tomando como base el nivel de riesgo residual a excepción de cuando el análisis se realiza sobre procesos nuevos, frente a lo cual el análisis se realiza con base en el nivel de riesgo inherente.

Los criterios de tratamiento del riesgo están enmarcados en las directrices definidas de Apetito al Riesgo, Tolerancia al Riesgo y Capacidad del Riesgo, establecidas en la Política Integral de Gestión del Riesgo de la SNR.

6.1 Tipos de Tratamiento al Riesgo

Los tratamientos del riesgo en la SNR pueden ser de diferentes tipos de acuerdo con su finalidad:

Aceptar el Riesgo: Bajo decisión informada y después de realizar el análisis del riesgo el responsable del proceso decide no intervenir el riesgo, aun cuando el riesgo supere los niveles de apetito y tolerancia al riesgo definidos en la Política Integral de Gestión del Riesgo, asumiendo los posibles efectos en caso de que el riesgo se materialice. Esta decisión debe quedar registrada en el mapa de riesgos de la entidad. Para el caso de los riesgos estratégicos esta decisión debe ser tomada por el Comité Institucional de Gestión y Desempeño.

Reducir el riesgo: Después de realizar el análisis del riesgo considerando los niveles de apetito y tolerancia al riesgo para la Entidad, el responsable del proceso puede adoptar dos medidas para reducir el nivel del riesgo mediante acciones para mitigar o transferir el riesgo de la siguiente manera:

- **Mitigar el riesgo**: Consiste en tomar acciones para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general, aunque no necesariamente conlleva a la implementación de controles.

- **Compartir el riesgo**: Consiste en reducir la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Puede darse a través del establecimiento de pólizas o subcontratación

- **Evitar el riesgo**: Como resultado del análisis del riesgo por parte del responsable del proceso se decide abandonar la actividad generadora del riesgo, considerando los efectos potenciales de la materialización del mismo, así como los efectos de no continuar realizando la actividad generadora. Esta decisión debe quedar registrada en el mapa de riesgos de la entidad.

6.2 Plan de Tratamiento al Riesgo

Para los tratamientos relacionados con reducir el riesgo se debe establecer un plan de tratamiento en dónde se especifiquen las acciones a realizar, el responsable, fecha de implementación y fecha de seguimiento.

La Oficina Asesora de Planeación, en articulación con los líderes de proceso y la Oficina de Control Interno, realizará actividades periódicas de monitoreo y seguimiento a los riesgos institucionales, controles y planes de tratamiento definidos en la Entidad de conformidad con lo establecido en la política y las responsabilidades de las líneas de defensa.

6.3 Gestión de Eventos de Riesgo.

Un evento de riesgo corresponde a un riesgo materializado. Con el objetivo de tener una base histórica de eventos, la Entidad debe registrar los posibles eventos de riesgo en donde se plasman las situaciones o incidentes que se han presentado y que generan o pueden generar pérdidas económicas o afectaciones a la reputación de la entidad. Se debe establecer si la situación presentada realmente corresponde a un riesgo materializado y de ser así se deben establecer las posibles fallas en los controles. En caso de que la situación presentada no tenga asociado un riesgo previamente identificado en el mapa de riesgos de la entidad, se debe proceder a su identificación y análisis en el mapa de riesgos de la entidad.

El registro de eventos de riesgos se debe realizar en el formato establecido para tal fin en la SNR por la Oficina Asesora de Planeación.

Algunas fuentes para identificar posibles eventos de riesgos son:

- Las PQRS
- Mesas de Ayuda.
- Resultados de auditorías internas y externas.
- Seguimiento a planes, procesos y proyectos.
- Oficina Jurídica
- Líneas internas de denuncia.

El registro de eventos de riesgos debe ser realizado por el responsable del proceso donde se presenta la situación y en caso de determinarse que se trata de una materialización de un riesgo, debe reportarse la Oficina de Control Interno para su seguimiento.

6.4 Riesgos en los Sistemas de Gestión

La metodología descrita en este manual también aplica para los riesgos de gestión de los sistemas de gestión de la SNR, es decir a los posibles eventos que puedan afectar el logro de los objetivos de los diferentes sistemas de gestión, como el sistema de gestión de la calidad, ambiental y seguridad y salud en el trabajo.

Es necesario precisar que cada sistema de gestión una metodología propia para abordar sus riesgos operacionales que a su vez son diferentes a los de gestión a saber:

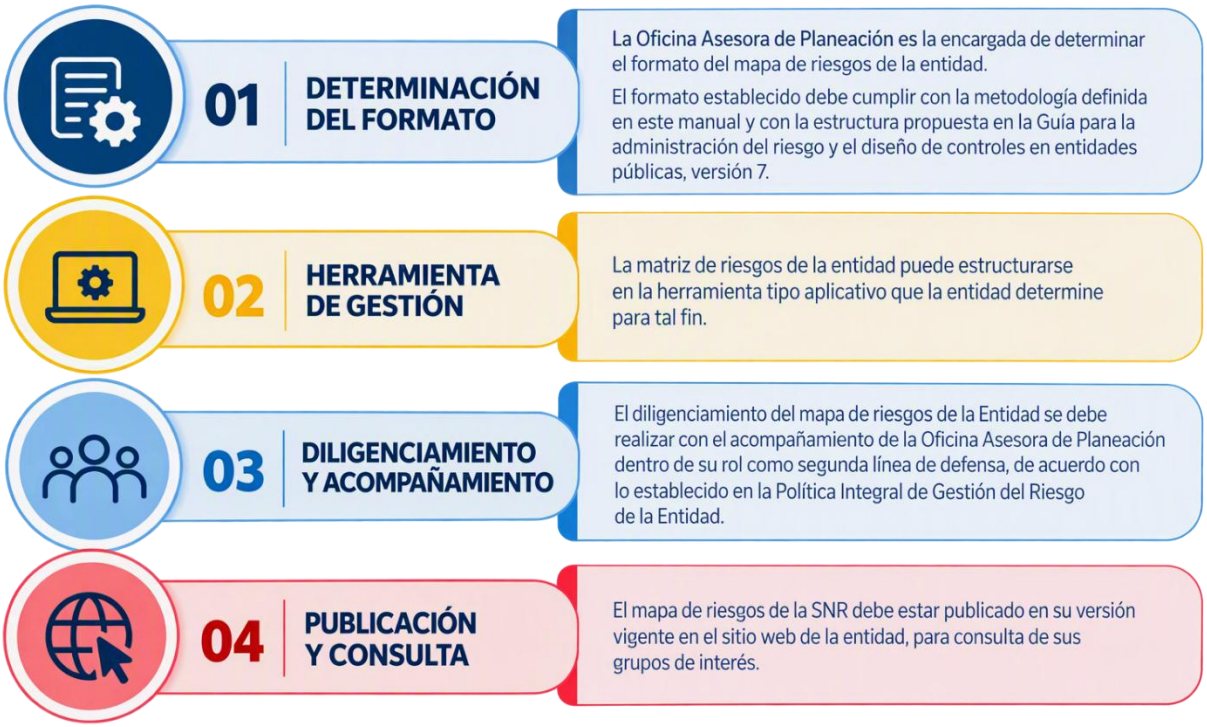
El sistema de gestión de calidad aborda los riesgos asociados a las desviaciones de la calidad de los productos o servicios mediante las disposiciones para la identificación y tratamiento de las posibles las salidas no conformes.

El sistema de gestión de ambiental aborda los riesgos asociados a los aspectos e impactos ambientales mediante las disposiciones para la identificación de aspectos y evaluación de impactos.

El sistema de gestión de seguridad y salud en el trabajo aborda los riesgos operacionales mediante las disposiciones para la identificación de peligros y evaluación de riesgos de seguridad y salud en el trabajo.

Cada responsable de segunda línea de defensa para cada sistema de gestión deberá establecer la metodología para abordar los riesgos operacionales del respectivo sistema de gestión.

6.5 Mapa de Riesgos de la Entidad.



7. BIBLIOGRAFÍA

- ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

- Departamento Administrativo de la Función Pública. (2022). GUÍA PARA LA GESTIÓN INTEGRAL DEL RIESGO EN ENTIDADES PÚBLICAS VERSIÓN 7. Bogotá D.C.

8. DOCUMENTOS ASOCIADOS

Política Integral de Gestión del Riesgo

9. ANEXOS

No aplica

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**
SIG-MN-001	1	19/10/2026	Se actualiza de conformidad con lo nuevos lineamientos que en materia de gestión de riesgos debe implementar la entidad, atendiendo las directrices del Departamento Administrativo de la Función Pública en la Guía para la Gestión Integral del Riesgo v7

ELABORACIÓN, REVISIÓN Y APROBACIÓN		
ELABORÓ	**REVISÓ**	**APROBÓ**
Erik Humberto Nieves Espitia	Laura Nathalia Cárdenas Jiménez	Sandra Patricia Ruiz Moreno Comité Institucional de Control Interno Acta No. 04
Contratista Especializado OAP	Profesional Especializado OAP	Jefe Oficina Asesora de Planeación (E)
Fecha: 30/04/2026	Fecha: 30/07/2026	Fecha: 19/10/2026