GESTIÓN INTEGRAL DEL RIESGO

Superintendencia Nacional de Salud

Fecha del documento (27 – 11 – 25)

Supersalud

Contenido

OBJETIVO

Establecer un enfoque sistemático que permita identificar, analizar, evaluar, tratar y monitorear los riesgos institucionales, promoviendo la toma de decisiones informadas y la protección del patrimonio público con el fin de lograr la seguridad razonable del logro de sus objetivos institucionales.

ALCANCE

Inicia con la definición de la Política Institucional para la Gestión del Riesgo, continua con la metodología aplicable a la gestión integral del riesgo y finaliza con el seguimiento y monitoreo asegurando su articulación con los sistemas de control interno y los mecanismos de planeación institucional. Este manual aplica para los riesgos generales de la gestión, los riesgos fiscales, los riesgos de seguridad de la información, los riesgos para la integridad pública y los riesgos derivados de la operatividad de los subsistemas del Sistema Integrado de Gestión.

NORMATIVIDAD

- **Decreto 1499 de 2017** "Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública"
- **Decreto 1122 de 2024** "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015

DEFINICIONES

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)
- **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. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)

- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)
- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)
- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)
- **Control:** Medida que permite reducir o mitigar un riesgo. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)
- **Punto de Riesgo:** Actividades en las que potencialmente se genera riesgo. (Guía para la Gestión Integral del Riesgo en Entidades Públicas, v7)
- **Riesgo fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales.
- **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean

susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.

- **Patrimonio público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica. [1]
- **Gestión del Riesgo Fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales
- **Riesgo fiscal:** Probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales.
- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado.[2]
- **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.[3]
- **Función de cumplimiento:** función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la

[1] Artículo 6 Ley 610 de 2000 y sentencia C-340-07
[2] Artículo 3 de la Ley 610 de 2000
[3] ISO 37001:2025 Sistemas de gestión antisoborno

integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública.

ABREVIATURAS

- **ISO:** Organización Internacional de Normalización.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **SUPERSALUD:** Superintendencia Nacional de Salud.

ROLES Y RESPONSABILIDADES

Los roles y responsabilidades asociados a la Gestión Integral del Riesgo se encuentran definidos en la Política Institucional de Riesgos, la cual establece las directrices para su implementación en la Supersalud. Estos roles se articulan y complementan con las responsabilidades frente al seguimiento y monitoreo de los Indicadores Clave de Riesgo (KRI), garantizando una visión integral que permite identificar, evaluar y controlar los riesgos, alineando la gestión preventiva con el análisis continuo de los indicadores.

Tabla 1 Roles y responsabilidades frente al seguimiento y monitoreo Indicadores Clave de Riesgo (KRI)

Línea de Defensa	Responsables	Responsabilidad frente a los Indicadores Clave de Riesgo (KRI)
Línea Estratégica	Alta Dirección y Comité Institucional de Coordinación de Control Interno	Incluir lineamientos sobre KRI en la política de gestión de riesgos.
		Analizar periódicamente los KRI institucionales y proponer mejoras.
		Revisar umbrales y ajustarlos según niveles aceptables.
		Retroalimentar al Comité de Gestión y Desempeño sobre ajustes necesarios.
	Comité Institucional de Gestión y Desempeño	Hacer seguimiento a indicadores de desempeño y riesgo.

Línea de Defensa	Responsables	Responsabilidad frente a los Indicadores Clave de Riesgo (KRI)
		Generar alertas según umbrales definidos.
1ra Línea	Líderes de procesos y Funcionarios Supersalud	Identificar y formular KRI para procesos, programas o proyectos.
		Medir y monitorear KRI alineados con KPI.
		Reportar avances y alertas críticas en el sistema definido para tal fin.
		Actuar ante desviaciones y aplicar acciones de mejora.
2da Línea	Oficina Asesora de Planeación	Asegurar alineación de KRI con objetivos estratégicos.
		Proponer lineamientos para la política de riesgos.
		Definir metodologías para medición y seguimiento.
		Consolidar KRI críticos y presentarlos a la Alta Dirección.
		Asesorar a la primera línea en identificación y aplicación de KRI.
3ra Línea	Oficina de Control Interno	Verificar definición y aplicación de KRI.
		Evaluar pertinencia y eficacia para alertas y correctivos.
		Informar deficiencias a la Alta Dirección y coordinar medidas.
		Acompañar análisis de resultados y estrategias de monitoreo.

Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

POLITICAS DE OPERACIÓN

La gestión por procesos representa un componente fundamental en la articulación entre la planeación estratégica y la operación diaria de la entidad, esta gestión actúa como el eslabón que conecta la estrategia institucional con su ejecución operativa, permitiendo que los objetivos estratégicos se traduzcan en acciones concretas y medibles.

Este enfoque toma como insumo el análisis del contexto interno, que incluye capacidades institucionales, recursos disponibles, procesos existentes y la estructura organizacional, así como el contexto externo, compuesto por factores del entorno político, económico, social, tecnológico, legal y ambiental. Al integrar estos elementos, la gestión por procesos no solo facilita la alineación entre lo estratégico y lo operativo, sino que también fortalece la capacidad de la entidad para anticipar, identificar y gestionar riesgos que puedan afectar el cumplimiento de sus objetivos misionales.

En este sentido, el ***DEMN04 Manual para la Formulación e Implementación de Planes Institucionales*** establece los lineamientos pertinentes al análisis del Contexto Organizacional para el desarrollo del Diagnóstico de Capacidades y entornos, a partir del cual se establece una visión basada en procesos que permite a la entidad mejorar su desempeño, aumentar la eficiencia y promover una cultura de mejora continua, todo ello enmarcado en una gestión pública más transparente, efectiva y orientada a resultados.

Como parte de la gestión integral del riesgo de la Superintendencia Nacional de Salud, los riesgos identificados, se documentan en el formato ***DEFT37 Mapa Integral de Riesgos,*** se exceptúan aquellos riesgos relacionados con los subsistemas de Seguridad y Salud en el Trabajo y de Gestión Ambiental, los cuales se gestionan de acuerdo con sus instrumentos, requisitos y normatividad aplicable conforme a lo establecido en el procedimiento ***DEPD06 Gestión del Riesgo.***

Política de riesgos

La política ***DEPI01 Política para la Administración del Riesgo*** establece un marco de referencia la línea de acción para la gestión del riesgo, la disposición de recursos necesarios y la asignación de responsabilidades, atendiendo la autoridad y responsabilidad, con el fin de con el fin de garantizar su eficiencia en la implementación y efectividad para evitar afectaciones por materializaciones del riesgo que impidan el logro de los objetivos y metas institucionales y el buen uso de los recursos públicos.

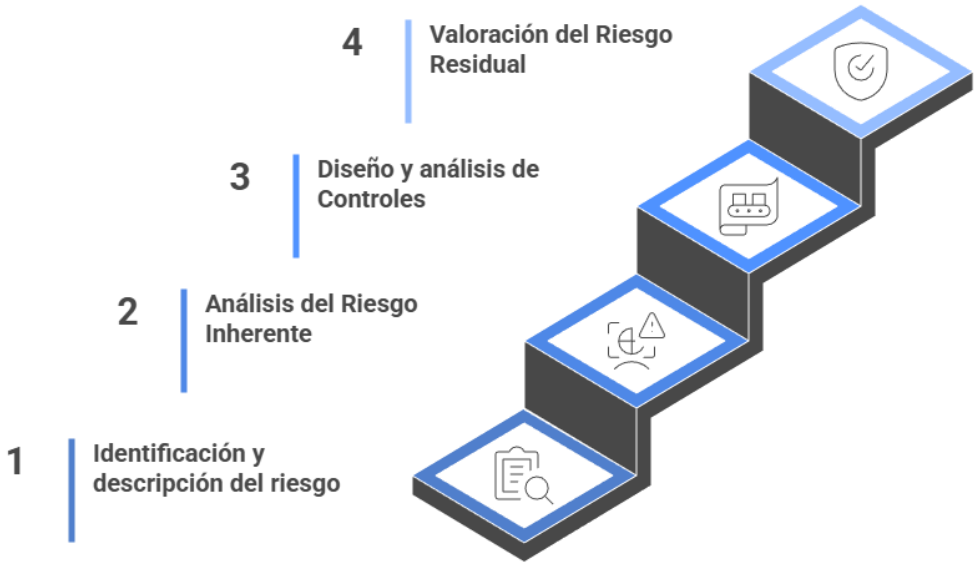
La política es aprobada por la Alta Dirección en el marco del Comité Institucional de Coordinación del Sistema de Control Interno, su difusión e implementación es liderada por el proceso ***Direccionamiento Estratégico*** mediante el asesoramiento y capacitación metodológica para la gestión de riesgos en la Entidad.

La revisión de la política se realiza anualmente y/o cuando los resultados de su evaluación lo sugieran pertinente, en dicho caso la revisión considera los objetivos institucionales, los niveles de responsabilidad frente al manejo de riesgos y los mecanismos de comunicación utilizados para dar a conocer la política en todos los niveles de la entidad.

1. Gestión del riesgo de la gestión

La gestión del riesgo en la Superintendencia Nacional de Salud es una actividad permanente que tiene como objetivo anticipar, analizar y tratar los eventos que puedan afectar el cumplimiento de los objetivos institucionales. Esta gestión comprende cuatro etapas:

Ilustración 1 Etapas para la gestión del riesgo



Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

Este enfoque permite fortalecer su capacidad de respuesta, la toma de decisiones, promover la prevención y consolidar una cultura organizacional basada en la prevención, la transparencia y la mejora continua en todos los niveles de la entidad. El liderazgo de los riesgos de la gestión está a cargo de la Oficina Asesora de Planeación.

1.1 Identificación y descripción del riesgo

Para la identificación de los riesgos claves, el Líder de Proceso considera aquellos eventos que podrían afectar de forma previsible el logro de los objetivos de proceso, estructura de este, actividades clave y aporte dentro de la cadena de valor de la Supersalud.

- **Identificación de los riesgos clave:** Considerar los atributos de los productos, servicios o resultados del proceso que podrían verse afectados dentro del ciclo del proceso objeto de análisis, así como el efecto de estos posibles eventos en el resultado de otros procesos.
- **Identificación de áreas de impacto:** Identificar la consecuencia económica o reputacional a la cual se ve expuesta la Entidad en caso de materializarse el riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.
- **Identificación de áreas de factores de riesgo:** Identificar la fuente generadora del riesgo, circunstancias o condiciones que aumentan la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

Tabla 2 Fuentes generadoras de riesgo

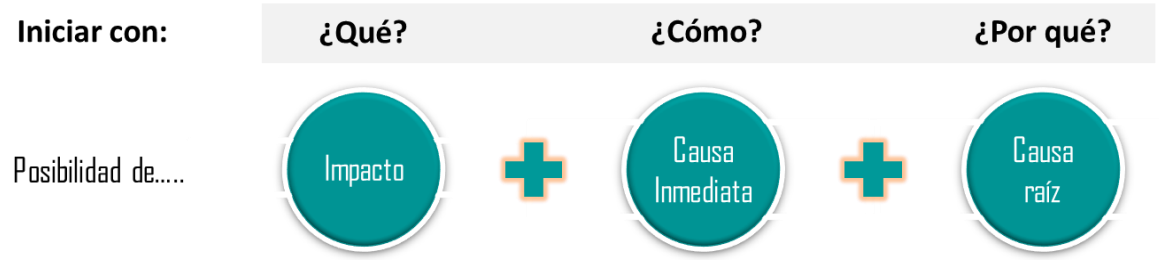
Factor	Definición	Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Falta de aplicación de los procedimientos
		Falta segregación de funciones
		Errores de grabación, autorización
		Falta de supervisión o interventoría
		Errores en cálculos para pagos internos y externos
		Alta rotación o insuficiencia de personal
		Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
		Acciones contrarias a las leyes o acuerdos contractuales
		Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la entidad (naturales o jurídicas)
		Productos (bienes o servicios) que oferta/requiere
		Canales utilizados para la operación
		Jurisdicciones (nacional o territorial)
Talento Humano	Eventos relacionados con las conductas o	Fraude Interno
		Soborno

Factor	Definición	Descriptores
	comportamientos de los empleados que afectan la Integridad Pública.	Canales utilizados para la operación
		Gestión inadecuada de conflicto de Intereses
		Corrupción
		Hurto activos
Tecnología	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Daño de equipos
		Caída de sistemas de información y aplicaciones
		Caída de redes
		Errores en hardware o software
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento Externo	Eventos por situaciones externas que afectan la entidad	Fraude Externo
		Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

- **Descripción del riesgo:** A partir del punto de riesgo, área de impacto y área(s) de factor(es) de riesgo identificados, se procede con la descripción del riesgo.

Ilustración 2 Estructura para la redacción del riesgo



Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

Donde;

- **Impacto**: Afectación económica y/o afectación reputacional
- **Causa inmediata**: Son las circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo.

- **Causa raíz**: Se plantea el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles.

1.2 Análisis de Riesgo Inherente

El análisis del riesgo inherente permite determinar el nivel de exposición de la Supersalud frente a un riesgo específico, en ausencia de controles o medidas de mitigación lo que proporciona una línea base para priorizar los riesgos identificados y orientar la toma de decisiones sobre la necesidad de implementar controles o acciones de tratamiento.

- **Determinar la probabilidad:** La probabilidad de ocurrencia está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente es el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Tabla 3 Criterios para definir el nivel de probabilidad

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

- **Determinar el impacto:** A través de la siguiente tabla, se establecen los criterios para definir el nivel de impacto, considerando como variables principales los efectos

económicos y reputacionales. Cuando se presenten los dos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se toma el nivel más alto.

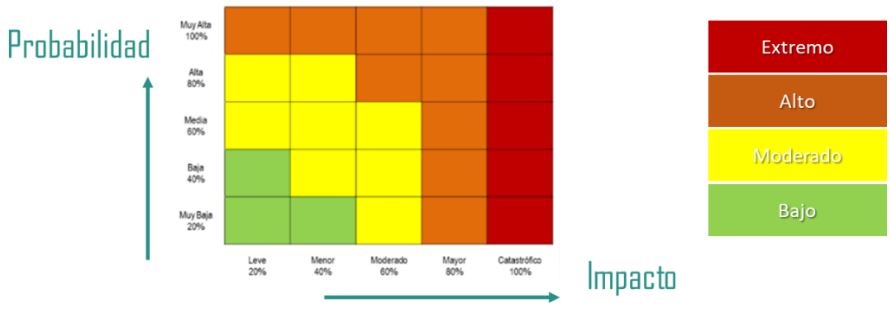
Tabla 4 Criterios para definir el nivel de impacto

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

- **Análisis de severidad:** El análisis del riesgo inherente tiene como objetivo determinar el nivel de severidad del riesgo antes de aplicar cualquier medida de control, mediante la combinación de dos variables: la probabilidad de ocurrencia y el impacto potencial del evento. Para ello, se utiliza la siguiente matriz de calor que clasifica los riesgos en cuatro zonas de severidad, Extremo, Alto, Moderado y Bajo, facilitando así su priorización.

Ilustración 3 Matriz de calor (niveles de severidad del riesgo)



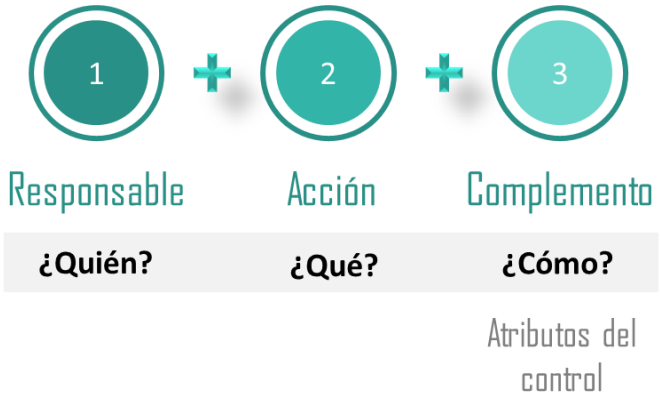
Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

1.3 Diseño y Análisis de Controles

Las actividades de control son acciones con unos atributos específicos establecidos a través de políticas, procedimientos u otras directrices o documentos institucionales que son implementadas con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos. Las actividades de control atienden las causas raíz identificadas y se enfocan en la gestión de los factores de riesgo previamente identificados. Estas son mayormente efectivas cuando cuenten con todos sus atributos y cuando estén directamente relacionadas con tales causas y factores de riesgo.

- **Estructura para la Descripción del Control:** Con el fin de garantizar un diseño adecuado de las actividades de control, se define la siguiente estructura de redacción, la cual integra los atributos esenciales que permiten su correcta implementación por parte del responsable.

Ilustración 4 Estructura para la redacción de controles



Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

Donde;

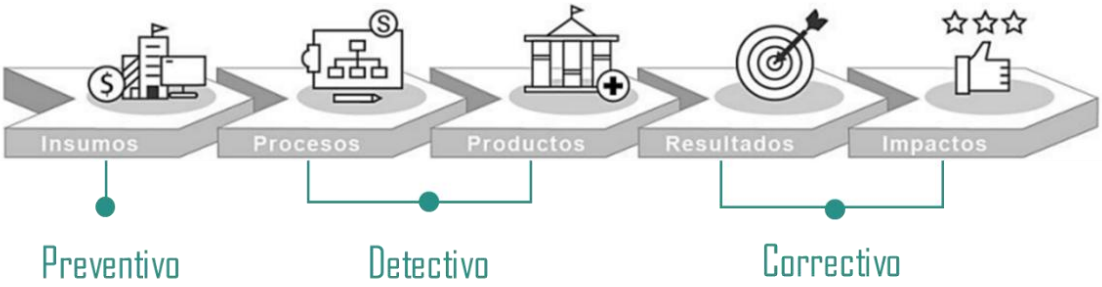
- **Responsable:** Identificar el cargo encargado de ejecutar el control, teniendo en cuenta la estructura organizacional, las diferentes denominaciones de empleo y su distribución en los grupos de trabajo internos. En el caso de controles automáticos,

se señala el responsable de realizar parametrización periódica en el sistema de información o software mediante el cual opera el control.

- **Acción:** Determinar para qué se realiza el control, utilizando verbos como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar.
- **Atributos Informativos o de formalización del control:** Son los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos:
    - Documentación: hace referencia a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
    - Frecuencia: corresponde a la periodicidad con la cual se ejecuta la actividad de control. (puede ser periódica o por evento).
    - Evidencia: permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
    - Ejecución: permite establecer cómo se ejecuta el control, y qué acciones se toman en caso de desviaciones o situaciones que se detecten.

- **Tipologías de Controles:** Con el fin de establecer la tipología de controles, es necesario revisar la cadena de valor del proceso, con el fin de precisar cuándo se activa el control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo, o una combinación de estos.

Ilustración 5 Cadena de valor del proceso y las tipologías de controles



Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

Donde;

- **Control preventivo**: accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo**: accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo**: accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Así mismo, de acuerdo con la forma como se ejecutan tenemos:
    - Control manual: ejecutados por personas.
    - Control automático: ejecutados por un sistema o software previamente programado o diseñado.

- **Valoración de Controles:** Las siguientes tablas determinan la forma como se califican los atributos o características de Eficiencia, y los demás atributos informativos o de formalización del control.

Tabla 5 Valoración de controles

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación	Automático	25%
	Manual	15%

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

Tabla 6 Análisis atributos formalización del control

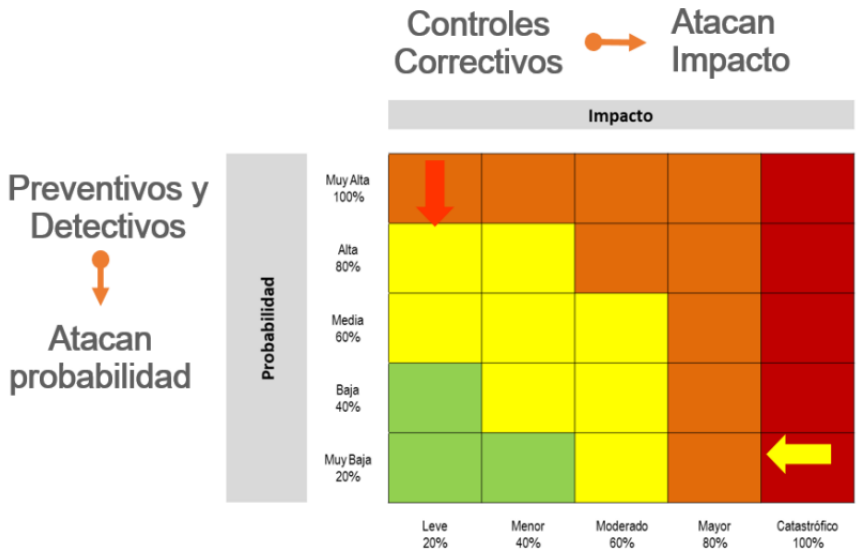
Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).

Características de Eficiencia		Descripción
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos
	Mixta	Combinación de datos de fuentes internas y externas formales.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

- **Aplicación de Controles en la matriz de severidad:** Los tipos de control y su efecto en la matriz se clasifican en tres: el control preventivo, que reduce la probabilidad de ocurrencia del riesgo antes de que se materialice, desplazándolo hacia la izquierda en la matriz; el control detectivo, que permite identificar el riesgo una vez ocurrido y disminuir el tiempo de respuesta, sin modificar la probabilidad pero reduciendo el impacto, moviéndolo hacia abajo en la matriz; y el control correctivo, que actúa después de materializado el riesgo para mitigar sus consecuencias, reduciendo el impacto y desplazando el riesgo hacia abajo en la matriz, en la siguiente ilustración se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Ilustración 6 Movimiento en la Matriz de Calor acorde con el tipo de control



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

1.4 Valoración de Riesgo Residual

El riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para su cálculo, se considera que los controles actúan de manera acumulativa, es decir, cada control reduce el nivel de riesgo con base en el efecto del control anterior. Por lo tanto, al aplicar múltiples controles, el valor del riesgo se ajusta progresivamente, partiendo del nivel de riesgo inherente y disminuyendo con cada control según su grado de efectividad.

2. Riesgos de Seguridad de la Información

Como parte del proceso de gestión integral del riesgo, los líderes de procesos, programas y proyectos de la Superintendencia Nacional de Salud identifican y registran en el mapa de riesgos institucional aquellos riesgos que estén relacionados con la seguridad de la información. Esta actividad se realiza en cumplimiento de la protección de activos institucionales y mejora continua, bajo el liderazgo de la Subdirección de Tecnologías de la Información.

2.1 Identificación de los riesgos clave

La identificación de estos riesgos considera, entre otros aspectos:

- La confidencialidad, integridad y disponibilidad de la información institucional.
- La exposición a amenazas internas o externas que puedan comprometer los sistemas de información.
- El cumplimiento de normativas legales y estándares técnicos en materia de protección de datos.
- La ocurrencia de incidentes tecnológicos, accesos no autorizados, pérdida de información o fallas en la infraestructura digital.
- La gestión de usuarios, contraseñas, privilegios y controles de acceso.
- La existencia de procesos críticos que dependan de plataformas tecnológicas.

El Inventario de Activos de Información es el insumo principal para la Gestión de Riesgos de Seguridad de la Información, según su criticidad, se pueden identificar los siguientes tres (3) riesgos inherentes:

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

Para cada riesgo, se asocian el grupo de activos o activos específicos del proceso o su ecosistema digital operativo, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Los riesgos identificados se documentan en el ***DEFT37 Mapa Integral de Riesgos***.

- **Identificación de áreas de impacto:** El área de impacto es la consecuencia negativa en los objetivos de la organización en caso de materializarse un riesgo o las que por causa de incidentes de seguridad de la información tenga consecuencias en la gestión de la entidad.
- **Identificación de áreas de factores de riesgo:** Son las fuentes generadoras de riesgos. Se analizan las amenazas que pueden afectar la confidencialidad,

integridad y disponibilidad de los activos y se identifican vulnerabilidades que podrían ser explotadas por esas amenazas. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Tabla 7 Tabla de amenazas comunes

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

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

* Deliberadas (D), fortuitas (F) o ambientales (A)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Tabla 8 Tabla de Vulnerabilidades Comunes

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

Tipo	Amenaza
	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
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

- **Descripción del riesgo:** El riesgo se formula como la combinación de impacto + activo + amenaza + vulnerabilidad.

Ilustración 7 Estructura para la redacción del riesgo

Fuente: Adaptado de Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, 2025

Donde;

- **Impacto**: Pérdida de Confidencialidad / Integridad / Disponibilidad.
- **Activo**: Nombre del activo de información.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022)
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022)

2.2 Análisis de Riesgo Inherente

A partir de este paso metodológico se incorporan la tablas y matrices establecidas en el numeral **1.2 Análisis de Riesgo Inherente** que desarrolla los lineamientos para los riesgos generales de la gestión.

3. Riesgos del Subsistema de Gestión Ambiental (SGA)

Como parte del compromiso institucional con la sostenibilidad ambiental y la mejora continua, la Superintendencia Nacional de Salud incorpora la gestión de riesgos en el marco de su Subsistema de Gestión Ambiental (SGA) bajo el liderazgo de la Dirección Administrativa, en concordancia con los requisitos de la norma ISO 14001 en su versión

vigente y la normatividad aplicable. Para tal efecto, se identifican los riesgos ambientales considerando:

- Aspectos e impactos ambientales derivados de las actividades institucionales.
- Obligaciones legales y otros requisitos aplicables.
- Condiciones internas y externas que puedan influir en el desempeño ambiental.
- Ciclo de vida de los productos, servicios y procesos.

La identificación y descripción del riesgo, contempla la siguiente estructura de redacción:

Ilustración 8 Estructura para la redacción del riesgo

Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

El análisis del riesgo inherente, el diseño y análisis de controles y la valoración del riesgo residual de los riesgos derivados del Subsistema de Gestión Ambiental que puedan impactar negativamente el medio ambiente, se realizan en cumplimiento de lo establecido en el ***BSMN04 Manual operacional para la gestión ambiental***.

4. Riesgos del Subsistema de Seguridad y Salud en el Trabajo (SST)

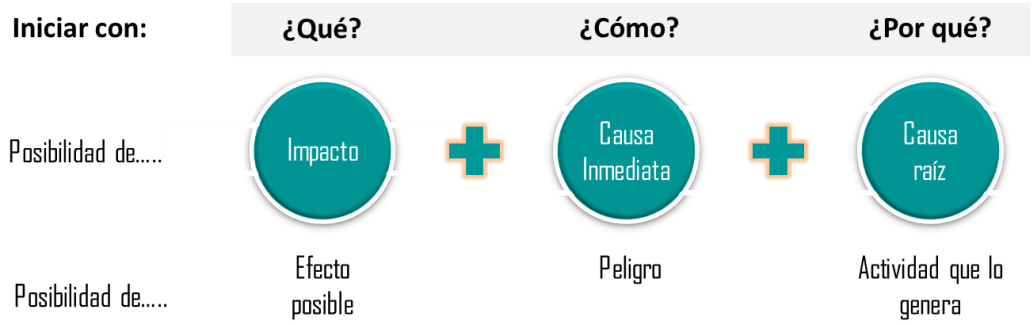
Como parte del compromiso institucional con la seguridad y salud en el trabajo de sus colaboradores y la mejora continua, la Superintendencia Nacional de Salud incorpora la gestión de riesgos en el marco de su Subsistema de Seguridad y Salud en el Trabajo (SG-

SST) bajo el liderazgo de la Dirección de Talento Humano, en concordancia con los requisitos de la norma ISO 45001 en su versión vigente y la normatividad aplicable. Para tal efecto, se identifican los peligros presentes en el entorno laboral, considerando:

- Condiciones físicas, químicas, biológicas, ergonómicas y psicosociales.
- Actividades rutinarias y no rutinarias.
- Infraestructura, equipos, herramientas y tecnologías utilizadas.
- Cambios organizacionales, operacionales o legales.

Para tal efecto, la identificación y descripción del riesgo, contempla la siguiente estructura de redacción:

Ilustración 9 Estructura para la redacción del riesgo



Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

El análisis del riesgo inherente, el diseño y análisis de controles y la valoración del riesgo residual de los riesgos que puedan afectar la seguridad, salud y bienestar de los servidores públicos, contratistas y demás colaboradores de la entidad, se realizan en cumplimiento de lo establecido en el ***PEMN10 Manual operativo del componente sistema de gestión de seguridad y salud en el trabajo*.**

5. Riesgos para la Integridad Pública

La gestión de los riesgos para la integridad pública permite prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), de manera integral. La Superintendencia Nacional de Salud incorpora en su operación la gestión de riesgos para la integridad pública bajo el liderazgo de la Función de Cumplimiento.

Tabla 9 Integridad Pública

<table>
<tr><th colspan="3">Integridad pública</th></tr>
<tr><th colspan="2">Integridad del Servidor Público</th><th>Integridad de las Instituciones Públicas</th></tr>
<tr><td>Riesgos de incumplimiento por conductas asociadas a Fraudes Internos</td><td>Riesgos de incumplimiento por conductas asociadas a Inadecuada gestión del conflicto de intereses</td><td rowspan="2">Riesgos de incumplimiento por conductas asociadas al Lavado de Activos, la Financiación del Terrorismo y la Financiación de Armas de Destrucción Masiva (LA/FT/FP)</td></tr>
<tr><td>Riesgos de incumplimiento por conductas asociadas a Soborno saliente y entrante</td><td>Riesgos de incumplimiento por conductas asociadas a Otras formas de corrupción</td></tr>
</table>

Fuente: Presentación Secretaría de Transparencia, 2025

5.1 Identificación y descripción del riesgo

Desde una perspectiva integral, los riesgos que afectan la integridad pública deben gestionarse de manera articulada con los riesgos generales de la gestión institucional, la gestión del riesgo fiscal y los riesgos asociados a la seguridad de la información.

- **Identificación de los puntos de riesgo:** En la gestión del riesgo de LA/FT/FP, los puntos de riesgo son momentos dentro de los procesos donde se realizan operaciones que implican intercambio de recursos. Esto ocurre, cuando la entidad

paga por un bien o servicio que recibe, o cuando entrega un bien o servicio por el cual recibe un pago.

En el caso del riesgo de corrupción y sus formas específicas como soborno, fraude o conflictos de interés mal gestionados, los puntos de riesgo no se limitan solo a las operaciones. Pueden encontrarse en cualquier actividad del proceso donde exista posibilidad de influencia indebida o falta de transparencia.

- **Identificación de áreas de impacto:** En la gestión de riesgos para la integridad pública, además del impacto económico y reputacional, se consideran consecuencias legales y de contagio.
    - **Legal:** Surge por incumplimiento normativo u obligaciones, desde la vinculación a procesos judiciales o administrativos.
    - **Contagio:** Afectación económica, reputacional o legal por conductas de partes relacionadas, aunque no estén directamente vinculadas.

El impacto del riesgo se analiza en términos económicos acorde a lo indicado en el numeral 1.2. Un riesgo se materializa cuando ocurre una situación que afecta objetivos institucionales (reputación, operación, cumplimiento o ejecución de recursos), sin implicar delito ni prejuzgamiento.

Toda operación sospechosa de LA/FT/FP se reporta, incluso si no se materializa el delito. La gestión del riesgo busca prevenir, detectar y corregir, sin derivar en sanciones ni juicios de responsabilidad. Ante la materialización, la Supersalud garantiza la continuidad del servicio y operación, independientemente de las acciones de otras autoridades.

- **Identificación de factores de riesgo:** Los factores de riesgo LA/FT/FP son: contrapartes, productos, canales y jurisdicciones, que en conjunto definen una transacción. Estos factores permiten: un mejor conocimiento de contrapartes, el diseño de señales de alerta e identificación de operaciones inusuales y reporte de sospechosas. Para ello, se requiere segmentación, agrupando contrapartes con características similares para establecer parámetros normales de comportamiento y

detectar desviaciones. Las señales de alerta se construyen con base en estos segmentos.

En este paso metodológico se incorporan la tabla de factores de riesgo establecida en el numeral **1.1 Identificación y descripción del riesgo** que desarrolla los lineamientos para los riesgos generales de la gestión.

- **Descripción del riesgo:** La descripción de los riesgos para la integridad pública tiene la misma fórmula definida en el numeral **1.1 Identificación y descripción del riesgo** de este manual. Todos inician con “Posibilidad de”, señalan el impacto, la causa inmediata y la causa raíz. Teniendo en cuenta las amenazas para la Integridad Pública, las causas inmediatas de los riesgos para la integridad pública son el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP.

Soborno: Ofrecer, dar, aceptar o solicitar ventajas indebidas (financieras o no) para influir en decisiones. Puede ser:

  - Entrante: Soborno al servidor público.
  - Saliente: Soborno desde la entidad hacia terceros.

Fraude: Errores, omisiones o informes falsos con dolo o culpa para beneficio propio o de terceros.

  - Interno: Involucra colaboradores.
  - Externo: Realizado por terceros; riesgo operativo.

Inadecuada gestión del conflicto de intereses: Surge cuando el servidor público decide sobre asuntos donde tiene interés personal o familiar. No siempre implica falta, pero requiere declaración y gestión según la ley.

Corrupción: Desviación de la gestión administrativa o recursos para beneficio propio o de terceros. Incluye: Uso indebido del poder, pérdida del patrimonio público, perjuicio social significativo, corrupción electoral.

LA/FT/FP: Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas afectan la integridad pública al usar entidades para dar apariencia de legalidad a recursos ilícitos o financiar actividades ilegales.

5.2 Análisis de Riesgo Inherente

En este paso metodológico se incorporan las tablas y matrices establecidas en el numeral **1.2 Análisis de Riesgo Inherente** que desarrolla los lineamientos para los riesgos generales de la gestión.

5.3 Diseño y Análisis de Controles

En este paso metodológico además de incorporar las tablas y matrices establecidas en el numeral **1.3 Diseño y Análisis de Controles** que desarrolla los lineamientos para los riesgos generales de la gestión. Se implementa:

- **Debida diligencia:** Manual que incorpora mecanismos que desarrollan el principio de debida diligencia en todas las interacciones con contrapartes, en las que existe una exposición a riesgos para la integridad pública, es decir, en aquellas interacciones en que se haya identificado un riesgo de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.

- **Función de cumplimiento:** La función de cumplimiento tiene como propósito asegurar el funcionamiento eficaz y oportuno de la Gestión del Riesgo de Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva. Para ello, supervisa sus componentes, apoya a los líderes de proceso en la gestión de riesgos, presenta informes periódicos a la Alta Dirección, recomienda

lineamientos normativos, promueve medidas correctivas y coordina con otras áreas para garantizar la operatividad del sistema.

Asimismo, participa en el diseño de metodologías e indicadores de riesgo, establece lineamientos de debida diligencia para el conocimiento de contrapartes, define criterios para identificar operaciones sospechosas y reporta oficialmente a las autoridades competentes.

- **Otras herramientas:** La gestión de riesgos para la integridad pública se complementa con un conjunto de políticas y procedimientos que fortalecen el sistema institucional. La Política Antilavado de Activos, Contra la Financiación del Terrorismo y de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP), la Política Antisoborno, la Política Antifraude, la Política para la Gestión de Conflictos de Interés, la Política para el Reporte de Operaciones Sospechosas y la Política para la operación del canal institucional de denuncias y buzón ético.

5.4 Valoración de Riesgo Residual

En este paso metodológico se incorporan las tablas y matrices establecidas en el numeral **1.4 Valoración de Riesgo Residual** que desarrolla los lineamientos para los riesgos generales de la gestión.

6. Riesgos Fiscales

La gestión preventiva de riesgos fiscales tiene como finalidad evitar afectaciones al patrimonio público y la generación de responsabilidades fiscales mediante la aplicación de controles internos eficaces, por lo anterior, la Superintendencia Nacional de Salud incorpora en su operación la gestión de estos riesgos bajo el liderazgo de la Función de Cumplimiento.

Por su parte, el concepto de 'gestor fiscal' incluye a los jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores de proyectos, responsables de la planeación contractual, supervisores, encargados de labores de cobro, entre otros roles cuyas funciones u obligaciones inciden directamente en la gestión fiscal.

6.1 Identificación de riesgos fiscales

A continuación, se detalla la identificación del riesgo fiscal, este proceso se integra con el análisis general de los riesgos institucionales, con el propósito de consolidar un esquema integral que facilite su seguimiento y control por parte de los líderes de cada proceso.

- **Puntos de riesgo fiscal:** Los puntos de riesgo fiscal corresponden a eventos o situaciones que, por su naturaleza, pueden generar afectaciones al patrimonio público o comprometer la responsabilidad fiscal de la entidad. Por esta razón, es necesario identificar aquellas actividades en las que se hayan identificado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal por parte de los órganos de control. A continuación, se listan los principales puntos de riesgo fiscal:

  a. **Planeación y presupuesto:** errores en la formulación, falta de estudios previos, asignación inadecuada de recursos.
  b. **Contratación:** ausencia de pluralidad de oferentes, pliegos restrictivos, falta de supervisión.
  c. **Ejecución contractual:** incumplimientos, modificaciones injustificadas, pagos sin verificación.
  d. **Gestión financiera:** registros contables incorrectos, conciliaciones incompletas, pagos indebidos.
  e. **Administración de bienes:** pérdida, deterioro o uso indebido de activos.

  Circunstancias inmediatas que aumentan el riesgo: deficiencias en controles internos, falta de segregación de funciones, ausencia de trazabilidad en procesos y debilidad en mecanismos de supervisión y auditoría.

- **Identificación de áreas de impacto:** Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponde a una consecuencia económica pues afecta el patrimonio público.
  - **Bienes públicos:** Muebles e inmuebles del Estado, clasificados en: bienes de uso público (para todos los habitantes), y bienes fiscales (destinados a funciones o servicios públicos).
  - **Recursos públicos:** Dinero comprometido y ejecutado en la función pública.
  - **Intereses patrimoniales de naturaleza pública:** Beneficios esperados que pueden estimarse económicamente.

- **Identificar el efecto económico:** El efecto económico del riesgo fiscal es el potencial detrimento del patrimonio público (pérdida, daño o deterioro). No todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales representan un efecto económico.
- **Identificación de la causa raíz o potencial hecho generador:** La causa raíz es cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro.[4].
- **Descripción del Riesgo Fiscal**: A partir del punto de riesgo, área de impacto y área(s) de factor(es) de riesgo identificados, se procede con la descripción del riesgo.

Ilustración 10 Descripción Riesgo Fiscal

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

[4] Auditoría General de la República, 2015

Donde;

- **Iniciar con la expresión**: Posibilidad de efecto dañoso sobre…
- **Impacto**: Recursos públicos, bienes o intereses patrimoniales de naturaleza pública.
- **Circunstancia inmediata**: Se refiere a aquella situación en la que se presenta el riesgo; pero no constituye la causa principal que lo genera.
- **Causa Raíz**: Es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño.

6.2 Análisis de Riesgo Inherente

A partir de este paso metodológico se incorporan la tablas y matrices establecidas en el numeral **1.2 Análisis de Riesgo Inherente** que desarrolla los lineamientos para los riesgos generales de la gestión.

7. Seguimiento, Monitoreo y Revisión

La medición del riesgo es una herramienta estratégica que permite establecer la efectividad de los controles, validar el cumplimiento de metas, analizar comportamientos y tendencias, así como identificar posibles desviaciones que puedan afectar la gestión institucional.

7.1 Indicadores Clave de Riesgo (KRI)

Como parte del proceso de monitoreo de la gestión integral del riesgo, la Superintendencia Nacional de Salud establece indicadores clave de riesgo (KRI) que permiten evaluar de manera sistemática y continua el comportamiento de los riesgos identificados, así como la efectividad de las acciones de tratamiento implementadas.

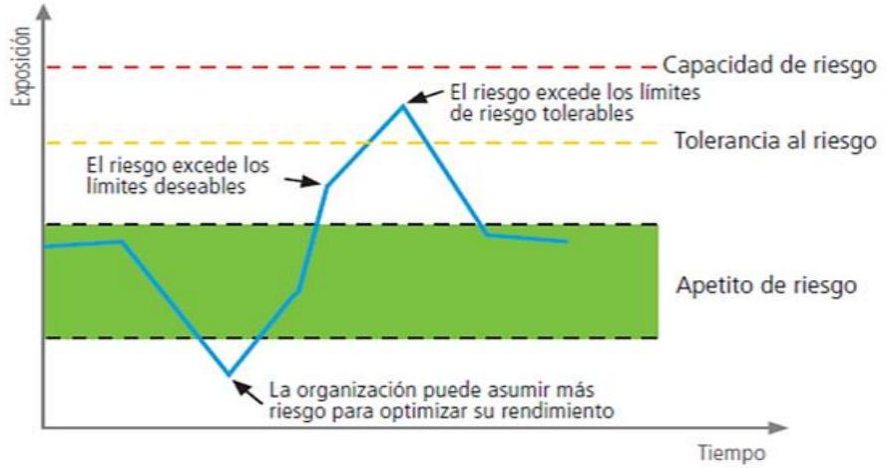
Los KRI son integrados en los informes de gestión, en el sistema de control interno y en los espacios de evaluación institucional, como herramienta clave para fortalecer la cultura de gestión del riesgo y la toma de decisiones basada en evidencia.

El resultado del cálculo del KRI se relaciona directamente con el apetito al riesgo, y se analiza de cara a la declaración de apetito de la entidad bajo las siguientes consideraciones.

Tabla 10 Valor KRI vs Apetito al riesgo

Valor del KRI	Interpretación	Acción Requerida
Dentro del apetito de riesgo	El riesgo se mantiene en el nivel aceptable definido por la entidad.	Continuar monitoreo según la periodicidad establecida.
Excede el apetito de riesgo	El riesgo supera el umbral tolerable para la entidad.	Implementar acciones correctivas o de mitigación.
Cercano al umbral de alerta	El riesgo está aumentando y podría superar el límite si la tendencia continúa.	Refuerzo del monitoreo y medidas preventivas inmediatas.

Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7

Los umbrales son establecidos por el responsable de proceso y aprobados por el comité de coordinación de control interno argumentando una base histórica. Cabe anotar que no se crean indicadores clave de riesgo para todos los riesgos solo para los más críticos.

7.2 Análisis de Eventos (Materializaciones del Riesgo)

En caso de evidenciar la materialización del riesgo, la primera línea de defensa informa al Líder de Proceso y demás involucrados, y registra el correspondiente evento en la

herramienta dispuesta por la Entidad para tal fin. Una vez registrado el evento, se procede a la formulación del respectivo Plan de Mejoramiento, de conformidad con lo establecido en el Procedimiento ***GMPD02 Mejoramiento Continuo*.** En adición, se realiza revisión del riesgo materializado y valida la pertinencia de su actualización.

Para el análisis de eventos que representan la materialización de riesgos en la Superintendencia Nacional de Salud, la información sobre eventos se recopila a partir de las siguientes fuentes internas:

- **Mesa de ayuda o soporte tecnológico:** Registro de incidentes relacionados con fallas en sistemas, accesos, infraestructura tecnológica y servicios digitales.
- **Área o proceso de atención al usuario:** Reportes derivados de la interacción directa con ciudadanos, prestadores y demás actores del sistema de salud.
- **PQRD (Peticiones, Quejas, Reclamos y Denuncias):** Información proveniente de los canales oficiales de atención, que permite identificar riesgos reputacionales, operativos y de corrupción.
- **Oficina Jurídica:** Casos relacionados con litigios, conceptos jurídicos, sanciones o actuaciones administrativas que evidencien riesgos legales o normativos.
- **Líneas internas de denuncia:** Mecanismos confidenciales para reportar posibles irregularidades, fraudes o conductas contrarias a la ética pública.
- **Reportes de líderes de proceso:** Cada líder de proceso tiene la responsabilidad de reportar formalmente los eventos que se presenten en su proceso, mediante el mecanismo interno establecido por la entidad.
- **Otros mecanismos institucionales:** Incluye auditorías internas, informes de supervisión, hallazgos de control interno, entre otros.

Toda la información recopilada es analizada en conjunto por la segunda línea de defensa, con el fin de:

- Clasificar el tipo de riesgo materializado.
- Determinar la causa raíz del evento.
- Evaluar el impacto en los objetivos institucionales.

- Proponer acciones de mejora y tratamiento.
- Retroalimentar el mapa de riesgos y los planes de gestión.

Control de cambios					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Lisseth Dayana Ortega Bravo	**Nombre**	Marcela Andrea García Guerrero John Alexander Bolaños Barros	**Nombre**	Gloria Rocío Pereira Oviedo
Cargo	Profesional Especializado	**Cargo**	Profesionales Especializados Oficina Asesora de Planeación	**Cargo**	Jefe de Oficina Asesora de Planeación
Fecha	21/11/2025	**Fecha**	24/11/2025	**Fecha**	27/11/2025