

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

OBJETIVO

Establecer los lineamientos para la gestión de los Riesgos Generales de la Gestión, Riesgos Fiscales, Riesgos de Seguridad de la Información y Riesgos para la Integridad Pública de la Superintendencia Nacional de Salud con el fin de lograr la seguridad razonable del logro de sus objetivos institucionales.

ALCANCE

Inicia con la identificación y descripción del riesgo, continua con el análisis del riesgo inherente, diseño y análisis de controles, la valoración del riesgo residual y finaliza con el seguimiento, monitoreo y revisión de estos. Este procedimiento 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.

RESPONSABLE DEL PROCEDIMIENTO

Oficina Asesora de Planeación

DEFINICIONES

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **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.
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Punto de Riesgo:** Actividades en las que potencialmente se genera riesgo.
- **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.

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

- **Riesgo fiscal:** Probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

ABREVIATURAS

ISO: Organización Internacional de Normalización.

MIPG: Modelo Integrado de Planeación y Gestión.

SUPERSALUD: Superintendencia Nacional de Salud.

LINEAMIENTOS GENERALES O POLÍTICAS DE OPERACIÓN

A continuación, se presentan los lineamientos generales para la implementación de la política institucional para la gestión integral del riesgo acorde a las directrices establecidas por el Departamento Administrativo de la Función Pública, basada en la norma internacional ISO 31000, los referentes normativos de cada Subsistema del Sistema Integrado de Gestión y su articulación con el Modelo Integrado de Planeación y Gestión (MIPG).

La implementación del presente procedimiento se realizará de manera gradual, en función de la actualización de los riesgos vigentes y/o la identificación de nuevos riesgos. Este enfoque permitirá una adaptación continua y efectiva de las medidas establecidas, garantizando que las acciones contempladas respondan oportunamente a las condiciones reales del entorno y a los cambios en la matriz de riesgos.

1. La tipología de riesgos permite categorizar de manera sistemática los eventos que podrían afectar el cumplimiento de los objetivos institucionales, facilitando su análisis, evaluación y tratamiento, cada uno con características particulares que requieren enfoques diferenciados de gestión. La gestión integral del riesgo de la Supersalud abarca los siguientes tipos de riesgo:

Tabla 1 Tipología de riesgos

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

Tipo de riesgo	Descripción
1. Riesgo General de la Gestión	Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Incluye los riesgos derivados de la operatividad de los Subsistemas del SIG.
2. 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.
3. Riesgos de Seguridad de la Información	Hace referencia a las amenazas y vulnerabilidades que pueden afectar la confidencialidad, integridad y disponibilidad de un activo de información.
4. Riesgos para la Integridad Pública	Integridad del servidor público Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Integridad de las instituciones públicas El riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas.

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

La gestión de estos riesgos se realiza conforme a la metodología institucional, garantizando la actualización periódica del mapa de riesgos y la adopción de acciones pertinentes por parte de los procesos correspondientes.

- La gestión del riesgo en la Superintendencia Nacional de Salud se establece como una actividad permanente orientada a anticipar, analizar y tratar los eventos que puedan afectar el cumplimiento de los objetivos institucionales. Este procedimiento se desarrolla mediante cuatro etapas: la identificación y descripción del riesgo, el análisis del riesgo inherente, el diseño y análisis de controles, y la valoración del riesgo residual, acorde con lo establecido en el **DEMNO2 Gestión Integral del Riesgo** garantizando así un enfoque sistemático y preventivo en la administración de riesgos.

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

- En cumplimiento lineamientos relacionados con la gestión de riesgos, la publicación del mapa de riesgos institucional se realiza a más tardar el 31 de enero de cada vigencia, previa consulta pública a los grupos de interés a través de la página web de la Supersalud. Los aportes y comentarios recibidos que resulten pertinentes son utilizados para retroalimentar la identificación de los riesgos, los cuales son evaluados por la primera línea de defensa, con el fin de validar su aplicabilidad. De esta actividad, se conserva evidencia digital tanto de la consulta realizada como de las observaciones presentadas por los grupos de interés.
- La Superintendencia Nacional de Salud establece responsabilidades en la gestión de riesgos y controles internos, asegurando que haya claridad en roles y funciones a través de la implementación del esquema de líneas de defensa:

Tabla 2 Roles y responsabilidades frente a la gestión integral de riesgos

	Rol	Responsabilidad
Línea estratégica	Comité Institucional de Gestión y Desempeño	Analizar la gestión del riesgo y definir las mejoras
	Comité Institucional de Coordinación de Control Interno	Analizar eventos y riesgos críticos
	Alta Dirección	Decidir e implementar estrategias para la gestión del riesgo y la mejora continua
1ra Línea de defensa	Servidores todos los niveles	Ejecutar los controles operativos en el día a día
	Líderes de proceso, Directores de proyectos, Responsables de la planeación contractual, Supervisores de contrato, Líderes de Subsistemas de Gestión, Gestores Fiscales	Gestionar los riesgos y hacer seguimiento a la 1a Línea aplica controles de gerencia operativa
2da Línea de defensa	Oficina Asesora de Planeación, Función de Cumplimiento, Comité de Contratación o quienes hagan sus veces y otras instancias de 2da Línea identificados	Definir metodología, capacita, acompaña, recomienda y hace seguimiento con enfoque preventivo. Generar alertas de materialización de riesgos en el Comité Institucional de Coordinación de Control Interno
3ra Línea de defensa	Oficina de Control Interno, Auditoría Interna o quien haga sus veces	Evaluación independiente, asesora y recomienda

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

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

5. Cuando un riesgo se ubique en zona residual '**Moderada**', '**Alta**' o '**Extrema**', se formula el plan de tratamiento correspondiente, orientado a fortalecer los controles existentes, reducir el impacto y/o disminuir la probabilidad de ocurrencia.
6. Previo a la formalización de acciones el líder del proceso verifica si para su ejecución se requiere la asignación de recursos de funcionamiento o inversión, y estos se gestionan a través de los instrumentos de planeación institucional teniendo en cuenta los periodos para la planificación de recursos y correspondiente aprobación.
7. Es responsabilidad del líder del proceso dar cumplimiento con las actividades formuladas en los planes de tratamiento, de acuerdo con los plazos que haya establecido y reportar los avances correspondientes. A su vez los responsables involucrados en los planes de tratamiento deben responsabilizarse de la ejecución de las actividades a su cargo, y proporcionar las evidencias respectivas.
8. Se puede solicitar la modificación de fechas de ejecución, responsables o actividades (incluyendo productos o entregables) de los planes de tratamiento en desarrollo, a más tardar dentro de los quince (15) días hábiles previos al vencimiento de la fecha programada. En caso de ampliación de plazo, este no puede exceder la mitad del tiempo de ejecución inicialmente definido para la actividad, salvo situaciones excepcionales.
9. La ampliación del plazo o la modificación de actividades definidas en planes con vencimiento podrá solicitarse por única vez, y el nuevo plazo no puede superar noventa (90) días calendario posteriores a la fecha de vencimiento inicial de la acción.
10. Cuando se materialice un riesgo, el Líder de Proceso informa el evento al Comité Institucional de Coordinación de Control Interno para su análisis, lo registra en la herramienta definida por la Entidad conforme al **DEMNO2 Gestión Integral del Riesgo**, y formula el plan de mejoramiento correspondiente en la misma herramienta, incorporando el análisis de la gestión del riesgo, la identificación de los factores que propiciaron su ocurrencia y realizando los ajustes necesarios para prevenir su repetición.

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

DIAGRAMA DE FLUJO

Diagrama de flujo anexo.

DESARROLLO -DESCRIPCIÓN

N.	Actividad	Responsable	Tiempo o frecuencia si aplica	Registro
1	Identificar y describir el riesgo Para realizar la descripción de los riesgos, se identifican los eventos que puedan afectar el logro de los objetivos institucionales, definir las causas, consecuencias, áreas de impacto y procesos involucrados y utilizar la estructura establecida en el numeral 1.1 Identificación y descripción del riesgo del <i>DEMN02 Gestión Integral del Riesgo</i> .	1ra Línea de Defensa	Cada vez que se requiera	DEFT37 Mapa Integral de Riesgos
2	Analizar el riesgo inherente Una vez finalizada la descripción, se evalúa el riesgo en ausencia de controles, considerando la probabilidad de ocurrencia y el impacto potencial. Esta valoración permite priorizar los riesgos y enfocar los esfuerzos de mitigación en los más críticos. Ver numeral 1.2 Análisis de Riesgo Inherente del <i>DEMN02 Gestión Integral del Riesgo</i> .	1ra Línea de Defensa	Cada vez que se requiera	DEFT37 Mapa Integral de Riesgos

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

N.	Actividad	Responsable	Tiempo o frecuencia si aplica	Registro
3	Diseñar y analizar controles El análisis del riesgo inherente permite identificar las medidas de prevención, detección y mitigación requeridas para la gestión del riesgo que llevan a establecer los puntos de control. Una vez establecidos, se analizan atributos como formalización, cobertura, efectividad y oportunidad, y se documentan los controles en la matriz de riesgos. Ver numeral 2.3 Diseño y Análisis de Controles del <i>DEMN02 Gestión Integral del Riesgo</i>.	1ra Línea de Defensa	Cada vez que se requiera	DEFT37 Mapa Integral de Riesgos
4	Valorar el riesgo residual Al establecer controles, se hace necesario determinar el nivel de riesgo que permanece después de aplicarlos al riesgo. Para tal efecto, se compara con los niveles de tolerancia definidos en la política con el fin de establecer si es aceptable o requiere tratamiento adicional. Ver numeral 2.4 Valoración de Riesgo Residual del <i>DEMN02 Gestión Integral del Riesgo</i>. Nota: Para los riesgos clasificados en zona residual 'Extrema', se define un Indicador Clave de Riesgo. En el caso de los riesgos ubicados en zona residual 'Alta', se evalúa la pertinencia de establecer un Indicador Clave de Riesgo, conforme a la metodología institucional.	1ra Línea de Defensa	Cada vez que se requiera	DEFT37 Mapa Integral de Riesgos

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

N.	Actividad	Responsable	Tiempo o frecuencia si aplica	Registro
5	© Revisar y validar la definición/actualización del Mapa de Riesgos Revisar y validar la definición/actualización del Mapa de Riesgos verificando su pertinencia y aplicabilidad a nivel de proceso. ¿La definición/actualización del Mapa de Riesgos es validada? Si: Continuar a la actividad No.6 Devolver a la actividad No.1 No: Devolver a la actividad No.1	Líder de Proceso	Cada vez que se requiera	DEFT37 Mapa Integral de Riesgos validado
6	Remitir Mapa de Riesgos Al finalizar la elaboración del Mapa de Riesgos, se remite a la Segunda Línea de Defensa para su correspondiente revisión acorde a los niveles de responsabilidad establecidos en la DEPI01 Política para la Administración del Riesgo.	Líder de Proceso	Cada vez que se requiera	DEFT37 Mapa Integral de Riesgos / Correo electrónico
7	© Revisar la definición/actualización del Mapa de Riesgos Recepcionar formato Mapa Integral de Riesgos y revisar la definición/actualización del Mapa de Riesgos, para tal efecto verificar que se haya aplicado correctamente la metodología.	2da Línea de Defensa	Cada vez que se requiera	DEFT37 Mapa Integral de Riesgos
	¿La definición/actualización del Mapa de Riesgos requiere ajustes? Si: Devolver a la actividad No.1 No: Continuar a la actividad No.8	2da Línea de Defensa	Cada vez que se requiera	DEFT37 Mapa Integral de Riesgos
8	© Realizar seguimiento y monitoreo 1ra Línea de Defensa	1ra Línea de Defensa	Trimestral	Registro de monitoreo

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

N.	Actividad	Responsable	Tiempo o frecuencia si aplica	Registro
	Realizar seguimiento continuo a los riesgos, controles y planes de tratamiento. Las actividades incluyen: • Revisar periódicamente los KRI definidos para cada riesgo, evaluando su comportamiento frente a los umbrales establecidos. • Verificar el cumplimiento de las acciones contenidas en los planes de tratamiento, asegurando que se ejecuten en los tiempos definidos y que contribuyan efectivamente a la mitigación del riesgo. • Determinar si los controles están funcionando adecuadamente o requieren ajustes. • Con base en los resultados del monitoreo, proponer ajustes a los controles, actualizar los mapas de riesgos. • Cuando se evidencie dentro de la operación normal del proceso un evento de materialización de un riesgo, registrar en la herramienta dispuesta por la Entidad para tal fin. De acuerdo con lo establecido en la Política de Operación No.10			
	¿Se presenta un evento de materialización del riesgo? Si: Devolver a la actividad No.1 No: Continuar a la actividad No.9	1ra Línea de Defensa	Cada vez que se requiera	Registro de monitoreo

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

N.	Actividad	Responsable	Tiempo o frecuencia si aplica	Registro
9	Realizar seguimiento y monitoreo 2da Línea de Defensa Realizar seguimiento continuo y verificar que los riesgos, controles y planes de tratamiento definidos por la primera línea de defensa estén siendo gestionados adecuadamente. Para tal efecto: - Analizar los reportes de seguimiento realizados por los líderes de proceso, verificando la consistencia, oportunidad y calidad de la información sobre riesgos, controles y planes de tratamiento. - Consolidar y evaluar los KRI definidos por los procesos, identificando tendencias, desviaciones y alertas que puedan requerir acciones correctivas o preventivas. - Verificar el avance en la ejecución de los planes de tratamiento, identificando retrasos, obstáculos o desviaciones que puedan comprometer la gestión del riesgo.	2da Línea de Defensa	Trimestral	Informe de monitoreo de 2da Línea de Defensa
10	Realizar seguimiento y monitoreo 3ra Línea de Defensa Ejecutar actividades de evaluación independiente sobre la eficacia del sistema de gestión de riesgos, controles y cumplimiento institucional. Para tal efecto: - Evaluar si los riesgos han sido identificados, valorados y tratados adecuadamente por la primera y segunda línea de defensa. - Verificar la eficacia, eficiencia y suficiencia de los controles implementados.	3da Línea de Defensa	Trimestral	Informe de monitoreo de 3ra Línea de Defensa

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

N.	Actividad	Responsable	Tiempo o frecuencia si aplica	Registro
	- Analizar los Indicadores Clave de Riesgo (KRI) reportados por las líneas anteriores, evaluando su pertinencia, seguimiento y utilidad para la toma de decisiones. - Comprobar el cumplimiento de los planes de tratamiento del riesgo, su alineación con los objetivos institucionales y su impacto en la mitigación de riesgos.			
11	Presentar resultados de la Gestión Integral del Riesgo De acuerdo con la programación del comité institucional de coordinación de control interno, se presentan los resultados de la Gestión Integral del Riesgo con el fin de retroalimentar a la Alta Gerencia sobre el cumplimiento de las responsabilidades a cargo y la socialización de recomendaciones resultantes frente a esta gestión de riesgos en los procesos. Cada vez que se requiera y de acuerdo con los criterios indicados en la política de operación 10, se podrá realizar actualización de las matrices de riesgos siguiendo la ruta metodológica definida en este procedimiento.	2da Línea de Defensa	Cada vez que se requiera	Acta de reunión / Listado de Asistencia

ANEXOS

No aplica

Control de cambios		
Versión	Fecha	Descripción de los cambios

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

1	27/11/2025	Se crea el procedimiento con base en los lineamientos definidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 (DAFP). Este procedimiento sustituye lo contenido en el proceso Direccionamiento estratégico (DEPD01) en la actividad clave de éxito “Gestionar riesgos” y en el proceso Gestión de mejora (GMPR01) en la actividad clave de éxito “Realizar monitoreo, seguimiento y evaluación del riesgo”.			
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

	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	DEPD06
	PROCEDIMIENTO GESTIÓN DEL RIESGO	VERSIÓN	01
		FECHA	27/11/2025

