

REPÚBLICA DE COLOMBIA



SUPERINTENDENCIA NACIONAL DE SALUD

RESOLUCIÓN NÚMERO DE 2017

“Por medio de la cual se establecen los lineamientos generales del marco de la Supervisión Basada en Riesgos del Sistema General de Seguridad Social en Salud”

EL SUPERINTENDENTE NACIONAL DE SALUD

En uso de sus facultades legales y reglamentarias, en especial las conferidas por la Ley 100 de 1993, el literal a) del artículo 39 de la Ley 1122 de 2007 y los artículos 6, numeral 4, y 7, numeral 5, del Decreto 2462 de 2013 y,

CONSIDERANDO

Que el Sistema General de Seguridad Social en Salud (SGSSS) ha logrado avances importantes en términos de cobertura universal, homologación de planes de beneficios entre los regímenes y mayor acceso a servicios de salud de la población colombiana. Sin embargo, el sistema está expuesto a diversos riesgos que pueden afectar su operación y el logro de sus objetivos en términos de resultados de salud en la población.

Que el Gobierno Nacional ha impulsado una serie de intervenciones dirigidas al fortalecimiento técnico, operativo y administrativo de los agentes participantes del sistema, el cual comprende la redefinición de los criterios para la habilitación y permanencia financiera de las EPS (Decreto 2702 de 2014 y sus modificaciones), la adopción de un modelo integral de atención en salud con énfasis en resultados (Resolución 429 de 2016), entre otras medidas. Estos nuevos aspectos están incluidos en el modelo de Supervisión Basada en Riesgos (SBR) de la Superintendencia Nacional de Salud (SNS), quien encabeza el Sistema de Inspección, Vigilancia y Control (IVC) del sector salud, de acuerdo con la Ley 1122 de 2007.

Que de conformidad con el artículo 14 de la Ley 1122 de 2007, se entiende por aseguramiento en salud la administración del riesgo financiero, la gestión del riesgo en salud y la articulación de los servicios que garanticen el acceso efectivo, la garantía de la calidad en la prestación de los servicios de salud y la representación del afiliado ante el prestador y los demás actores, sin perjuicio de la autonomía del usuario.

Que aunado a lo anterior, la SNS adelantó los estudios necesarios sobre experiencias internacionales y sectoriales para identificar reconocidas metodologías e instrumentos que le permitan realizar una adecuada identificación, seguimiento y control de prácticas riesgosas de sus entidades supervisadas en todos los aspectos, con lo cual evidenció los beneficios y determinó a la SBR como la mejor modalidad para su desarrollo, al ser una adecuada práctica internacional que responde a las exigencias del Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud del Sistema General de Seguridad Social en Salud. De esta manera, los sistemas de gestión de riesgos de las entidades supervisadas constituyen las medidas preventivas por excelencia para el control y mitigación de las prácticas riesgosas que atentan contra la estabilidad del SGSSS.

Que la SBR es la estrategia que está implementando la SNS para complementar a la Supervisión Basada en el Cumplimiento, y de esta manera garantizar la protección de los derechos de los usuarios y el cumplimiento de las normas que regulan el sistema, al utilizar ambas formas de Supervisión de forma combinada y transversal.

Que la SBR busca en el marco de un modelo de supervisión prudencial y activo, fortalecer el SGSSS a través de una mayor estabilidad de las diferentes instituciones que lo componen, apoyada en una cultura de autocontrol y adecuados sistemas de administración o gestión de riesgos.

Que mediante el Decreto 1599 de 2005 se adoptó el Modelo Estándar de Control Interno (MECI) para todas las entidades del Estado, en el que la "Administración del Riesgo" se define como uno de los componentes del módulo de Control de Planeación y Seguimiento, y este a su vez cuenta con tres (3) elementos: **i)** Políticas de Administración del Riesgo; **ii)** Identificación del Riesgo y **iii)** Análisis y Valoración del Riesgo, lo que le permite a las entidades públicas del sector salud contar con experiencia en la gestión de riesgos, la cual, requiere ser adaptada a los requerimientos propios del SGSSS.

Que el Decreto 943 de 2014 derogó el Decreto 1599 de 2005 y actualizó el MECI, con el que se proporciona a las entidades del Estado, una estructura para el control de la estrategia, la gestión y la evaluación, y cuyo propósito es orientarlas hacia el cumplimiento de sus objetivos institucionales y la contribución de estos, a los fines esenciales del Estado bajo los principios de autocontrol, autorregulación y autogestión.

Que la Ley 1438 de 2011 por la cual se fortalece el SGSSS, introduce un modelo de prestación del servicio público en salud en el marco de la estrategia de Atención Primaria en Salud y fortalece a la SNS en sus funciones de IVC, particularmente en las entidades territoriales, con la reestructuración y la desconcentración planteadas en esta Ley.

Que el artículo 12 de la Ley 1474 de 2011 o Estatuto Anticorrupción, crea el Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud del SGSSS y ordena a la SNS, entre otras cosas, definir para sus sujetos vigilados, el conjunto de medidas preventivas para su control, así como los indicadores de alerta temprana y ejercer sus funciones de Inspección, Vigilancia y Control (IVC) sobre la materia.

Que para hacer efectivo el Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud, mediante el Decreto 2462 de 2013 se modificó la estructura de la SNS y se creó la Oficina de Metodologías de Supervisión y Análisis de Riesgo y el Despacho del Superintendente Delegado para la Supervisión de Riesgos; unidades con funciones concretas de diseño, vigilancia, recolección y análisis de información relevante para la aplicación de la SBR mediante la identificación y prevención de riesgos con la incorporación de alertas tempranas.

Que la experiencia en la implementación voluntaria del Sistema de Administración de Riesgos (SAR) en las Entidades Promotoras de Salud (EPS) del régimen contributivo y entidades adaptadas, introducido por la Resolución 1740 de 2008, posteriormente derogada por el Decreto 2702 de 2014, permitió establecer su importancia para el fortalecimiento institucional de las entidades supervisadas e identificar la necesidad de unificar definiciones y conceptos que permitan profundizar en las diferentes categorías de riesgos.

Que las experiencias previas del SAR y el MECI, han determinado la necesidad que las entidades supervisadas cuenten con una estructura encargada de monitorear los riesgos que dependa del máximo órgano decisorio de dichas supervisadas.

Que la Ley 1753 de 2015 por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "*Todos por un nuevo país*", expone en su Prioridad VI, Movilidad Social, Objetivo 2, Mejorar las condiciones de salud de la población colombiana y propiciar el goce efectivo del derecho a la salud, en condiciones de calidad, eficiencia, equidad y sostenibilidad; Objetivo específico c. Recuperar la Confianza y la legitimidad en el sistema; que una vez culminada la primera fase del fortalecimiento de la dimensión de supervisión (funciones de IVC), a partir de un enfoque de gestión de riesgo, la SNS deberá implementar un modelo de SBR que establezca para las entidades vigiladas la obligatoriedad de la identificación de los riesgos y el establecimiento de controles, para que a su vez la SNS realice la supervisión basada en la evaluación de la gravedad, la probabilidad de los riesgos significativos a los que están expuestos los sujetos vigilados y la efectividad de los controles, con el fin de anticiparse a situaciones indeseables, no solo desde el punto de vista financiero en el sistema, sino también en la gestión de riesgo en salud.

Que la Resolución 429 de 2016 expedida por el Ministerio de Salud y Protección Social (MSPS) por la cual se adopta la Política de Atención Integral en Salud (PAIS), desarrollando un marco estratégico y un modelo operacional (Modelo Integral de Atención en Salud - MIAS) que buscan permitir la acción coordinada de las normas, reglas, reglamentos, agentes y usuarios, a efectos de orientar la intervención de los diferentes integrantes hacia la generación de las mejores condiciones de salud de la población y el goce efectivo del derecho fundamental a la salud, al interrelacionar los elementos

esenciales que lo configuran, mediante un enfoque de resultados y la Gestión Integral del Riesgo en Salud (GIRS).

Que, en virtud de lo anteriormente expuesto,

RESUELVE

ARTÍCULO PRIMERO. OBJETO. Establecer los lineamientos generales del modelo de la Supervisión Basada en Riesgos (SBR) para la identificación, evaluación, medición, control, seguimiento y monitoreo de los riesgos a los que se encuentran expuestas las entidades supervisadas por la Superintendencia Nacional de Salud, para prevenir posibles impactos negativos y mejorar los resultados en salud, la satisfacción de los usuarios, la estabilidad financiera del sistema y fortalecer la confianza de la población en los componentes de salud del Sistema General de Seguridad Social (SGSS). Lo anterior, bajo el marco del Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud establecido por el artículo 12 de la Ley 1474 de 2011.

La evaluación de los riesgos de las entidades supervisadas, permite identificar los principales determinantes de los eventos de riesgo, el impacto de los riesgos inherentes y la correspondencia y efectividad de los controles implementados, para así determinar las prioridades e intensidad del trabajo de supervisión por parte de la SNS sobre los vigilados del sistema, y de esta forma, cumplir con los objetivos misionales, al identificar alertas tempranas de los eventos de riesgo y adoptar medidas correctivas y preventivas.

Asimismo, por medio de la implementación de este modelo, se busca:

- Fortalecer la prestación del servicio y el cumplimiento de metas en salud, para velar por el mejoramiento de la salud de los individuos y la mitigación de los riesgos en salud, brindando servicios con mayor calidad y oportunidad.
- Dirigir la supervisión desde un enfoque preventivo, estableciendo un perfil de riesgo que permita determinar la prioridad de supervisión para cada vigilado y optimizar el uso de los recursos de supervisión para los riesgos más significativos y que puedan amenazar la estabilidad del SGSS.
- Incrementar la probabilidad de que los eventos de mayor impacto sean detectados a tiempo y prevenidos antes de que se materialicen.
- Incentivar a las entidades vigiladas a identificar, gestionar y monitorear sus riesgos, bajo un esquema eficiente de autorregulación.
- Fomentar una cultura de gestión de riesgos por parte de los vigilados, de manera que esta sea una política empresarial o de gobierno organizacional que se interiorice en toda la estructura corporativa, incluyendo políticas de control interno.
- Generar condiciones de estabilidad operativa y financiera de las instituciones que componen el sector salud, a través de la implementación de Sistemas de Gestión de Riesgos estratégicamente diseñados e implementados y debidamente documentados mediante Políticas de Gestión de Riesgo y manuales de procesos y procedimientos donde incluyan Metodologías de valoración de riesgos y las funciones de los Órganos de control (Control Interno y Revisoría Fiscal).
- Robustecer la infraestructura de supervisión dentro de las entidades que componen el SGSS (Auditoría Interna, Revisoría Fiscal y/o Contralor Normativo, entre otros), encaminada a fortalecer el control y gestión de riesgos al interior de las entidades supervisadas.
- Promover la cultura de autocontrol hacia una supervisión y administración basada en riesgos que desarrolle habilidades evaluativas sobre la calidad de la gestión de riesgos de cada entidad.
- Aumentar el compromiso y responsabilidad de las Juntas Directivas y órganos administrativos de las entidades frente a la adecuada gestión de los riesgos, además de establecer criterios de idoneidad y reputación para la Alta Gerencia.
- Consolidar los canales de comunicación coordinados entre la SNS y las entidades, que permitan desarrollar espacios de discusión constructiva (por ejemplo, mesas de trabajo con el sector) y

faciliten la puesta en marcha de los diferentes cambios normativos, producto de este proceso de adaptación.

- Estimular la transparencia, la calidad, la preservación de la información y la mejora continua en todos los procesos relacionados, como insumo fundamental para la gestión de los diversos riesgos que permitan implementar y fortalecer la SBR.
- Impulsar las mejores prácticas de Gobierno Organizacional y los Códigos de Ética y Conducta en el sector de la salud.

ARTÍCULO SEGUNDO. ÁMBITO DE APLICACIÓN. La presente Resolución está dirigida a los representantes legales, socios, accionistas, revisores fiscales, la Alta Gerencia, los Máximos Órganos Sociales, Oficiales de Cumplimiento, administradores y personas naturales o jurídicas que hacen parte de los Integrantes del Sistema General de Seguridad Social (SGSS) vigilados por la Superintendencia Nacional de Salud.

Las disposiciones de la presente Resolución serán de aplicación y obligatorio cumplimiento para todas las entidades vigiladas por la Superintendencia Nacional de Salud, de acuerdo con la función de cada uno dentro del SGSS.

ARTÍCULO TERCERO. DEFINICIONES. Las definiciones para el entendimiento e interpretación de los lineamientos generales del marco de la Supervisión Basada en Riesgos objeto de esta Resolución, son las siguientes:

- **Administrador:** De acuerdo con el artículo 22 de la Ley 222 de 1995, "son administradores el representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones". El administrador debe obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios. Sus actuaciones se cumplirán en interés de la sociedad, teniendo en cuenta los intereses de sus asociados, y en el cumplimiento de su función, deben realizar como mínimo las expresadas en el artículo 23 de la mencionada Ley.
- **Alta Gerencia:** Personas del más alto nivel jerárquico en el área administrativa (denominados administradores) u organizacional de la entidad. La Junta Directiva la hace responsable del giro ordinario del negocio de la sociedad y la encarga de idear, ejecutar y controlar los objetivos y estrategias de la misma. También se incluye en la Alta Gerencia al Auditor Interno.
- **Asamblea General:** Reunión colectiva de los miembros del Máximo Órgano Social, que puede darse de manera ordinaria o extraordinaria, según lo establece el Código de Comercio o la norma que regule cada tipo especial de entidad y los estatutos de la entidad.
- **Categorías prioritarias de riesgo,** agrupadores de distintos tipos de riesgos en torno a un elemento común, prioritarios para fines de supervisión definidos por la SNS.
- **Ciclo general de gestión de riesgo,** son las etapas que incorpora un Sistema de Gestión de Riesgos para cada uno de los tipos o categorías de riesgo.
- **Contralor Normativo:** Puede ser un cargo o un área especializada dentro o fuera de la organización. El contralor normativo es nombrado por la Junta Directiva o quien haga sus veces, y ejerce control para asegurar la observancia de las disposiciones normativas aplicables, por lo que las funciones del contralor son dependientes de la Junta o quien haga sus veces, a quien debe asesorar y rendir cuentas.
- **Controles,** medidas prudenciales y correctivas que ayudan a contrarrestar la exposición a los diferentes riesgos. Entre estas se encuentra la implementación de políticas, procesos, prácticas u otras estrategias de gestión.
- **Junta Directiva:** Es el máximo órgano colegiado encargado de la dirección de la entidad. Sus miembros se conocen como directores. Lo aquí dispuesto para la Junta Directiva y sus directores se entiende dicho para el Consejo de Administración de las cooperativas y sus consejeros, respectivamente. Tal denominación puede variar según la figura jurídica de la que se trate.

- **Máximo Órgano Social:** Es el máximo órgano de gobierno de la entidad. Es la Asamblea General o quien haga sus veces y puede variar su denominación según la figura jurídica de la que se trate. Se entenderán "miembros del Máximo Órgano Social" o "miembros" al accionista, en el caso de una sociedad comercial por acciones, al socio en las sociedades comerciales con cuotas o partes de interés, al miembro en una mutual, al cooperado en una cooperativa, al empresario afiliado en caso de una caja de compensación, al miembro del Consejo del más alto rango en una Fundación, o por cualquier denominación que se adopte de acuerdo con la naturaleza jurídica de la respectiva entidad.

Su principal función es velar por el cumplimiento de los objetivos misionales de la entidad, mediante la realización de Asambleas, que pueden darse de manera ordinaria o extraordinaria, según lo establece el Código de Comercio o la norma que regule cada tipo especial de entidad y los estatutos de la entidad.

- **Presidente Ejecutivo:** Posición individual dentro de la entidad que responde ante la Junta Directiva. El Presidente Ejecutivo es el máximo responsable del giro ordinario de la entidad y a él reportan de forma directa la mayoría de los miembros de la Alta Gerencia. También identificado como Gerente General o Director General y generalmente actúa como Representante Legal Principal o Titular de la sociedad. Tal denominación puede variar según la figura jurídica de la que se trate.
- **Riesgo,** es la posibilidad de que ocurra un evento adverso que pueda afectar negativamente el cumplimiento de la operación de una Entidad y que atenten contra los objetivos del SGSSS.
- **Riesgo inherente,** cualquier nivel de riesgo propio de la actividad, cuya evaluación se efectúa sin considerar el efecto de los mecanismos de mitigación y de control.
- **Riesgo residual,** es el nivel de riesgo que resulta luego de la aplicación de las medidas de control o mitigación existentes a los riesgos inherentes.
- **Riesgo neto global,** es el resultado de la combinación de cada uno de los riesgos residuales de la entidad supervisada, teniendo en cuenta su importancia relativa.
- **Supervisión Basada en Riesgos,** es un proceso dinámico y continuo mediante el cual se busca identificar los factores de riesgo que presentan mayores amenazas para la Entidad, además de evaluar la gestión que ésta realiza para mitigar y evitar que dichos riesgos se materialicen.

ARTÍCULO CUARTO. RIESGOS PRIORITARIOS. Las entidades vigiladas deben gestionar todos los riesgos que se presenten dentro de su operación, y dependerán de la discrecionalidad y organización que cada entidad supervisada les quiera dar para su tratamiento. Sin embargo, deberá contemplar como mínimo, de acuerdo a su función dentro del SGSS, los siguientes:

A. Área de riesgo en Salud: Compuesta como mínimo, por las siguientes dos categorías:

- I. **Resultados sanitarios.** La probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo, que puede ser también el empeoramiento de una condición previa, la necesidad de requerir más consumo de bienes y servicios que hubiera podido evitarse. El evento, la ocurrencia de la enfermedad / traumatismos o su evolución desfavorable y sus causas son los diferentes factores asociados (Definición del Plan Decenal de Salud Pública del MSPS 2012-2021).
- II. **Actuarial.** Esta categoría aplica principalmente para las Entidades Administradoras de Planes de Beneficios (EAPB) vigiladas integralmente por la SNS y para Instituciones Prestadoras de Salud (IPS) que mantengan contrataciones por capitación que representen más del 40% de sus ingresos operativos (este límite se monitoreará constantemente y podrá ser ajustado en el futuro de ser necesario).

Esta categoría incluye principalmente los siguientes tipos:

- **Riesgos de concentración y hechos catastróficos:** Corresponde a la probabilidad de pérdida en que puede incurrir una entidad supervisada como consecuencia de una concentración de riesgos, bien sea por género, franjas de edades, regiones, patologías,

por la ocurrencia de hechos catastróficos o situaciones similares que afecten un número elevado de afiliados.

- **Riesgos de incremento inesperado en los índices de morbilidad y en los costos de atención:** Corresponde a la probabilidad de pérdida de un periodo contable que se genera como consecuencia de diferencias apreciables entre las condiciones de morbilidad asumidas y las actuales, así como pérdidas derivadas de incrementos inesperados en los costos de atención.
- **Riesgos de cambios permanentes en las condiciones de salud o cambios tecnológicos:** Corresponde a la probabilidad de que ocurran cambios permanentes en las condiciones de salud de la población objetivo o derivados de la disponibilidad e incorporación al plan de beneficios de nuevas tecnologías, que requieran ajustes en la financiación de este plan de beneficios.
- **Riesgos de insuficiencia de reservas técnicas:** Probabilidad de pérdida como consecuencia de una subestimación en el cálculo de las reservas técnicas y otras obligaciones contractuales (servicios autorizados y servicios facturados).
- **Riesgo de tarificación:** Probabilidad de pérdida como consecuencia de que las tarifas o precios calculados por la entidad, en aquellos planes diferentes al Plan de Beneficios / Plan Obligatorio de Salud (POS), resulten insuficientes para cubrir las obligaciones futuras que de ellos se deriven.

B. Área de riesgos económicos: Compuesta como mínimo por las siguientes tres categorías:

- I. **Riesgo de Liquidez.** Es la probabilidad que una entidad no tenga la capacidad financiera para cumplir sus obligaciones de pago tanto a corto, como a largo plazo. En el caso de las EPS del régimen contributivo y subsidiado, se consideran parte de las obligaciones las reservas técnicas que exija la normatividad vigente. También se consideran parte de las obligaciones, los compromisos de inversiones destinados a las reposiciones que puedan llegar a afectar la continuidad de la operación.
- II. **Riesgo de Crédito.** Es la probabilidad que una entidad incurra en pérdidas como consecuencia de que sus deudores no cumplan sus obligaciones en los términos acordados.
- III. **Riesgo de Mercado de Capitales.** Corresponde a la probabilidad de incurrir en pérdidas derivadas de un incremento no esperado, de sus obligaciones con acreedores externos o la pérdida en el valor de sus activos, por causa de las variaciones en las tasas de interés, en la tasa de cambio o cualquier otro parámetro de referencia que afecte el valor del Activo.
- IV. **Riesgo de Grupo.** La probabilidad de pérdida que surge como resultado de transacciones con entidades que forman parte del mismo grupo empresarial. Éste se deriva de la exposición a fuentes de riesgo adicionales a las propias del negocio de la entidad, por el hecho de mantener operaciones o transacciones con empresas relacionadas que pudiesen incumplir sus compromisos. Los riesgos pueden ser directos, mediante exposición financiera, o indirectos, mediante daño a la reputación.
- V. **Riesgo de Fallas del mercado de salud.** La probabilidad que la estructura del mercado de salud genere pérdidas en el bienestar y beneficios de la entidad. Ejemplos: mercado monopólico, oligopólico, monopsonio; prácticas de competencia desleal (selección de riesgo, barreras de acceso a los servicios, etc.), entre otros.
- VI. **Riesgo de Lavado de activos y financiación del Terrorismo.** Es la posibilidad que, en la realización de las operaciones de una entidad, estas puedan ser utilizadas por organizaciones criminales como instrumento para ocultar, manejar, invertir o aprovechar dineros, recursos y cualquier otro tipo de bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos de recursos vinculados con las mismas.

C. Área de riesgos operativos: Compuesta como mínimo por las siguientes categorías de riesgos:

- I. **Riesgo Operacional.** Es la probabilidad que una entidad presente desviaciones en los objetivos de sus procesos como consecuencia de deficiencias, inadecuaciones o fallas en los procesos, en el talento humano, en los sistemas tecnológicos y biomédicos, en la infraestructura, por fraude y corrupción, o acontecimientos externos, entre otros, que impliquen pérdidas.

Se reconocen al menos 5 ámbitos de gestión del riesgo operacional:

- De los procesos de las operaciones.
- De los procesos con actores externos para garantizar el objeto del servicio; en el caso de las EPS del régimen contributivo y subsidiado, el acceso y prestación de los servicios de salud. Para las IPS (Instituciones Prestadoras de Servicios de Salud), la externalización de procesos y servicios complementarios de atención.
- De tecnologías de la información y comunicación.
- Del recurso humano.
- De la continuidad de negocio y recuperación de desastres.

Para la gestión del riesgo operacional se recomienda la adopción de normas técnicas nacionales o internacionales. En cualquiera de los casos la entidad supervisada deberá contar con mapas de procesos en los que se identifique su criticidad de acuerdo con el riesgo inherente. No obstante, ésta Superintendencia supervisará en especial los procesos relacionados con las garantías de acceso a los servicios de salud, la oportunidad, continuidad y calidad de los mismos.

- II. **Riesgo Reputacional.** La probabilidad que el buen nombre y prestigio de una entidad supervisada sea afectada negativamente por uno o más de un evento reputacional, tal como el impacto de la publicidad negativa sobre las prácticas comerciales de la entidad, conducta o situación financiera. Tal publicidad negativa, ya sea verdadera o no, puede mermar la confianza pública en la entidad, dar lugar a litigios costosos, o dar lugar a una disminución de su base de clientes, los negocios o los ingresos.

Para cada uno de los riesgos prioritarios descritos anteriormente, se deberá contar con una definición específica adaptada dentro de la política de gestión de riesgos de la entidad supervisada, así como con metodologías de estimación del riesgo y procedimientos de gestión, en los que se fijen montos o límites de aceptación, además de conductas de actuación en situaciones de normalidad o de estrés.

Las metodologías seleccionadas deberán tomar en cuenta el comportamiento histórico y la capacidad de formular proyecciones futuras.

Adicionalmente, cada categoría deberá contar con mecanismos de comunicación y reporte a los organismos de Gobierno Organizacional ante los posibles desajustes y resultados de la administración.

ARTÍCULO QUINTO. CICLO GENERAL DE GESTIÓN DE RIESGO. Para cada una de las categorías de riesgo a supervisar por ésta Superintendencia, se incluyen las siguientes etapas:

1. **Identificación de riesgos:** Consiste en reconocer, explorar exhaustivamente y documentar todos los riesgos internos y externos que podrían afectar tanto los objetivos de la entidad supervisada como la salud de los usuarios a su cargo, en los casos que aplica, identificando sus causas, efectos potenciales y la posible interrelación entre los diferentes tipos de riesgos, para lo cual se recomienda la utilización de normas técnicas nacionales o internacionales.

Para esta identificación, las entidades supervisadas podrán seleccionar las metodologías y técnicas que consideren más adecuadas, dentro de las que se encuentran encuestas, entrevistas estructuradas con expertos, talleres, lluvia de ideas, técnicas de escenarios, entre otros.

2. **Evaluación y medición de riesgos:** Es la valoración de los efectos asociados a los riesgos que han sido identificados, considerando la frecuencia y la severidad de su ocurrencia. También se

deberá considerar el análisis de los riesgos inherentes y residuales, y su participación en el riesgo neto global.

Se entenderá por valoración del riesgo la medida, cualitativa o cuantitativa, de su probabilidad de ocurrencia y su posible impacto.

En la medida que avance el plan de implementación del modelo de Supervisión Basada en Riesgos, las entidades deberán contar, en la medida de lo posible, con evaluaciones cuantitativas relacionadas con la probabilidad de ocurrencia de los riesgos identificados y su impacto. Independientemente de contar con modelos cuantitativos o cualitativos, estos deben estar sustentados técnicamente y documentados.

3. Selección de estrategias para el tratamiento y control de los riesgos. Una vez identificados y evaluados los riesgos, deben compararse con los límites (tolerancia) de riesgos aprobados por la instancia definida en el Gobierno Organizacional de la entidad supervisada y su política de riesgos. Todo riesgo que exceda los límites aceptados debe ser objeto de actividades de mitigación y control a fin de regresar al nivel de riesgo tolerado, conforme la estrategia adoptada.

Se deben determinar las acciones tendientes a gestionar los riesgos a los que se ve expuesta la entidad supervisada, de acuerdo con los niveles de riesgo determinados y las tolerancias al riesgo definidas.

Todas las acciones de gestión del riesgo deberán identificar formalmente responsables, plazos y formas de ejecución, y reportes de avances. Asimismo, deberán estar aprobadas por la instancia del Gobierno Organizacional que corresponda.

La SNS en su labor de IVC evaluará las funciones de control que tenga cada entidad en lo correspondiente al análisis financiero, el cumplimiento, la gestión de riesgos, la actuaría, la auditoría interna, el Gobierno Organizacional, la Alta Gerencia y la Junta Directiva o quien haga sus veces. La existencia y características de estas funciones dependerán de la naturaleza, tamaño y complejidad de cada Entidad.

4. Seguimiento y monitoreo. Una vez establecidos los posibles mecanismos o conjunto de mecanismos para la mitigación y control de los riesgos que se han identificado como relevantes para la entidad supervisada, ésta deberá poner en práctica tales mecanismos y reflejarlos en el plan de implementación. Todas las acciones deberán contar con un responsable, plazos, reportes de avance y de evaluaciones periódicas sobre las acciones que incluyan monitoreo de los indicadores propuestos para el seguimiento de las acciones de gestión del riesgo planteadas. Definidos mediante cronograma, dichos reportes de avance deben pasar por un proceso de verificación y calidad de la información.

Las mediciones de riesgos esperadas, los riesgos derivados y sus controles deben ser contrastados regularmente con la realidad observada, de forma tal que permita establecer si los sistemas de gestión de riesgos han logrado corregir oportunamente eventuales deficiencias.

En esta etapa cobra importancia la comunicación y entrega de resultados a todos los involucrados y responsables, en especial a los órganos de seguimiento definidos por el Gobierno Organizacional.

ARTÍCULO SEXTO. MARCO GENERAL DE SUPERVISIÓN. El Marco Institucional para la gestión de riesgos de cada entidad (políticas, procesos y procedimientos) y los distintos tipos y categorías de riesgos prioritarios que afectan negativamente la estabilidad del SGSS, serán supervisados de acuerdo con lo que defina la SNS para cada tipo de riesgo, teniendo en cuenta las funciones y el rol de cada vigilado dentro del SGSS.

ARTÍCULO SÉPTIMO. ASPECTOS DE SUPERVISIÓN. Para los efectos de aplicar el Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud, la Superintendencia Nacional de Salud evaluará, en las entidades vigiladas, los siguientes aspectos:

- **Calidad del marco institucional de gestión de riesgos:** el cual deberá estar integrado a la estructura organizacional y los procesos de la entidad supervisada, además de contar con mecanismos de rendición de cuentas y de comunicación.

- **Calidad en la aplicación del ciclo de gestión de riesgos:** hace referencia a las etapas en la gestión para cada uno de los tipos o categorías de riesgo.
- **Calidad del gestor / Junta Directiva o quien haga sus veces:** los lineamientos de los directivos deben abordar temas como responsabilidades, experiencia, competencia e integridad, además de los procesos a seguir ante la presencia de conflictos de interés.
- **Controles de gestión:** comprende la estructura de administración y la gestión de calidad, además de los procesos de toma de decisiones, de planificación estratégica y la actitud de control de riesgo que la Administración de la entidad tiene implementado.
- **Plan de continuidad dada la contingencia:** se refiere al mecanismo para identificar con antelación situaciones de riesgo que pueden afectar la operación, actividades a realizar cuando se presentan fallas o interrupciones, alternativas de operación y regreso a la actividad normal.

Asimismo, mediante este plan se busca administrar y operar una entidad en situaciones inusuales de una manera oportuna y eficaz.
- **Procedimientos y cultura de cumplimiento:** relativa al cumplimiento de la legislación y la regulación, involucra evaluación de la competencia, integridad e independencia del personal responsable, así como la eficacia de los sistemas de información.
- **Efectividad de la gestión operativa:** hace referencia a promover entornos con estructura organizacional transparente, relaciones claras entre actividades, unidades de administración y funciones de grupo, que faciliten y garanticen la administración de los riesgos inherentes.
- **Idoneidad de los sistemas de gestión de riesgo:** implica la adopción de sistemas para identificar y medir los riesgos, fijar límites, monitorear que los controles sean suficientes y presentar los respectivos reportes a las instancias respectivas. Adicionalmente, dentro del marco institucional de gestión de riesgos, la SNS evaluará las funciones de controles específicos de riesgos que cada entidad haya incorporado en cuanto a reportes en salud, financieros y administrativos, controles de riesgo de operaciones, controles de auditoría interna, controles de cumplimiento, controles de tecnologías de información, controles de Recursos Humanos (RRHH), controles de gestión de riesgos, actuaría y Gobierno Organizacional (entre ellos la Alta Gerencia y la Junta Directiva). Asimismo, se tiene que prever que el modelo de gestión debe ser fácilmente ajustable y adaptable a los cambios en el perfil de riesgos de cada entidad.
- **Idoneidad de la revisión independiente:** este factor se refiere tanto a la independencia como a las competencias al aplicar los más altos criterios profesionales de los auditores o quien haga sus veces, así como de la calidad de sus reportes y funciones.

PARÁGRAFO PRIMERO. Las Entidades deben tener la capacidad institucional para evaluar, controlar y mitigar los riesgos que puedan afectar el logro de sus objetivos y, especialmente, el cumplimiento de los objetivos del SGSS y sus obligaciones contractuales.

PARÁGRAFO SEGUNDO. La SNS velará por la generación y monitoreo de los perfiles de riesgo de las entidades vigiladas a partir de la información recibida por ellos y la que reciba de terceros como el MSPS, el Departamento Administrativo de la Función Pública (DAFP), el Ministerio de Hacienda y Crédito Público, demás Superintendencias, entre otros, incluyendo el seguimiento a los riesgos inherentes, los controles, los riesgos residuales y los riesgos netos globales de las entidades supervisadas, bajo el marco de la Supervisión Basada en Riesgos en salud, económicos y operativos, incluidos en esta Resolución.

PARÁGRAFO TERCERO. La SNS hará evaluaciones específicas de la capacidad de gestión de las categorías de riesgos prioritarios de acuerdo con el perfil de riesgo de cada entidad supervisada, las reclamaciones de los usuarios y otros criterios que identifique ésta Superintendencia.

PARÁGRAFO CUARTO. Posteriormente, y de manera progresiva se estarán expidiendo instrucciones adicionales para la implementación, los detalles de la medición estándar y los aspectos de supervisión para cada una de las categorías de riesgos prioritarios y para cada tipo de vigilado, de acuerdo a su función dentro del SGSS.

ARTÍCULO OCTAVO. PLAZOS PARA LA IMPLEMENTACIÓN. Los elementos descritos en el presente acto administrativo tendrán como plazo máximo para su implementación lo siguiente:

Etapa	Entregables	Plazo máximo
Definición marco institucional del riesgo	<p>La definición de la instancia de gobierno organizacional que tendrá a cargo la implementación del <i>Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud del Sistema General de Seguridad Social en Salud (dependencias o áreas involucradas, junto a la definición de funciones)</i>.</p> <ul style="list-style-type: none"> • La determinación del plan de implementación (objetivos, estrategias, actividades, responsables y plazos) • Los lineamientos generales para la gestión de riesgos en la entidad. 	3 meses
Identificación de riesgos	<ul style="list-style-type: none"> • La identificación o actualización de los diferentes tipos de riesgos internos y externos que pueden afectar el cumplimiento del objeto social de la entidad. • La descripción para cada tipo de riesgo identificado de: causa del riesgo, evento de riesgo y efecto(s) del riesgo. • El análisis de relación entre los diferentes tipos de riesgo identificados. 	3 meses
Evaluación y medición de riesgos	<ul style="list-style-type: none"> • Evaluación cualitativa y/o cuantitativa del impacto y la probabilidad de ocurrencia de cada uno de los riesgos identificados. • Matriz de priorización de riesgos según la evaluación de su severidad 	6 meses
Selección de estrategias para el tratamiento y control de los riesgos	<ul style="list-style-type: none"> • Definición de las estrategias de tratamiento y control para todos los riesgos priorizados. • Detalle de acciones con plazos y responsables para llevar a cabo las estrategias definidas. • Valoración del costo de la estrategia. • Determinación del riesgo residual. 	3 meses
Seguimiento y monitoreo	<ul style="list-style-type: none"> • Definición de mecanismos y periodicidades de seguimiento y monitoreo al <i>Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud del Sistema General de Seguridad Social en Salud</i> 	3 meses

Una vez culminados los plazos estipulados, la Superintendencia Nacional de Salud realizará los requerimientos respectivos para verificar el cumplimiento de las etapas descritas en el presente artículo. Los soportes de cada uno de los entregables deberán mantenerse en todo momento y quedar a disposición de la SNS, para ser revisados y validar que cumplen con lo establecido en la presente Resolución, para fines de supervisión.

PARÁGRAFO PRIMERO. Para entidades que, a la fecha de expedición de la presente Resolución, ya cuentan con un sistema de gestión de riesgos, los plazos mencionados anteriormente regirán para la respectiva actualización a que haya lugar según los lineamientos dados.

ARTÍCULO NOVENO. PUBLICACIÓN. El contenido de la presente Resolución se publicará en el Diario Oficial y en la página web de la Superintendencia Nacional de Salud.

ARTÍCULO DÉCIMO. VIGENCIA. La presente Resolución rige a partir de su publicación. Las entidades obligadas al cumplimiento de lo aquí dispuesto, deben adaptar sus procesos a las condiciones aquí establecidas, sin perjuicio del cumplimiento de la normatividad vigente.

A partir de la fecha de publicación y dentro de un plazo máximo de veinticuatro (24) meses, la Superintendencia Nacional de Salud emitirá instrucciones a los diferentes tipos de vigilados, estableciendo los plazos, las metodologías, instrumentos, indicadores y contenidos mínimos del plan de implementación del Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud del Sistema General de Seguridad Social en Salud para cada uno de los riesgos prioritarios del SGSSS.

Dada en Bogotá D.C., a los

PUBLÍQUESE Y CÚMPLASE

NORMAN JULIO MUÑOZ MUÑOZ
Superintendente Nacional de Salud

Proyectó: César Augusto Piñeros García, Profesional Especializado de la Oficina de Metodologías de Supervisión y Análisis de Riesgo

Revisó: Francisco Morales Falla, Jefe de la Oficina Asesora Jurídica (E)

Edna Paola Najjar, Directora de Riesgos Económicos de la Superintendencia Delegada para la Supervisión de Riesgos

Luz Adriana Zuluaga Salazar, Directora de Riesgos en Salud de la Superintendencia Delegada para la Supervisión de Riesgos

Aprobó: José Oswaldo Bonilla, Superintendente Delegado para la Supervisión de Riesgos

Daniel Andrés Pinzón Fonseca, Jefe de la Oficina de Metodologías de Supervisión y Análisis de Riesgo