

**MANUAL PARA LA GESTIÓN INTEGRAL DEL RIESGO**

**ESE UNIVERSITARIA DEL ATLANTICO**

## CONTENIDO

1.	INTRODUCCIÓN.....	4
2.	ALCANCE.....	4
3.	OBJETIVOS.....	4
3.1.	OBJETIVO GENERAL.....	4
4.	MARCO LEGAL.....	5
5.	DEFINICIONES.....	6
6.	LINEAMIENTOS.....	8
7.	CICLO GENERAL DE GESTIÓN DE RIESGOS.....	9
8.	POLITICAS DE GESTION DEL RIESGO.....	23
9.	PROCESOS, PROCEDIMIENTOS Y MANUALES DE GESTIÓN DEL RIESGO.....	23
10.	DOCUMENTACIÓN PARA LA GESTIÓN DE RIESGOS.....	23
11.	ESTRUCTURA ORGANIZACIONAL – FUNCIONES Y/O RESPONSABILIDADES.....	24
11.1.	JUNTA DIRECTIVA.....	24
12.	REPRESENTANTE LEGAL.....	25
13.	OFICIAL DE CUMPLIMIENTO.....	26
14.	REQUISITOS DEL OFICIAL DE CUMPLIMIENTO.....	26
15.	FUNCIONES DEL OFICIAL DE CUMPLIMIENTO.....	27
16.	PROCESO DE GESTIÓN DEL RIESGO.....	28
17.	COMITÉ DE RIESGOS.....	29
18.	REVISOR FISCAL.....	30
19.	MÁXIMO ORGANO SOCIAL.....	30
20.	AUDITORIA INTERNA.....	31
21.	ORGANOS DE CONTROL.....	31
22.	INFRAESTRUCTURA TECNOLÓGICA.....	31
23.	DIVULGACIÓN DE INFORMACIÓN Y CAPACITACIONES.....	32
24.	DIVULGACIÓN DE INFORMACIÓN INTERNA.....	32
25.	DIVULGACIÓN DE INFORMACIÓN EXTERNA.....	32
25.1.	LINEAMIENTOS ESPECIFICOS DE LOS SUBSISTEMAS DE ADMINISTRACIÓN DE RIESGOS.....	32
26.	GESTIÓN DE RIESGO EN SALUD.....	33
27.	CICLO DE LA GESTION DE RIESGO EN SALUD.....	33
27.1.	IDENTIFICACIÓN DEL RIESGO EN SALUD.....	33
27.2.	MEDICIÓN Y EVALUACIÓN DEL RIESGO EN SALUD.....	34
27.3.	TRATAMIENTO Y CONTROL DE RIESGOS EN SALUD.....	34
28.	GESTIÓN DE RIESGO OPERACIONAL.....	34
29.	CICLO GENERAL DE GESTIÓN DEL RIESGO OPERACIONAL.....	35
29.1.	IDENTIFICACIÓN DEL RIESGO OPERACIONAL.....	35
29.1.1.	MEDICION Y EVALUACION DE RIESGO OPERACIONAL.....	36
29.1.2.	TRATAMIENTO Y CONTROL DE RIESGO OPERACIONAL.....	36
31.	GESTIÓN DE RIESGO ACTUARIAL.....	37
32.	CICLO GENERAL DE GESTIÓN DE RIESGO ACTUARIAL.....	37
32.1.	IDENTIFICACIÓN DEL RIESGO ACTUARIAL.....	37
32.2.	MEDICIÓN Y EVALUACIÓN DEL RIESGO ACTUARIAL.....	38
32.3.	TRATAMIENTO Y CONTROL DE RIESGO ACTUARIAL.....	38

33. GESTIÓN DEL RIESGO DE CRÉDITO.....	38
33.1. CICLO DE GESTIÓN DE RIESGO DE CRÉDITO .....	39
33.2. IDENTIFICACIÓN DE RIESGO DE CRÉDITO.....	39
33.3. EVALUACIÓN Y MEDICIÓN DE RIESGO DE CRÉDITO.....	39
33.4. TRATAMIENTO Y CONTROL DE RIESGO DE CRÉDITO.....	40
34. GESTIÓN DEL RIESGO DE LIQUIDEZ .....	41
34.1. CICLO DE GESTIÓN DE RIESGO DE LIQUIDEZ.....	41
34.2. IDENTIFICACIÓN DE RIESGOS DE LIQUIDEZ .....	41
34.2.3. EVALUACIÓN Y MEDICION DE RIESGO DE LIQUIDEZ .....	42
34.2.4. TRATAMIENTO Y CONTROL DE RIESGO DE LIQUIDEZ .....	42
35. GESTIÓN DEL RIESGO DE MERCADO DE CAPITALES.....	43
35.1. CICLO DE GESTIÓN DE RIESGOS DE MERCADO CAPITAL .....	43
35.1.1. IDENTIFICACIÓN DEL RIESGO DE MERCADOS CAPITALES.....	43
35.1.2. EVALUACIÓN Y MEDICIÓN DEL RIESGO DE MERCADO DE CAPITALES .....	44
35.1.3. TRATAMIENTO Y CONTROL DE RIESGO DE MERCADOS CAPITALES .....	44
36. GESTIÓN DE RIESGO DE GRUPO.....	44
36.1. CICLO GENERAL DE GESTIÓN DEL RIESGO DE GRUPO .....	44
36.1.1. IDENTIFICACIÓN DEL RIESGO DE GRUPO .....	45
36.1.2. EVALUACIÓN Y MEDICIÓN DEL RIESGO DE GRUPO .....	45
36.1.3. TRATAMIENTO Y CONTROL DEL RIESGO DE GRUPO .....	45
37. OTROS RIESGOS.....	46
37.1. RIESGO DE FALLAS DE MERCADO .....	46
37.2. GESTIÓN DE RIESGO REPUTACIONAL.....	46
38. RESPONSABILIDADES POR SUBSISTEMA (INTEGRANTES DE COMITÉ DE RIESGO).....	47
39. COMPROMISOS INSTITUCIONALES .....	49
40. REPORTES Y FUENTES DE INFORMACIÓN .....	49
41. CONTROL DEL CUMPLIMIENTO DEL MANUAL.....	49
42. FICHA DE CONTROL DE CAMBIOS .....	50
43. APROBACIÓN DEL DOCUMENTO .....	50

## 1. INTRODUCCIÓN

En desarrollo de las operaciones de la ESE Universitaria del Atlántico, existe una exposición constante a numerosos riesgos, que deben ser identificados y administrados a través de un Sistema Integrado de Gestión de Riesgos (SIGR), que promueva el autocontrol y la autorregulación a fin de evitar o mitigar la ocurrencia de eventos que impacten negativamente los objetivos de la institución.

Los Sistemas Integrados de Gestión de Riesgos deben responder a políticas claras y, a la vez, reflejarse en procesos y procedimientos que materialicen las estrategias de prevención y control de los riesgos identificados.

Las políticas y procedimientos que se adopten deben permitir el eficiente, efectivo y oportuno funcionamiento del Sistema Integrado de Gestión de Riesgos de las entidades, y traducirse en reglas de conducta y directrices que orienten la actuación de la entidad, sus empleados y sus socios.

## 2. ALCANCE

El siguiente manual va dirigido a los líderes de los procesos directamente relacionados con la gestión de los riesgos, los líderes de dichos procesos y los funcionarios bajo su cargo encargados de proporcionar la información necesaria para cumplir con todas las etapas de gestión de riesgo de cada uno de los subsistemas que componen el sistema integrado de gestión del riesgo (SIGR)

## 3. OBJETIVOS

### 3.1. OBJETIVO GENERAL

Impartir al personal ESE Universitaria del Atlántico las instrucciones generales relativas al código de conducta y de buen gobierno Organizacional, el sistema integrado de gestión de riesgos y a los Subsistemas de administración de riesgos que componen este sistema. Esto con el fin de facilitar la identificación, evaluación, medición, control y monitoreo eficaz de los riesgos prioritarios a los que está expuesta la institución en desarrollo de sus operaciones.

### 3.2. OBJETIVO ESPECIFICO

Por medio de la implementación del Sistema Integrado de Gestión de Riesgos, se busca:

- a. Fortalecer la Prestación de Servicios de Salud y el cumplimiento de metas en salud de acuerdo con el Plan Decenal de Salud Pública, Resolución 1841 de 2013, y 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.
- b. Incrementar la probabilidad que los eventos de mayor impacto (eventos en salud, administrativos, financieros, corrupción, entre otros), sean detectados antes de su materialización, o mitigados posterior a su ocurrencia.
- c. Fomentar una cultura de autocontrol y de gestión de riesgos por parte de los vigilados, de manera que sea una política empresarial o de gobierno organizacional que se interiorice en toda la estructura corporativa, incluyendo políticas de control interno.
- d. Generar condiciones de estabilidad operativa y financiera de las entidades a través de la implementación de Subsistemas de Administración de Riesgos estratégicamente diseñados e implementados, y debidamente documentados mediante Políticas de Gestión de Riesgo y manuales de procesos y procedimientos donde se incluyan Metodologías de valoración de los riesgos y las funciones de los Órganos de Control (Auditoría o Control Interno y Revisoría Fiscal, entre otros).
- e. Robustecer la infraestructura de supervisión dentro de la institución (Auditoría Interna, Revisoría Fiscal o Contralor Normativo, entre otros), encaminada a fortalecer el control y gestión de riesgos al interior de cada institución.

- f. Promover la cultura institucional hacia una supervisión y administración basada en riesgos que desarrolle habilidades evaluativas sobre la calidad de la gestión de los riesgos por parte de cada entidad.
- g. Extender 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.
- h. 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.
- i. Impulsar las mejores prácticas de Gobierno Organizacional e incorporar e interiorizar el Código de Conducta y Buen Gobierno en todas las instancias de las organizaciones que hacen parte del sector de la salud

#### 4. MARCO LEGAL

- El artículo 4° de la Ley 1751 de 2015: por medio de la cual se reguló el derecho fundamental a la salud y se dictaron otras disposiciones, definió al Sistema de Salud como “...el conjunto articulado y armónico de principios y normas; políticas públicas; instituciones; competencias y procedimientos; facultades, obligaciones, derechos y deberes; financiamiento, controles; información y evaluación, que el estado disponga para la garantía y materialización del derecho fundamental de la salud.”
- Decreto 1011 de 2006 y 780 de 2016: implementación del Sistema de Gestión de los Riesgos en Salud de las Instituciones Prestadoras de Servicios de Salud que deben acogerse a lo definido por el marco normativo de los componentes del Sistema Obligatorio de la Garantía de la Calidad en Salud (SOGCS)
- Resolución 2626 de 2019: adopción de la Política de Atención Integral en Salud (PAIS) con énfasis en resultados en salud y disminución de la carga de enfermedad.
- Ley 1122 de 2007: Sistema de Inspección, Vigilancia y Control (IVC) del sector salud.
- Para hacer efectivo el Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud, mediante el Decreto 2462 de 2013 fue modificada la estructura de la SNS, creando la Oficina de Metodologías de Supervisión y Análisis de Riesgo.
- 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, el cual define que, para sus sujetos vigilados, un conjunto de medidas preventivas para control, así como la implementación de indicadores de alerta temprana y ejercer sus funciones de IVC sobre la materia.
- Resolución 518 de 2015: se dictaron disposiciones en relación con la Gestión de la Salud Pública (...) y en cumplimiento del párrafo del artículo 5 de dicha Resolución, el Ministerio de Salud y Protección Social (MSPS) generó las Directrices para la caracterización y ejecución de los procesos para la Gestión de la Salud Pública en el contexto de la Política de Atención Integral en Salud (PAIS).
- NTC-ISO 31000: principios y directrices genéricos para la gestión del riesgo en una organización sin importar su naturaleza, industria y sector.
- Resolución 4559 de 2018: “Por la cual se adopta el modelo de Inspección, Vigilancia y Control para la Superintendencia Nacional de Salud para el ejercicio de la supervisión de los riesgos inherentes al Sistema General de Seguridad Social en Salud”
- Circular Externa 003 de 2018: recomendaciones para la implementación y la ejecución de mejores prácticas organizacionales (Código de Conducta y de Buen Gobierno empresarial) para las INSTITUCIÓN vigiladas por la Superintendencia Nacional de Salud pertenecientes a los grupos C1 y C2 establecidos en la Circular Externa 018 de 2015
- CIRCULAR EXTERNA 2021170000004-5 DE 2021: por la cual se imparten instrucciones generales relativas al código de conducta y de buen gobierno organizacional, el sistema integrado de gestión de riesgos y a sus subsistemas de administración de riesgos.

## 5. DEFINICIONES

- **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 detentan esas funciones”. El administrador debe obrar de buena fe, con lealtad y con diligencia. 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.
- **Atención en Salud:** Servicios o tecnologías en salud suministrados a los individuos y a la comunidad para promover, mantener, monitorizar o restaurar el estado de salud.
- **Categorías de riesgos prioritarios:** Agrupadores de distintos tipos de riesgos en torno a un elemento común, prioritarios para fines de supervisión definidos por la SNS. Cabe resaltar que las INSTITUCIÓN deben gestionar todos los riesgos que se presenten dentro de su operación, y dependerá de la discrecionalidad y organización que cada entidad les quiera dar para su tratamiento. Sin embargo, deberán contemplar como mínimo, los siguientes riesgos: Riesgo en Salud, Riesgo Actuarial; Riesgo de Crédito, Riesgo de Liquidez, Riesgo de Mercado de Capitales, Riesgo Operacional, Riesgo de Grupo y Riesgo de Lavado de Activos y Financiación del Terrorismo.
- **Ciclo general de gestión de riesgo:** Son las etapas que incorpora un Subsistema de Administración de Riesgos para cada uno de los tipos o categorías de riesgo identificadas.
- **Conflicto de interés:** Se considera que existe un conflicto de interés cuando por una situación de control, influencia directa o indirecta entre entidades, personas naturales o jurídicas, se realicen operaciones, transacciones, decisiones, traslado de recursos, situaciones de ventaja, mejoramiento en la posición de mercado, competencia desleal, desviaciones de recursos de seguridad social, o cualquier situación de hecho o de derecho que desequilibre el buen funcionamiento financiero, comercial o de materialización del riesgo al interior del sector. Estos desequilibrios tienen su fundamento en un “interés privado” que motiva a actuar en contravía de sus obligaciones y puede generar un beneficio personal, comercial o económico para la parte que incurre en estas conductas.
- **Contralor Normativo:** Cargo o área especializada dentro o fuera de la organización, el cual es nombrado por la Junta Directiva o quien haga sus veces, y ejerce control para asegurar la observancia de las disposiciones normativas aplicables. Sus funciones son dependientes de la Junta o quien haga sus veces, a quien debe asesorar y rendir cuentas.
- **Controles:** Medidas prudenciales, preventivas 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.
- **Cultura de autocontrol:** Concepto integral que agrupa todo lo relacionado con el ambiente de control, gestión de riesgos, sistemas de control interno, información, comunicación y monitoreo. Permite a la entidad contar con una estructura, unas políticas y unos procedimientos ejercidos por toda la organización (desde la Junta Directiva y la Alta Gerencia, hasta los propios empleados), los cuales pueden proveer una seguridad razonable en relación con el logro de los objetivos de la entidad.
- **Evento:** Situación que se presenta en un lugar específico y durante un intervalo de tiempo determinado.
- **Eventos externos:** Son eventos ocasionados por terceros, o, asociados a la naturaleza que, debido a su causa y origen, se escapan del control de la entidad.
- **Evento de pérdida:** Son las situaciones que generan pérdidas a las entidades al exponerse a cualquier riesgo.

- **Factores de riesgo:** Fuentes generadoras de eventos tanto internas como externas a la entidad y que pueden o no llegar a materializarse en pérdidas.  
Cada riesgo identificado puede ser originado por diferentes factores que pueden estar entrelazados unos con otros. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura, los acontecimientos externos, entre otros.
- **Falla de mercado:** Una situación en la que un mercado no asigna eficientemente los recursos por sí solo.
- **Gestión de Riesgo:** Es un enfoque estructurado y estratégico liderado por la Alta Gerencia que busca implementar un conjunto de acciones y actividades coordinadas para disminuir la probabilidad de ocurrencia o mitigar el impacto de un evento de riesgo potencial (incertidumbre) que pueda afectar los resultados y, por ende, el logro de los objetivos de cada entidad, así como el cumplimiento de sus objetivos y obligaciones. Dentro de este conjunto de acciones se incluye, entre otros, el ciclo general de gestión de riesgo.
- **Grupos de Riesgo:** Conjunto de personas con condiciones comunes de exposición y vulnerabilidad a ciertos eventos que comparten la historia natural de la enfermedad, factores de riesgo relacionados, desenlaces clínicos y formas o estrategias eficientes de entrega de servicios.
- **Gobierno Organizacional:** Es el conjunto de normas, procedimientos y órganos internos aplicables a cualquier tipo de entidad, mediante los cuales se dirige y controla la gestión de estas de conformidad con las disposiciones contenidas en la presente Circular y demás disposiciones sobre la materia. Tiene como objeto la adopción de mejores prácticas para garantizar que la gestión de las entidades se realice bajo los principios de transparencia, eficiencia, equidad, y propender por la calidad en la prestación de los servicios de salud centrados en el usuario.
- **Influencia Significativa:** El poder de intervenir en las decisiones de política financiera y de operación en la participación, sin llegar a tener el control ni el control conjunto de dichas decisiones.
- **Pérdidas:** Cuantificación económica que representa la materialización de un evento de Riesgo Operacional, donde se incluyen los gastos derivados de su atención.
- **Perfil de riesgo:** Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.
- **Pruebas de desempeño o de autocomprobación (Back Testing):** Se desarrolla para evaluar y calibrar la consistencia y confiabilidad de la medición de los indicadores de riesgos estimados por parte del modelo que se está utilizando, mediante la comparación de los resultados que el modelo arrojó, frente a los resultados observados.
- **Pruebas de tensión (Stress Testing):** Herramienta de diagnóstico donde bajo varios escenarios de estrés, se simulan diferentes choques extremos a los factores de riesgo para evaluar su sensibilidad e impacto, además de la capacidad de respuesta que las entidades tienen para enfrentarlos.
- **Reputación:** Percepción agregada que sobre una organización tienen los agentes relacionados con ella, sean estos clientes, accionistas, grupos de interés, partes vinculadas o público en general, la cual tiene el potencial de afectar la confianza en la entidad, influenciando su volumen de negocios, y su situación general.
- **Riesgo:** Posibilidad que ocurra un evento que pueda afectar negativamente el cumplimiento de la operación de una Entidad y que atenten contra los objetivos del SGSSS.

- **Riesgo inherente:** Nivel de riesgo propio de la actividad, cuya evaluación se efectúa sin considerar el efecto de los mecanismos de mitigación y de control.
  - **Riesgo neto o residual:** Nivel de riesgo que resulta luego de la aplicación de las medidas de control o mitigación existentes a los riesgos inherentes.
  - **Riesgo significativo:** Riesgo identificado y valorado de incorrección material que, a juicio del auditor, requiere una consideración especial en la auditoría.
- **Seguridad del Paciente:** Es el conjunto de elementos estructurales, procesos, instrumentos y metodologías basadas en evidencias científicamente probadas que propenden por minimizar el riesgo de sufrir un evento adverso en el proceso de atención de salud o de mitigar sus consecuencias.

## 6. LINEAMIENTOS

### I. CODIGO DE CONDUCTA Y BUEN GOBIERNO

Para lograr un mayor compromiso y responsabilidad frente a la gestión de riesgos es indispensable la implementación y la ejecución de mejores prácticas organizacionales mediante la formulación, implementación, desarrollo y seguimiento de un Código de Conducta y de Buen Gobierno en cada entidad. Como buenas prácticas para la implementación y fortalecimiento del Gobierno Organizacional y Código de Conducta en las entidades, se debe tener en cuenta las medidas mencionadas en la Circular Externa 003 de 2018 o las que la modifiquen, sustituyan o eliminen para su implementación. ESE Universitaria del Atlántico se compromete a la creación, divulgación y cumplimiento de su **propio Código de Conducta y Buen Gobierno**. El cumplimiento de los lineamientos aquí impartidos será respaldado por la implementación de un **programa de transparencia y ética empresarial**.

Por medio de la implementación y fortalecimiento del Gobierno Organizacional, se busca:

- a. Eficiencia en la Prestación del Servicio de Salud (Pertinencia, Accesibilidad, Calidad, Oportunidad y Seguridad), y así promover el uso debido y eficiente de los recursos.
- b. Reconocer los derechos de las diferentes partes interesadas, entre ellas, los usuarios del sistema de salud, para equilibrar los intereses y mejorar las relaciones e interlocución, para alcanzar el mayor grado de coordinación posible.
- c. Evitar y/o gestionar los posibles conflictos de interés.
- d. Establecer políticas anticorrupción (entre ellas establecer políticas antisoborno).
- e. Facilitar el ejercicio de los derechos y el trato equitativo a los miembros del Máximo Órgano Social, para promover la independencia y equidad.
- f. Garantizar la revelación oportuna y precisa de la información para lograr una mayor transparencia.
- g. Garantizar la orientación estratégica, el control efectivo de la dirección ejecutiva y la responsabilidad de esta frente a la empresa y a los miembros del Máximo Órgano Social.
- h. Mejorar el desempeño operacional de la entidad, que se debe ver reflejada en la creación de valor de la empresa.

### II. SISTEMA INTEGRADO DE GESTIÓN DE RIESGOS Y SUS SUBSISTEMAS.

#### II-I. LINEAMIENTOS GENERALES DEL SISTEMA INTEGRADO DE GESTIÓN DE RIESGO Y SUS SUBSISTEMAS

Tanto el Sistema Integrado de Gestión de Riesgos como los Subsistemas que lo componen deben contar al menos con los siguientes elementos mínimos: i) Ciclo General de Gestión de Riesgos, ii) Políticas de Gestión de Riesgos, iii) Procesos y Procedimientos, iv) Documentación, v) Estructura Organizacional, vi)

Infraestructura Tecnológica y, vii) Divulgación de la Información y Capacitaciones.

En este contexto, las entidades deben gestionar todos los riesgos a los que estén expuestas dentro de su operación, y su gestión dependerá de la discrecionalidad y organización que cada entidad les quiera dar para su tratamiento.

Sin embargo, deberán contemplar como mínimo, los siguientes riesgos priorizados y sus respectivos subsistemas:

1. Riesgo en Salud (SARS)
2. Riesgo Operacional (SARO)
3. Riesgo Actuarial
4. Riesgo de Crédito (SARC)
5. Riesgo de Liquidez (SARL)
6. Riesgo de Mercado de Capitales (SARM)
7. Riesgo de Grupo
8. Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT)  
Ver Manual SARLAFT
9. Riesgo de Corrupción opacidad y fraude (SICOF)  
Ver Manual SICOF
10. Otros riesgos

## 7. CICLO GENERAL DE GESTIÓN DE RIESGOS

Para cada una de las categorías de riesgo a supervisar por esta Superintendencia, se incluyen las siguientes etapas en los Subsistemas de Administración de Riesgos:

### a) 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 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 la ejecución de este paso del ciclo se hará uso de una Matriz de Riesgo Institucional, que funcionará de manera transversal para todas las áreas de la institución y tratará todos los diferentes subsistemas de riesgo.

La identificación de los riesgos se utilizará la **metodología de Delphi**. Esta consiste en la definición de un panel de expertos, que en el caso de U.N.A., serán los coordinadores o delegados de los mismos de las áreas de: Subgerencia corporativa, subgerencia científica, seguridad del paciente, jurídica, calidad, control interno, contratación, planeación institucional / gerencia, gestión del riesgo, talento humano, financiera; con colaboración ocasional de los coordinadores de otras áreas de apoyo como lo son atención al usuario, sistemas, compras, almacén o inventario.

El método Delphi es un sistema que se basa en el uso estratégico de las opiniones de un panel de expertos sobre algún tema en particular, con el fin de llegar a soluciones específicas y una mejor toma de decisiones. Utiliza técnicas que requieren de un mediador, un panel de expertos, un cuestionario y mucha interacción entre los involucrados.

A cada riesgo identificado se le ha de relacionar un proceso responsable por su vigilancia y mitigación, unas causas para su posible materialización, y las consecuencias de la materialización del mismo.

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

Para la evaluación y medición de cada uno de los riesgos identificados, la institución debe contar con información suficiente, completa y de calidad para generar los mejores pronósticos. La valoración de los riesgos ha de realizarse con cada uno de los riesgos identificados, y tendrá como resultado un nivel inherente de riesgo después de realizada la primera valoración.

**RIESGO INHERENTE (RI) = VECTOR (PROBABILIDAD INHERENTE (PI)\* IMPACTO INHERENTE (II))**

El ejercicio implica determinar el riesgo inherente para cada uno de los procesos y para la INSTITUCIÓN en general, ubicando cada riesgo inherente en el mapa calor:

Convenciones	
Calificación	Color
Alto	Rojo
Por encima promedio	Naranja
Moderado	Amarillo
Bajo	Verde

Anexo 1. Convenciones mapa de calor

Mapa de calor						
Probabilidad		Impacto				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Frecuencia		1	2	3	4	5
Casi Seguro	5	0	0	0	0	0
Probable	4	0	0	0	0	0
Posible	3	0	0	0	0	0
Improbable	2	1	0	0	0	0
Muy raro	1	0	0	0	0	0

Anexo 2. Mapa de calor

Se realiza la evaluación preliminar del riesgo (multiplicando la calificación preliminar de probabilidad con la del impacto), estableciendo así la clasificación en la cual se encuentra el riesgo.

Para determinar la **Probabilidad/Frecuencia** inherente se tomará el **factor más alto** de los siguientes criterios:

- **Historia:** número de veces que se ha materializado en un periodo de tiempo determinado.

Calificación	Descripción	Factor
Raro	Nunca ha ocurrido y, de hecho, se considera casi imposible que ocurra	1
Improbable	No se sabe si ha ocurrido o no, pero cabe alguna posibilidad de ocurrencia, aunque se considera muy remota	2
Posible	Ha ocurrido, hace más de dos años, pero se considera que las posibilidades de volver a suceder no son remotas.	3
Probable	No ha ocurrido durante el año en curso, pero sí el año anterior y se considera probable que vuelva a presentarse.	4
Casi seguro	Ha ocurrido, durante el año en curso, y se considera que las posibilidades de repetirse son muy altas.	5

- **Frecuencia:** número de veces que se materializa el riesgo sobre número de veces que se ejecuta la actividad.

Calificación	Descripción	Factor
--------------	-------------	--------

Extraordinario	0% - 0,05%	1
Esporádico	0,051% - 2%	2
No repetitivo	2,01% - 5%	3
Repetitivo	5,01% - 10%	4
Altamente repetitivo	10,01% - 100%	5

- **Futuro:** Probabilidad estimada de su ocurrencia en un futuro

Calificación	Descripción	Factor
Raro	Prácticamente imposible que ocurra el próximo año	1
Improbable	Poco probable que ocurra en el próximo año	2
Posible	Es probable que ocurra el próximo año	3
Probable	Bastante probable que ocurra el próximo año	4
Casi seguro	Ocurrirá con alto nivel de certeza el próximo año	5

Para determinar el **Impacto** inherente se tomará el factor más alto de los siguientes criterios:

- **Impacto Sistémico/Operativo:** Valoración del nivel en el cual la interrupción del proceso genera incumplimientos y/o retrasos en la cadena de valor de **ESE UNIVERSTIRARIA DEL ATLÁNTICO**

Calificación	Descripción	Factor
Insignificante	No existe una afectación.	1
Menor	Podría generar impactos cuantitativos y/o cualitativos a nivel de pocos clientes. El impacto es concentrado no generalizado	2
Moderado	Podría generar impactos cuantitativos y/o cualitativos en un grupo clientes de alto impacto para el negocio.	3
Mayor	Podría generar impactos en la eficiencia operacional de todos los clientes o participantes de la cadena de valor.	4
Catastrófico	Podría generar impactos cuantitativos y en la reputación de todos los clientes y participantes de la cadena de valor.	5

- **Impacto Legal:** Contempla repercusiones a nivel de incumplimiento con compromisos contractuales o exigencias de entes supervisores producidas por la interrupción del proceso.

Calificación	Descripción	Factor
Insignificante	Evento de riesgo registrado que podría llamar la atención de la SNS o las autoridades	1

Menor	Sanciones económicas menores por incumplimiento de normatividad / EJ: Glosas de la SNS	2
Moderado	Eventos derivados de las categorías de riesgo legal que pueden implicar procesos de investigación por parte de la SNS y sanciones económicas significativas. Determinación de responsabilidades a los administradores o Suspensión de administradores. Se puede generar un impacto en la continuidad en la prestación de servicios no principales del negocio.	3
Mayor	Eventos derivados de las categorías de riesgo legal que generen un impacto en la capacidad de operar parcialmente afectando una línea de negocio (CORE) u objeto principal, generando un incumplimiento normativo de disposiciones legales y normativas o emisión o cambio de normas que afecten el normal desarrollo de las actividades de la organización o emisión de sanciones judiciales a cargo produciendo: - Declaración de práctica insegura y no autorizada - Determinación de responsabilidades a los administradores Sanciones a la entidad integrada.	4
Catastrófico	Situaciones o eventos derivados de las categorías de riesgo legal que generen un impacto en la capacidad de operar afectando de manera sistémica la capacidad de operar las líneas de negocio CORE u objeto principal derivadas de elementos tales como el incumplimiento normativo, la misión de nuevas normas o de nuevas disposiciones legales que afecten el normal desarrollo de las actividades de la INSTITUCIÓN. Igualmente se predica de la emisión de sanciones judiciales a cargo produciendo entre otras la declaración de práctica insegura y no autorizada, y procesos legales en contra de la entidad integrada y sus administradores.	5

- **Impacto Económico:** Criterio que incorpora variables asociadas a la afectación económica que pueda presentarse por la materialización del riesgo. La descripción asociada a este impacto se define teniendo en cuenta la Utilidad Neta del año inmediatamente anterior al que se está realizando el análisis.

Calificación	Descripción	Factor
Insignificante	0,001 de la Utilidad Neta	1
Menor	0,005 de la Utilidad Neta	2
Moderado	0,02 de la Utilidad Neta	3
Mayor	0,1 de la Utilidad Neta	4
Catastrófico	> 0,1 Utilidad neta	5

- **Impacto Reputacional:** Acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de una entidad, tales como el impacto de la publicidad negativa sobre las prácticas comerciales, conducta o situación financiera de la entidad.

Calificación	Descripción	Factor
Insignificante	No se afecta la imagen de la institución	1
Menor	Se afecta la imagen de la institución con el sector, el cliente o proveedor crítico	2
Moderado	Se afecta la imagen de la institución en el mercado	3
Mayor	Se afecta la imagen de la institución dificultando la relación con contrapartes	4
Catastrófico	Se afecta la imagen de la institución impidiendo la relación con contrapartes	5

- **Impacto a la Salud:** Variables asociadas a la afectación de la salud de un paciente o colaborador por la materialización del riesgo.

Calificación	Descripción	Factor
Insignificante	No genera una lesión o complicación en el paciente. Puede afectar transitoriamente la ejecución de una tarea, pero sin interrupción a la prestación del servicio.	1
Leve	Puede ocasionar una lesión transitoria en el paciente sin secuelas, no requiere tratamiento médico, afecta transitoriamente la ejecución de una tarea, pero no la prestación del servicio	2
Moderado	Genera lesión o complicación a la salud del paciente, requiere tratamiento médico en un periodo limitado. Afecta la ejecución de una tarea temporalmente y la prestación del servicio en un periodo corto de tiempo.	3
Grave	Genera lesión o complicación grave en el paciente con discapacidad irreversible. Requiere tratamiento médico por tiempo indefinido, causa interrupción prolongada en la prestación de un servicio.	4
Catastrófico	Muerte(s) de paciente, suspensión definitiva de la prestación del servicio.	5

Basado en el total obtenido en la evaluación preliminar de del riesgo, se les asigna la siguiente clasificación de nivel de riesgo, junto con una serie de opciones de tratamiento a partir de la clasificación obtenida.

Nivel de Riesgo	Calificación	Definición	Tratamiento de Riesgo
0 a 5	<b>Bajo</b>	Cuando hay una probabilidad menor que el promedio de una perdida debido a la exposición y a la incertidumbre derivada de la materialización de un riesgo	Se <b>ACEPTARÁ</b> el riesgo y se administrará por medio de las actividades propias del proceso asociado, y su control y registro de avance, se realizará en el reporte mensual de su desempeño. Los planes de acción para la implementación de controles no se priorizarán.
6 a 10	<b>Moderado</b>	Cuando hay una probabilidad promedio de una perdida debido	Se establecerán acciones de Control Preventivas, que permitan <b>REDUCIR</b> la probabilidad de

		a la exposición y a la incertidumbre derivada de la materialización de un riesgo	ocurrencia del riesgo, se administrarán mediante seguimiento preferiblemente BIMESTRAL y se registrarán sus avances en el Sistema de Planificación Institucional- SGI.
11 a 16	Por encima del promedio	Cuando hay una probabilidad mayor el promedio de una pérdida debido a la exposición y a la incertidumbre derivada de la materialización de un riesgo	Se establecerán acciones de Control Preventivas, que permitan <b>EVITAR</b> la materialización del riesgo. La Administración de estos riesgos será con periodicidad <b>sugerida al menos MENSUAL</b> y su adecuado control se registrará en el Sistema de Planificación Institucional- SGI.
17 a 25	Alto	Cuando hay una probabilidad mucho mayor que la del promedio de una pérdida debido a la exposición y a la incertidumbre derivada de la materialización de un riesgo	Se establecerán acciones de Control Preventivas y correctivas, que permitan <b>EVITAR</b> la materialización del riesgo. La Administración de estos riesgos será con periodicidad <b>MÍNIMA MENSUAL</b> y su adecuado control se registrará en el Sistema de Planificación Institucional- SGI. Adicionalmente se deberán documentar al interior del proceso, planes de contingencia para tratar el riesgo materializado, con criterios de oportunidad, evitando el menor daño en la prestación del servicio; estos planes estarán documentados.

**Anexo 3: Tratamiento del riesgo**

Para la ejecución de este paso del ciclo se empleará las secciones de “Evaluación de riesgo inherente” en la **Matriz de Riesgos**.

La evaluación inicial de riesgo inherente será realizada por un grupo de expertos designados (Ver procedimiento de ciclo de riesgo). Posteriormente se definirá por cada riesgo evaluado un nivel de riesgo esperado después de la aplicación de controles. En base al **nivel de riesgo esperado** se definirá el nivel de riesgo residual, después de la implementación de controles.

**c) CONTROL DE RIESGOS (Selección de estrategias para el tratamiento y control)**

Una vez identificados y evaluados los riesgos, deben compararse con los **límites** (tolerancia) de riesgos aprobados por la instancia definida en la institución y su política de riesgos, siempre dentro del marco normativo establecido. Todo riesgo que exceda los límites o desviaciones aceptadas, 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, de acuerdo con los niveles de riesgo determinados y las tolerancias al riesgo definidas.

Se asociarán **controles** a cada riesgo identificado, al igual que el tipo/objetivo del control (preventivo, correctivo, detectivo), el/los responsables de la implementación del control, frecuencia de seguimiento, fecha de inicio de la implementación y fecha final de la implementación y seguimiento. Se asociará a cada control un indicador que ayudará a medir la efectividad de este durante el periodo de seguimiento definido.

La información referente a los controles y su seguimiento se registrarán en la sección de Control y tratamiento de riesgo en el formato de **Matriz de riesgo institucional**.

Con el fin de disminuir la probabilidad y el impacto del riesgo en caso de materializarse, se busca en esta etapa definir los controles y las acciones de tratamiento, teniendo en cuenta las siguientes alternativas:

#### ➤ Opciones de manejo de tratamiento del riesgo

**Evitar el riesgo:** Implica dejar de ejecutar las actividades o desistir de una decisión que posiblemente generaría que el evento se materialice, o tomar planes de contingencia para reducir el impacto del riesgo materializado.

**Reducir el Riesgo:** Desarrollar actividades que propendan por reducir la probabilidad o la severidad en caso de materializarse el evento.

**Aceptar el riesgo:** Tiene lugar cuando la organización decide no impartir ningún tipo de acción que evite su materialización y/o severidad en el impacto. Está dispuesta a asumir los costos derivados de la materialización del evento. También se puede tomar esta opción de manejo cuando las actividades propias del proceso relacionado son suficientes para impedir la materialización del mismo.

**Transferir el riesgo:** Tiene lugar cuando se traslada el riesgo a otra compañía, ya sea por medio de la tercerización, contratación de una póliza de seguros u otros.

**Tercerización – Outsourcing:** Se podrá contratar bajo la modalidad de tercerización a personas naturales y/o jurídicas para el desarrollo de sus procesos, siempre que no implique la delegación de la profesionalidad. En todo caso, ESE UNIVERSTIRARIA DEL ATLÁNTICO debe:

- Realizar un análisis de riesgo para determinar los procesos y/o actividades a tercerizar.
- Comprender el riesgo operacional asociado a los procesos y/o actividades tercerizadas.
- Contar con políticas eficaces para incorporar en su estrategia de riesgos, aquellos derivados de la tercerización.
- Determinar dentro de los procesos y/o actividades tercerizadas aquellos que se consideren críticos.

Tratándose de los procesos y/o actividades identificadas como **críticos** para la ESE UNIVERSTIRARIA DEL ATLÁNTICO, se debe cumplir como mínimo con los siguientes requerimientos:

- Definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros.
- Incluir en los contratos que se celebren con los terceros, o en aquellos que se prorroguen, al menos, aspectos tales como obligaciones de las partes, niveles de servicio, operación en situaciones contingentes, gestión de los riesgos operacionales que puedan afectar el cumplimiento de las obligaciones del tercero, acuerdos de confidencialidad sobre la información manejada y las actividades desarrolladas.
- Gestionar los riesgos que se derivan de la prestación del servicio por parte del tercero, en particular, cuando atiende a varias entidades.
- Contar con los procedimientos necesarios para verificar el cumplimiento de las obligaciones por parte del tercero.
- Incluir dentro del alcance de las evaluaciones que haga la función de gestión de riesgos y la auditoría interna, las actividades tercerizadas.

#### ➤ Aceptación de riesgos

En ESE UNIVERSTIRARIA DEL ATLÁNTICO, los riesgos son aceptados conforme lo establecido en el nivel admisible del apetito de riesgo, cuando su severidad se encuentra dentro de la categoría de **Moderado y Bajo** presentadas en el anexo 3 del presente manual. A los riesgos Moderados se les recomienda la asignación de un plan de acción para su mitigación, pero la intensidad del seguimiento a sus controles puede ser definida por la institución.

Los riesgos ubicados en categorías **Por encima del Promedio** y **Altos** no pueden ser asumidos por la institución y la asignación de controles y seguimientos de carácter mensual es **obligatoria**.

#### d) SEGUIMIENTO Y MONITOREO

Una vez establecidos los mecanismos o un conjunto de estos, para la mitigación y control de los riesgos que se han identificado como relevantes para la entidad y después de realizar un análisis de causa y efecto para determinar los puntos más críticos a intervenir con mayor prelación, las instituciones deberán poner en práctica tales mecanismos y reflejarlos en un plan de implementación de las acciones planteadas en la fase anterior.

Con el fin de realizar el respectivo seguimiento y monitoreo permanente y continuo de la evolución de los perfiles de riesgo y la exposición frente a posibles pérdidas a causa de la materialización de cada uno de los riesgos identificados, la entidad debe desarrollar un sistema de alertas tempranas que facilite la rápida detección, corrección y ajustes de las deficiencias en cada uno de sus Subsistemas de Administración de Riesgo para evitar su materialización. Lo anterior, con una periodicidad acorde con los eventos y factores de riesgo identificados.

De materializarse uno de los riesgos se ha de realizar una descripción y análisis de causa raíz del mismo, así como fecha de inicio y finalización del evento riesgoso y las acciones correctivas tomadas o a realizar en respuesta ha dicho evento. Definir plazos de seguimiento a acciones correctivas. Apoyarse con formatos y procedimientos de **Plan de Acción Correctiva**.

➤ **Las prioridades de monitoreo y revisión pueden comprender:**

- Riesgos de alto impacto.
- Fallas en las estrategias de tratamiento, especialmente cuando éstas pueden resultar en consecuencias altas o frecuentes.
- Riesgos relacionados con actividades que tienen alta incidencia de cambio.
- Criterios de tolerancia al riesgo especialmente aquellos cuyos resultados son de alto nivel o de riesgo residual.
- Avances tecnológicos que puedan ofrecer mayor efectividad o menor costo que el tratamiento del riesgo.

➤ **Las prácticas de monitoreo y revisión pueden ser de los siguientes tipos:**

- Monitoreo continuo, como rutinas de medición o chequeo sobre parámetros definidos.
- Revisiones de autocontrol.
- Procesos de auditoría interna o externa.

Cada vez que se realicen cambios en los tratamientos como resultado de la revisión de la matriz de riesgos, se debe documentar esta información en la matriz de riesgos del macroproceso.

➤ **Actualización de las matrices de riesgo por macroprocesos**

Permanentemente los procesos están expuestos a cambios y mejoras como la materialización de eventos de riesgo, informes de auditoría, implementación de nuevos productos y metodologías e implementación de planes de mejora que llevan a la revisión y actualización del perfil de riesgos. Por lo anterior, cada vez que se considere necesario el líder del proceso deberá informar al Proceso de Gestión del Riesgo dichos cambios para que con el apoyo de esta, se realicen las modificaciones respectivas.

El perfil de riesgos deberá ser actualizado por el proceso de Gestión del Riesgo, revisado por la Gerencia General y presentado en Comité de Riesgos.

La administración podrá realizar testeos a controles que considere se requiere evaluar su eficacia operacional.

### ➤ Seguimiento a los planes de acción

Mensualmente los líderes de cada proceso (ver responsables de gestión de riesgo por subsistema en Anexo 6) deberán reportar al Proceso de Gestión del Riesgo el porcentaje de avance en la implementación de los planes de acción relacionados con los riesgos que no dan cumplimiento a los criterios de aceptación del riesgo.

Los resultados generados a través de los análisis y evaluaciones desarrolladas por la Coordinación de Riesgos y Procesos deben ser soportados e informados a la Gerencia, como también el reporte de cualquier hallazgo, anomalías, oportunidades y/o debilidades; así como, las consideraciones individuales detectadas en los análisis y evaluaciones de riesgo desarrollados de forma particular a cada proceso.

Para la ejecución de este paso del ciclo se empleará las secciones de “**Seguimiento materialización del riesgo**” en la **Matriz de Riesgos**.

### ➤ Herramientas para seguimiento a riesgos:

#### Formulación de indicadores

De acuerdo con el perfil del riesgo que tiene la organización, existen diferentes indicadores que sirven para generar alertas tempranas, para ello existen dos tipos de indicadores que se ajustan a las necesidades que requiere ESE UNIVERSITARIA DEL ATLANTICO para gestionar sus riesgos, los cuales son:

- **Los indicadores clave de Riesgo - (KRI):** cuantifican el perfil de riesgo de la compañía. Se constituyen de acuerdo con el nivel de relevancia en los indicadores de riesgo y de control. Por ejemplo, el volumen de operaciones, rotación de personal, número de veces que cae el sistema, etc. Cada KRI deberá ser capaz de ser medido con precisión y reflejar de manera precisa el impacto negativo que tendría sobre los indicadores de desempeño clave de la organización. Los KRI son métricas creadas para poder sintetizar objetivamente aquellos riesgos que se consideran significativos y que necesitan un tratamiento diferenciado. Estas métricas permiten llevar un registro de incidencias, monitorear su comportamiento, informar sobre su evolución, reportarlos y establecer planes de acción cuando salen de la tendencia esperada.
- **Los indicadores clave de control – (KCI):** Se encargan de medir la efectividad, tanto del diseño como de desempeño de un control específico. Un deterioro en un KCI puede significar un aumento en la probabilidad e impacto de un riesgo.

La asignación de indicadores se priorizará sobre riesgos que presenten niveles de riesgo **por encima del promedio** y **altos** en la matriz de riesgos. La información dada por indicadores permitirá generar planes de acción en aquellos indicadores que estén por debajo de los límites permitidos de aceptación y brindaran información cuantitativa confiable al momento de valorar la efectividad de los controles al final de un periodo de gestión de los riesgos.

### ➤ EVALUACIÓN DE CONTROLES

En base al grado de tolerancia (clasificación del nivel de riesgo), se aclaran cuáles son los **controles** que se llevan actualmente para la mitigación y como evidencia o sustento del tratamiento. Se evaluará a través de un sistema de valoración de controles la calidad de los mismos para tratar con los riesgos analizados.

La calidad de los controles se medirá a través de un cálculo de valoración donde el puntaje de calidad de los controles se dividirá en cuatro posibles opciones dependiendo de su desempeño para la mitigación de los riesgos asociados. Se tendrán

en cuenta también otros aspectos relacionados con la efectividad de las herramientas y del seguimiento hecho a dichos controles. La ponderación de los resultados arrojará un porcentaje que ubicará al control en **cuatro categorías** (Fuerte, Aceptable, Requiere Mejora, Débil).

Ver Anexo 4. A continuación para explicación detallada del cálculo para valoración de la calidad de los controles por riesgo.

Calidad de las funciones de control	
Las funciones de control muestran de forma consistente un desempeño efectivo y superior a las prácticas de la industria de los seguros comúnmente observadas y/o Clasificación del control con énfasis en lo preventivo.	20
Las funciones de control muestran desempeño efectivo y similar a las prácticas de la industria comúnmente observadas.	15
Las funciones de control muestran potencial para un desempeño efectivo, pero pueden ser mejoradas y no arriesgan la situación financiera de la compañía.	10
Las funciones de control muestran un desempeño inferior a las prácticas observadas de la industria y su efectividad debe ser mejorada para no comprometer la situación financiera y operativa de la compañía.	5



Valoración de los controles		
Parámetros	Criterios	Puntaje
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.	0 - 1
	Existen manuales instructivos o procedimientos para el manejo de la herramienta	0 - 1
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.	0 - 1
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.	0 - 1
	La frecuencia de la ejecución del control y seguimiento es adecuada.	0 - 1
<b>TOTAL</b>		<b>Sumatoria de cada uno de los criterios (0-5)</b>



Rangos de calificación de los controles		
Calidad del control	Definición	Rangos
Fuerte	Existen controles fuertes: acciones preventivas, planes de mejora y contingencia.	80 - 100
Aceptable	Existen controles aceptables: acciones preventivas, planes de mejora.	60 - 79
Necesita mejora	Existen controles mínimos que requieren mejoras.	40 - 59
Débil	No existen controles o son mínimos.	0 - 39

**Anexo 4:** Calificación de controles de Gestión del riesgo.

Para el **tratamiento** de cada riesgo individual se deberán identificar las acciones preventivas a tomar, responsables de la acción, periodos de seguimiento, plazos de inicio y terminación de la acción y acciones de contingencia ante la posible materialización del riesgo.

Para la ejecución de este paso del ciclo se utilizarán las secciones de “Evaluación de calidad de controles” y “Tratamiento de riesgos” en la **Matriz de Riesgos**

➤ **Nivel de cumplimiento de los controles implementados**

En la pestaña designada para medición de calidad de los controles se medirá también su adherencia y comportamiento dentro del SIGR.

Naturaleza	Nivel de cumplimiento de los controles en la gestión de la calidad de los controles						
	El control es manual o automático?	Documentado	Publicado en el SGC	Socializado	Implementado	Evaluado (Nivel de adherencia)	Observaciones
	Manual	SI	SI	SI	SI	NO	

**Anexo 5.** Evaluación de nivel de cumplimiento; no tiene efecto sobre la clasificación cuantitativa del control, pero si da una visión cuantitativa del nivel de incorporación del control en la institución.

- **Naturaleza del control**

**Control Manual:** Es cuando existe la presencia e intervención de una persona en la acción de controlar.

**Control Automatizado:** Es cuando la acción de controlar no requiere de la intervención de una persona y es realizado por una aplicación o sistema.

**Control Combinado:** Es cuando la acción de controlar cuenta con una parte automatizada, pero requiere la presencia e intervención de una persona. Esto incluye los controles que se realizan en Excel.

- **Documentado**

**SI:** El control y su información están incluidos dentro de la documentación del proceso.

**PARCIAL:** El control y su información se encuentran incluido dentro de algún documento del área que describe la actividad dentro del proceso.

**NO:** No existe registro sobre el control y su información en ningún documento del proceso.

- **Publicado en el SGC**

**SI:** El control y su información son de fácil acceso al personal designado para medir, vigilar y prevenir la materialización del riesgo.

**PARCIAL:** Existe personal directamente relacionado con el proceso en el que se puede materializar el riesgo que no tiene acceso a los controles.

**NO:** La información no está publicada en el SGC.

- **Socializado**

**SI:** Los controles fueron socializados al personal del proceso relacionado con el riesgo.

**PARCIAL:** Los controles fueron socializado mínimo al coordinador del proceso relacionado con el riesgo.

**NO:** Los controles aún no han sido socializados.

- **Evaluado**

**SI:** Se hizo evaluación de la adherencia del personal en el proceso relacionado con el riesgo al control asignado.

**NO:** No se hizo evaluación de adherencia a los controles.

- **Implementado:**

**SI:** Un control débil es el que tiene una alta probabilidad de fallar, dado que depende del criterio de la persona que lo está ejecutando y no cumple con los criterios enunciados (Tipo, funcionalidad, asignación, documentación, frecuencia, naturaleza y efectividad del control).

**PARCIAL:** Un control moderado es el que puede cumplir con algunos criterios enunciados (Tipo, funcionalidad, asignación, documentación, frecuencia, naturaleza y efectividad del control) y puede depender del criterio de la persona que lo ejecuta.

**NO:** Un control fuerte, es el que tiene una combinación efectiva de los criterios calificados enunciados (Tipo, funcionalidad, asignación, documentación, frecuencia, naturaleza y efectividad del control) y no depende del criterio de quien lo ejecuta.

➤ **PERFIL DE RIESGO RESIDUAL**

La efectividad de los controles en el riesgo inherente lleva como resultado el nivel del riesgo residual. Esto quiere decir que al determinar los atributos de eficiencia e informativos del control será posible identificar la zona del riesgo en estado residual.

El riesgo residual de **ESE UNIVERSTIRARIA DEL ATLÁNTICO** será determinado por los riesgos inherentes que hayan obtenido una valoración **Por encima del promedio y Alta** y los riesgos asociados a fraude y LA/FT que hayan obtenido una valoración diferente a **baja** después del resultado de la evaluación de los controles.

Finalmente, si en el riesgo residual de **ESE UNIVERSTIRARIA DEL ATLÁNTICO** se ha obtenido como resultado riesgos operacionales que mantienen una valoración muy alta o diferente a baja para el caso de LA/FT y fraude, se deberán analizar las opciones de planes de mejora que permitan bajar el nivel de los riesgos a una zona aceptable. Para lo anterior se hace pertinente evaluar el costo beneficio de las acciones a tomar, si la entidad está dispuesta a administrar el riesgo, si se está en capacidad de reducir la probabilidad o si se pudiera optar por transferir el riesgo (pólizas de seguros, tercerización).

Para definir el nivel de **riesgo residual** de la INSTITUCIÓN se utilizará la siguiente metodología, que se apoyará en la evaluación de efectividad de los controles para reducción del nivel de riesgo inherente:

- a) Definir el periodo de seguimiento a los riesgos identificados. Durante este periodo los colaboradores encargados del seguimiento de cada riesgo deberán hacer entrega de los indicadores relacionados.
- b) Definir **el nivel de riesgo esperado** de cada riesgo identificado.
- c) Una vez se termine el periodo de seguimiento de los riesgos y de implementación de controles y planes se valoran los controles como se describió en el punto **c)** de **1. CICLO GENERAL DE GESTIÓN DEL RIESGO**.
- d) Se empleará **la matriz de escala de clasificación para riesgo residual**, cruzando el resultado de riesgo inherente del riesgo evaluado y el resultado de valoración de calidad de control.
- e) De cumplirse con el mínimo aceptable para que el control pueda considerarse como efectivo, el nivel de riesgo propuesto cambiará.
- f) El nuevo nivel de riesgo será sobre el que se trabajará para el próximo periodo.

Se incluirá este resultado de riesgo residual en la **matriz de riesgo** y se construirá un nuevo mapa de calor, donde se visualizará la evolución del nivel de riesgo de la institución después de implementados los controles.

Riesgo Residual				
Calidad de los controles	Nivel del Riesgo Inherente			
	Bajo	Moderado	Por encima del promedio	Alto
Fuerte	Bajo	Bajo	Moderado	Por encima del promedio
Aceptable	Bajo	Moderado	Por encima del promedio	Alto
Necesita mejorar	Moderado	Por encima del promedio	Alto	Alto
Débil	Por encima del promedio	Alto	Alto	Alto

Anexo 5. Matriz - escala de clasificación para riesgo residual

Se incluirá este resultado de riesgo residual en la **matriz de riesgo** y se construirá un nuevo mapa de calor, donde se visualizará la evolución del nivel de riesgo de la institución después de implementados los controles.

#### e) PERIODICIDAD DE IMPLEMENTACIÓN CICLO DE GESTIÓN DEL RIESGO

Todas las etapas que componen el ciclo de gestión del riesgo volverán a implementarse con una periodicidad anual. Después de finalizada la evaluación de calidad de los controles para mitigación o prevención de los riesgos inherentes al final del periodo, se reevaluará el proceso por medio de comité de riesgos. Aspectos a tener en cuenta durante la reevaluación son:

- Durante el comité de riesgo realizado en la fecha inmediata a la finalización del ciclo de gestión de riesgo, se reevaluarán los riesgos identificados, es decir se considerará la inclusión o eliminación de riesgos en la matriz de gestión de riesgo institucional.
- No se podrán eliminar riesgos que presenten un riesgo residual diferente a “BAJO” o que tenga una Opción de Manejo/Tratamiento diferente a “Aceptar el Riesgo”.
- Se hará la inclusión de riesgos que se materializaron durante el último periodo, o que debido a factores internos o externos de la empresa tienen una alta probabilidad de materializarse en la institución e impactar negativamente sus operaciones.
- Se evaluará el cambio o eliminación de controles asociados a los riesgos identificados. Se tendrán en cuenta los criterios de evaluación de controles y el comportamiento de los indicadores relacionados a los riesgos.
- La eliminación, cambio o inclusión de un riesgo o control en la matriz deberá quedar registrada en el **acta de comité de riesgo**, junto a la respectiva justificación de la acción. Es necesario respaldar la decisión en resultados de evaluación de controles e indicadores.
- La inclusión o cambio de riesgos o controles en la matriz se puede considerar semestralmente en el tercer comité del periodo evaluado. No se pueden eliminar riesgos de la matriz durante esta sesión de comité semestral.

## 8. POLITICAS DE GESTION DEL RIESGO

La institución adopta en relación con el marco de su Sistema Integrado de Gestión de Riesgos, las políticas o lineamientos generales que permitan el desarrollo del ciclo de la gestión de los riesgos prioritarios de forma eficiente y oportuna. Cada una de las etapas y elementos para cada uno de los Subsistemas de Administración de Riesgos cuenta con políticas claras y aplicables.

Las políticas de Gestión de Riesgos deberán ser comunicadas a todos los colaboradores, socios, proveedores, directivos, administradores, con el fin que sean entendidas e implementadas en todos los niveles de la institución. Serán revisadas con una periodicidad **anual** con el fin de actualizarlas en base a las condiciones particulares de la entidad y a las del mercado. Tanto la aprobación como las modificaciones que se efectúen a dichas políticas, deben tener constancia en **actas**. (Ver **Políticas**)

## 9. PROCESOS, PROCEDIMIENTOS Y MANUALES DE GESTIÓN DEL RIESGO

La INSTITUCIÓN debe establecer los procesos y procedimientos que instrumenten su Política de Gestión de Riesgos y que sean aplicables para la adecuada implementación y funcionamiento de cada uno de sus Subsistemas de Administración de Riesgos. Estos deben ser documentados, debidamente codificados, socializados al personal encargado del proceso de Gestión del Riesgo (con actas de aprobación y socialización al personal encargado del proceso) y puestos a disposición en la carpeta de archivos compartidos para su consulta por parte del personal de la INSTITUCIÓN.

Será la responsabilidad de la gerencia, proceso de gestión de riesgo y proceso de gestión integral de la calidad de la INSTITUCIÓN la aprobación de los manuales y procedimientos del Sistema de Gestión de Riesgo.

## 10. DOCUMENTACIÓN PARA LA GESTIÓN DE RIESGOS

Las etapas del ciclo general de riesgos y los elementos específicos de los diferentes Subsistemas de Administración de Riesgos deben quedar plasmados en documentos y registros, garantizando la integridad, oportunidad, trazabilidad, confiabilidad y disponibilidad de la información allí contenida.

Los procesos y procedimientos mencionados en el anterior numeral se deben adoptar y plasmar mediante documentos controlados, en los cuales deben quedar claramente definidas las funciones, responsabilidades y atribuciones específicas para cada uno de los colaboradores involucrados en la administración de los diversos riesgos.

En UNA se maneja la siguiente documentación de gestión del riesgo:

- a. Las políticas para la administración de cada uno de los riesgos.
- b. Las metodologías y procedimientos para la identificación, medición, control y monitoreo de los riesgos identificados. A su vez, el establecimiento de los niveles de aceptación y límites de exposición.
- c. La estructura organizacional que garantice el desarrollo de cada uno de los Subsistemas de Administración de Riesgos y que, a su vez, fortalezca el Sistema Integrado de Gestión de Riesgos de la entidad.
- d. Los roles y responsabilidades de quienes participan en la gestión de los diversos riesgos identificados, especialmente los prioritarios.
- e. Las medidas necesarias para asegurar el cumplimiento de las políticas y objetivos de cada uno de los Subsistemas de Administración de Riesgos.
- f. Roles, responsabilidades y acciones de los órganos de control interno frente a cada uno de los Subsistemas de Administración de Riesgos.
- g. Las estrategias de capacitación y divulgación de cada uno de los Subsistemas de Administración de Riesgos.

## 11. ESTRUCTURA ORGANIZACIONAL – FUNCIONES Y/O RESPONSABILIDADES

Sin perjuicio de las responsabilidades y obligaciones que se encuentren establecidas en otras disposiciones legales, estatutarias o en reglamentos, para el diseño y adopción de cada uno de los Subsistemas de Administración de Riesgos, se deben establecer como mínimo las siguientes actividades a cargo de los órganos de dirección, administración y el revisor fiscal de las entidades dentro de sus Códigos de Conducta y Buen Gobierno:

### 11.1. JUNTA DIRECTIVA

- a. Diseñar y actualizar las políticas para la prevención y control del riesgo de LA/FT/FPADM que harán parte del SARLAFT, para una posterior aprobación por el máximo órgano social o quien haga sus veces.
- b. Aprobar el manual de procedimientos y sus actualizaciones.
- c. Garantizar los recursos técnicos y humanos que se requieran para implementar y mantener en funcionamiento el SARLAFT, teniendo en cuenta las características del riesgo de LA/FT/FPADM y el tamaño de la entidad. Este equipo de trabajo humano y técnico debe ser de permanente apoyo para que el Oficial de Cumplimiento lleve a cabalidad sus funciones.
- d. Asignar un presupuesto anual para contratación de herramientas tecnológicas, contratación de personal, capacitación, asesorías, consultorías, y lo necesario para mantener la operación del SARLAFT en la compañía y la actualización normativa del Oficial de Cumplimiento y su equipo.
- e. Designar al Oficial de Cumplimiento y su respectivo suplente. Para efectos de dar cumplimiento a las circulares, la Junta Directiva o quien haga sus veces dará a conocer el nombramiento del Oficial de Cumplimiento a la Superintendencia Nacional de Salud, indicando nombre, profesión, cargo adjunto o de desempeño alterno (si procede), teléfonos de contacto y correo electrónico. **Esta información y su respectiva actualización o modificación, deberá realizarse a través del módulo de datos generales o aplicativos de reporte de información que la Superintendencia Nacional de Salud disponga para ellos.** En el caso de las entidades públicas la designación se realizará de acuerdo a los términos de Ley que les aplique.
- f. Incluir en el orden del día de sus reuniones, la presentación del informe del Oficial de Cumplimiento, por lo menos una vez al año o cuando éste lo determine necesario.
- g. Pronunciarse sobre los informes presentados por el Oficial de Cumplimiento y la Revisoría Fiscal y realizar el seguimiento a las observaciones o recomendaciones adoptadas, dejando constancia en las actas.
- h. Aprobar los criterios objetivos y establecer los procedimientos y las instancias responsables de la determinación y Reporte de las Operaciones Sospechosas (ROS).
- i. Aprobar las metodologías de segmentación, identificación, medición, control y monitoreo del SARLAFT.
- j. Designar la(s) instancia(s) responsable(s) del diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de las operaciones inusuales.
- k. Aprobar las políticas de la entidad en materia de administración de todos los riesgos que pueden afectar los objetivos de la entidad y que son presentadas por el Comité de Riesgos, a partir del trabajo con el área de gestión de riesgos.
- l. Aprobar los reglamentos, manuales de procesos, procedimientos y funciones de las áreas pertenecientes a la entidad, así como sus respectivas actualizaciones.

- m. Aprobar el Código de Conducta y de Buen Gobierno, el sistema de control interno, la estructura organizacional y tecnológica del Sistema Integrado de Gestión de Riesgos.
- n. Aprobar el diseño y definir la periodicidad de los informes internos para los reportes de la gestión de los riesgos, especialmente los prioritarios que se van a presentar a las diferentes áreas de la entidad.
- o. Aprobar el marco general de indicadores de alerta temprana y los límites de exposición como mínimo a los riesgos prioritarios.
- p. Aprobar las actuaciones en caso de sobrepasar o exceder los límites de exposición como mínimo frente a los riesgos prioritarios o cualquier excepción de las políticas, así como los planes de contingencia a adoptar en caso de presentarse escenarios extremos.
- q. Conocer los resultados de las pruebas de tensión (stress test) en el caso que apliquen y el plan de acción a ejecutar con base en ellos, presentado por el Comité de Riesgos u órgano equivalente.
- r. Garantizar los recursos técnicos y humanos que se requieran para implementar y mantener en funcionamiento el Sistema Integrado de Gestión de Riesgos, teniendo en cuenta las características de cada riesgo y el tamaño y complejidad de la entidad.
- s. Realizar el nombramiento del Comité de Riesgos en caso de que la entidad decida establecerlo, definir sus funciones y aprobar su reglamento, de acuerdo con las normas legales que le apliquen.
- t. Pronunciarse y hacer seguimiento sobre los informes periódicos que elabore el Comité de Riesgos y la Revisoría Fiscal, respecto a los niveles de riesgo asumidos por la entidad, las medidas correctivas aplicadas para que se cumplan los límites de riesgo previamente establecidos y las observaciones o recomendaciones adoptadas para el adecuado desarrollo de cada uno de los Subsistemas de Administración de Riesgo.
- u. Designar la(s) instancia(s) responsable(s) del diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de la exposición como mínimo a los riesgos prioritarios en los casos que aplique.
- v. Aprobar las metodologías de segmentación, identificación, medición, control y monitoreo de los diferentes Subsistemas de Administración de Riesgos, diseñadas por la instancia responsable.
- w. Monitorear el cumplimiento de los lineamientos de los diferentes Subsistemas de Administración de Riesgos promoviendo su continuo fortalecimiento y que la toma de decisiones este en función de la selección e implementación de las estrategias para el tratamiento y control de los diversos riesgos y de su comportamiento.

## 12. REPRESENTANTE LEGAL

Dentro de la implementación del Sistema Integrado de Gestión de Riesgos y de cada uno de los Subsistemas de Administración de Riesgos de la entidad, se deberán asignar como mínimo las siguientes funciones a cargo del Representante Legal:

- a. Apoyar y garantizar el efectivo cumplimiento de las políticas definidas por la

Junta Directiva.

- b. Adelantar un seguimiento permanente del cumplimiento de las funciones del Comité de Riesgos y mantener informada a la Junta Directiva.
- c. Conocer y discutir los procedimientos a seguir en caso de sobrepasar o exceder los límites de exposición frente a los riesgos, así como los planes de contingencia a adoptar respecto de cada escenario extremo.
- d. Hacer seguimiento y pronunciarse respecto de los informes periódicos que presente el Comité de Riesgos sobre el grado de exposición de riesgos asumidos por la entidad y los controles realizados, además de los informes presentados por la Revisoría Fiscal. Lo anterior debe plasmarse en un informe a la Junta Directiva o, quien haga sus veces, y hacer énfasis cuando se presenten situaciones anormales como mínimo en algún riesgo prioritario o existan graves incumplimientos a las políticas, procesos y procedimientos para cada uno de los Subsistemas de Administración de Riesgos.
- e. Realizar monitoreo y revisión de las funciones del área de control interno.
- f. Velar porque se dé cumplimiento a los lineamientos establecidos en el **Código de Conducta y Buen Gobierno** de la entidad en materia de conflictos de interés y uso de información privilegiada que tengan relación con el Sistema Integrado de Gestión de Riesgos.
- g. Vigilar cuidadosamente las relaciones de todas las personas que hacen parte de la entidad tanto interna como externamente, para identificar y controlar de manera eficiente los posibles conflictos de interés que puedan presentarse.
- h. Informar de manera oportuna mediante Oficio a la Superintendencia Nacional de Salud, acerca de cualquier situación excepcional que se presente o prevea que pueda presentarse como mínimo en el ámbito de la administración de los riesgos prioritarios, de las causas que la originan y de las medidas que se propone poner en marcha por parte de la entidad para corregir o enfrentar dicha situación, si procede.

### 13. OFICIAL DE CUMPLIMIENTO

De manera voluntaria y sin perjuicio del cumplimiento de otras disposiciones, la institución cuenta con un proceso de apoyo, orientación y evaluación, que tendrá a su cargo la administración y gestión de los diferentes riesgos a los cuales se encuentra expuesta (incluyendo los riesgos priorizados) a través de la identificación, medición, control y monitoreo de cada uno de ellos de tal manera que se realice la evaluación continua del ciclo para detectar las desviaciones y generar insumos para la formulación de los planes de mejoramiento y demás información que requiera el Comité de Riesgos. La persona encargada del proceso de Gestión de riesgo será un Oficial de Cumplimiento, que gestionará el proceso, liderará los comités de riesgo y trabajará en conjunto con otros procesos y subprocesos de la institución para administrar los riesgos de manera óptima.

### 14. REQUISITOS DEL OFICIAL DE CUMPLIMIENTO

El oficial de cumplimiento debe cumplir como mínimo con los siguientes requisitos:

- a. Depender directamente del Órgano de Administración o Dirección dentro de la estructura organizacional. Es decir, pertenecer como mínimo al segundo nivel jerárquico en el área administrativa.

- b.** Tener capacidad decisoria frente a los reportes y temas relacionados con la prevención de riesgos en cada uno de los Subsistemas que componen el Sistema Integrado de gestión de Riesgo.
- c.** Acreditar conocimiento en materia de administración de riesgos mediante certificación expedida por parte de instituciones autorizadas por el Ministerio de Educación Nacional para impartir información de dicha materia, en la que conste que la duración del diplomado no sea inferior a 90 horas y el curso e-learning de la UIAF. En caso de que sea una especialización, será válida en riesgos en general. Si no posee ninguna de las anteriormente mencionadas certificaciones, se puede certificar con cuatro (4) años de experiencia laboral en áreas de administración de riesgos.
- d.** No pertenecer a órganos de control ni a las áreas directamente relacionadas con las actividades previstas en el objeto social principal.
- e.** Ser empleado directo de la entidad.

En caso de que exista un Oficial de Cumplimiento suplente debe cumplir con los requisitos del **b** al **e**.

## 15. FUNCIONES DEL OFICIAL DE CUMPLIMIENTO

El oficial de cumplimiento debe desempeñar como mínimo las siguientes funciones:

- a.** Apoyar en el diseño de las metodologías de segmentación, identificación, medición, control y monitoreo de los riesgos a los que se expone la entidad, para mitigar su impacto.
- b.** Sugerir al Comité de Riesgos, en los casos que aplique, los ajustes o modificaciones necesarios a las políticas de los diferentes Subsistemas de Administración de Riesgos.
- c.** Proponer al Comité de Riesgos, en los casos que aplique, el manual de procesos y procedimientos, a través de los cuales se llevarán a la práctica las políticas aprobadas para la implementación de los diferentes Subsistemas de Administración de Riesgos. Asimismo, velar por su actualización, divulgación y apropiación en todos los niveles de la organización y su operatividad.
- d.** Velar por el adecuado diseño e implementación de los controles a los diferentes riesgos para mitigar su impacto, en todos los niveles de la organización y su operatividad.
- e.** Realizar seguimiento o monitoreo a la eficiencia y la eficacia de las políticas, procedimientos y controles establecidos.
- f.** Apoyar a las áreas en la identificación y evaluación de los límites de exposición para cada uno de los riesgos identificados, y presentar al Comité de Riesgos, en los casos que aplique, las observaciones o recomendaciones que considere pertinentes.
- g.** Monitorear las condiciones de suficiencia patrimonial y financiera de la entidad, de acuerdo con la Resolución 3100 de 2019 o las normas que la sustituyan o modifiquen.
- h.** Velar por el adecuado archivo de los soportes documentales y demás información relativa al Sistema Integrado de Gestión de Riesgos de la entidad.

- i. Participar en el diseño y desarrollo como mínimo de los programas de capacitación sobre los riesgos identificados y velar por su cumplimiento. Incluir por lo menos los riesgos de los Subsistemas de Administración de Riesgos.
- j. Analizar los informes presentados por la Auditoría Interna o quien haga sus veces, y los informes que presente el Revisor Fiscal para que sirvan como insumo para la formulación de planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.
- k. Monitorear e informar al Comité de Riesgos, en los casos que aplique, el avance en los planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.
- l. Presentar de forma semestral a planeación Institucional y anual a la Junta Directiva, un informe escrito donde se exponga el resultado de su gestión, donde se mencionen:
- los procesos establecidos para llevar a la práctica las políticas aprobadas,
  - los resultados de monitoreo y seguimiento a los controles de riesgo establecidos,
  - medidas y acciones correctivas adoptadas para corregir falencias en los monitoreo de controles,
  - cumplimiento de los requerimientos exigidos por las autoridades,
  - propuestas de ajuste o modificaciones a políticas,
  - últimas normas o reglamentaciones expedidas sobre la prevención y control del riesgo y medidas adoptadas para darles cumplimiento a las mismas.

No podrán contratarse con terceros las funciones asignadas al Oficial de Cumplimiento, ni aquellas relacionadas con la identificación y reporte de operaciones inusuales.

## 16. PROCESO DE GESTIÓN DEL RIESGO

De manera voluntaria y sin perjuicio del cumplimiento de otras disposiciones, UNA cuenta con un área de apoyo, orientadora y de evaluación, que tendrá a su cargo la administración y gestión de los diferentes riesgos a los cuales las entidades se encuentran expuestas (incluyendo los riesgos priorizados) a través de la identificación, medición, control y monitoreo de cada uno de ellos de tal manera que se realice la evaluación continua del ciclo para detectar las desviaciones y generar insumos para la formulación de los planes de mejoramiento y demás información que requiera el Comité de Riesgos, en los casos que aplique, mediante el trabajo conjunto con todas las áreas.

El proceso de gestión del riesgo tiene las siguientes funciones:

- a. Apoyar en el diseño de las metodologías de segmentación, identificación, medición, control y monitoreo de los riesgos a los que se expone la entidad, para mitigar su impacto.
- b. Sugerir al Comité de Riesgos, en los casos que aplique, los ajustes o modificaciones necesarios a las políticas de los diferentes Subsistemas de Administración de Riesgos.
- c. Proponer al Comité de Riesgos, en los casos que aplique, el manual de procesos y procedimientos, a través de los cuales se llevarán a la práctica las políticas aprobadas para la implementación de los diferentes Subsistemas de Administración de Riesgos. Asimismo, velar por su actualización, divulgación y apropiación en todos los niveles de la organización y su operatividad.

- d. Velar por el adecuado diseño e implementación de los controles a los diferentes riesgos para mitigar su impacto, en todos los niveles de la organización y su operatividad.
- e. Realizar seguimiento o monitoreo a la eficiencia y la eficacia de las políticas, procedimientos y controles establecidos.
- f. Apoyar a las áreas en la identificación y evaluación de los límites de exposición para cada uno de los riesgos identificados, y presentar al Comité de Riesgos, en los casos que aplique, las observaciones o recomendaciones que considere pertinentes.
- g. Monitorear las condiciones de suficiencia patrimonial y financiera de la entidad, de acuerdo con la Resolución 3100 de 2019 o las normas que la sustituyan o modifiquen.
- h. Velar por el adecuado archivo de los soportes documentales y demás información relativa al Sistema Integrado de Gestión de Riesgos de la entidad.
- i. Participar en el diseño y desarrollo como mínimo de los programas de capacitación sobre los riesgos identificados y velar por su cumplimiento. Incluir por lo menos los riesgos de los Subsistemas de Administración de Riesgos.
- j. Analizar los informes presentados por la Auditoría Interna o quien haga sus veces, y los informes que presente el Revisor Fiscal para que sirvan como insumo para la formulación de planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.
- k. Monitorear e informar al Comité de Riesgos, en los casos que aplique, el avance en los planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.

## 17. COMITÉ DE RIESGOS

- a. Evaluar y formular a la Junta Directiva o quien haga sus veces, las metodologías de segmentación, identificación, medición, control y monitoreo de los riesgos a los que se expone la entidad, para mitigar su impacto, presentadas y diseñadas por el área de gestión de riesgos. Asimismo, las actualizaciones a las que haya lugar.
- b. Velar por el efectivo, eficiente y oportuno funcionamiento del ciclo general de gestión de riesgos, incluyendo todas las etapas que se mencionaron en el punto anterior, para cada uno de los riesgos identificados.
- c. Evaluar y formular a la Junta Directiva o quien haga sus veces, los ajustes o modificaciones necesarios a las políticas de los diferentes Subsistemas de Administración de Riesgos, presentadas y diseñadas por el área de gestión de riesgos.
- d. Evaluar y proponer a la Junta Directiva o quien haga sus veces, el manual de procesos y procedimientos y sus actualizaciones, a través de los cuales se llevarán a la práctica las políticas aprobadas para la implementación de los diferentes Subsistemas de Administración de Riesgos.
- e. Identificar las consecuencias potenciales que pueda generar la materialización de los diferentes riesgos sobre las operaciones que realiza la entidad.
- f. Evaluar los límites de exposición para cada uno de los riesgos identificados, y presentar a la Junta Directiva y al Representante Legal, las observaciones o recomendaciones que considere pertinentes, presentadas y diseñadas por el área de gestión de riesgos.
- g. Objetar la realización de aquellas operaciones que no cumplan con las políticas o límites de riesgo establecidas por la entidad o grupo empresarial oficialmente reconocido al cual esta pertenezca. Cabe resaltar que de acuerdo con las políticas que establezca la entidad, cada instancia podrá tener diferentes atribuciones para aprobar operaciones que incumplan las

políticas establecidas inicialmente por la entidad y que violen los límites de exposición para cada uno de los riesgos identificados.

**h.** Conocer y discutir los resultados de las pruebas de tensión (stress test) en el caso que apliquen y el plan de acción a ejecutar con base en ellos para informarlo a la Junta Directiva, Consejo de Administración u órgano que haga sus veces.

**i.** Informar a la Junta Directiva y al Representante Legal sobre los siguientes aspectos:

- El comportamiento y los niveles de exposición de la entidad a cada uno de los riesgos (como mínimo los riesgos prioritarios), así como las operaciones objetadas. Los informes sobre la exposición de riesgo deben incluir un análisis de sensibilidad por escenarios y pruebas bajo condiciones extremas basadas en supuestos razonables (stress testing).
- Las desviaciones con respecto a los límites de exposición de riesgo previamente establecidos, si se llegasen a presentar (posibles incumplimientos frente a los límites), operaciones poco convencionales o por fuera de las condiciones de mercado y las operaciones con vinculados.
- Validar e informar a la Junta Directiva y al Representante Legal, el avance en los planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.”

## 18. REVISOR FISCAL

El revisor fiscal deberá cerciorarse que las operaciones, negocios y contratos que celebre se ajusten a las instrucciones y políticas aprobadas por el máximo órgano social.

Deberá también dar cuenta por escrito de forma anual a la Junta Directiva, al representante legal, las disposiciones contenidas en el SARLAFT y el resto de los subsistemas.

De igual forma, deberá poner en conocimiento del Oficial de Cumplimiento, las inconsistencias y falencias que detecte respecto a la implementación de los controles establecidos.

Finalmente, deberá rendir los informes que le solicite la Superintendencia Nacional de Salud.

## 19. MÁXIMO ORGANO SOCIAL

Se tienen como funciones aquellas dispuestas en los estatutos y en el reglamento de funcionamiento de la propia Asamblea General, sin perjuicio de lo dispuesto por la normatividad legal vigente para cada entidad en particular.

El Máximo Órgano Social se encarga entre otras actividades de:

- a.** Estudiar y aprobar las reformas de los estatutos.
- b.** Velar por el cumplimiento de los objetivos de la entidad y sus funciones indelegables, mediante la realización de asambleas, que pueden celebrarse de manera ordinaria a extraordinaria.
- c.** Examinar, aprobar a improbar los balances de fin de ejercicio y las cuentas que deban rendir los administradores o representantes legales.
- d.** Considerar los informes de los administradores a del Representante Legal sabré el estado de los negocios sociales, y el informe del Revisor Fiscal.

- e. Analizar y aprobar los principios y procedimientos para la selección de miembros de la Alta Gerencia y de la Junta Directiva de la entidad, definición de funciones y responsabilidades, organización, estrategias para la toma de decisiones, evaluación y rendición de cuentas.
- f. Las demás que les señalen los estatutos o las leyes.

## 20. AUDITORIA INTERNA

Sin perjuicio de las funciones asignadas en otras disposiciones a la Auditoría Interna, o quien ejerza el control interno, ésta debe evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SICOF y SARLAFT, con el fin de determinar las deficiencias y sus posibles soluciones. Así mismo, deberán informar los resultados de la evaluación al representante legal o junta directiva.

## 21. ORGANOS DE CONTROL

Los órganos de control serán, por lo menos, Revisoría Fiscal y la Auditoría Interna, cuando apliquen. Estos deberán identificar las operaciones realizadas con entidades o personas vinculadas a la entidad, y promover revisiones independientes para validar la efectividad del Sistema Integrado de Gestión de Riesgos de la entidad y de los Subsistemas por los cuales está conformado, además de las responsabilidades y obligaciones que se encuentren establecidas en otras disposiciones legales, estatutarias o en reglamentos.

## 22. INFRAESTRUCTURA TECNOLÓGICA

La INSTITUCIÓN hará uso de todas las herramientas a su disposición para garantizar el funcionamiento efectivo, eficiente y oportuno del Sistema Integrado de Gestión de Riesgos, siendo la matriz de riesgo el medio principal para lograr el cumplimiento de todas las etapas del sistema.

En base a la información consolidada en la matriz se generarán informes semestrales dirigidos a gerencia y al comité de riesgo donde se expondrá el comportamiento de cada uno de los subsistemas, así como capacitaciones realizadas, resultados de las búsquedas en listas vinculantes, reportes presentados a entidades de control y reevaluación de los riesgos.

La información referente al sistema de gestión de riesgos será gestionada digitalmente por el líder de proceso de Gestión de riesgos y puesta a disposición en la carpeta de archivos compartidos para consulta por parte de otros empleados de la institución. La información se almacenará en la carpeta compartida institucional de la institución. Solo tendrán acceso para edición de la información los líderes del proceso de Gestión de Riesgo y de Gestión Integral para la calidad. La información será de acceso para consulta únicamente para el resto de los colaboradores. Cualquier modificación propuesta a alguno de los manuales del proceso deberá ser comunicada al proceso de Gestión Integral para la calidad.

Para la revisión de listas de clientes (tanto proveedores como nuevas contrataciones asistenciales y administrativas), se implementará un software especializado.

## 23. DIVULGACIÓN DE INFORMACIÓN Y CAPACITACIONES

ESE Universitaria del Atlántico programará y coordinará planes de divulgación y capacitación una vez al año a todos los procesos y colaboradores de la organización, priorizando los procesos de Gestión Integral de la calidad, Planeación Institucional, Gestión del Recurso Humano y SST, Gestión de facturación y Gestión Jurídica. Se comunicará a dichos procesos sobre las políticas, procedimientos, herramientas y controles adoptados por la institución para dar cumplimiento al Sistema. Ver Cronograma de actividades Gestión del Riesgo y Seguimiento de estos en **Matriz de riesgos**.

Los lineamientos de cada uno de los Subsistemas de Administración de Riesgos se divulgarán en los procesos de inducción de nuevos contratados y será divulgado como re-inducción a colaboradores que se encuentren actualmente trabajando en la INSTITUCIÓN y no hayan recibido dicha capacitación.

Se debe dejar constancia de las capacitaciones realizadas por medio de la presentación de una prueba de los temas expuestos a los participantes con el fin de incentivar la adherencia y el entendimiento, y, en donde se indique como mínimo la fecha, los temas tratados y el nombre de los asistentes.

## 24. DIVULGACIÓN DE INFORMACIÓN INTERNA

Como resultado del monitoreo y control de cada uno de los riesgos identificados y especialmente los prioritarios, las entidades deben elaborar reportes semestrales como mínimo, que permitan establecer el perfil de riesgo de éstas.

Asimismo, se elaboran informes de gestión al cierre de cada ejercicio contable sobre el cumplimiento de las políticas, los límites establecidos y su grado de cumplimiento, el nivel de exposición a los diferentes riesgos a los que se ve expuesta la INSTITUCIÓN que incluya los prioritarios y la cuantificación de los efectos de la posible materialización de estos sobre la salud de la población de su área de influencia, las utilidades, el patrimonio y el perfil de riesgo. Esta información será extraída y analizada de la matriz de riesgo de la cual se encargará de hacer seguimiento el Oficial de Cumplimiento.

Los informes irán dirigidos a Gerencia, a la Junta Directiva o quien haga sus veces y los líderes de los procesos involucrados, los cuales deben quedar plasmados en **acta donde se socialicen estos informes**.

## 25. DIVULGACIÓN DE INFORMACIÓN EXTERNA

Los administradores de las entidades, en su informe de gestión, al cierre de cada ejercicio contable, incluirán en las notas a los estados financieros un apartado sobre la gestión adelantada en materia de administración como mínimo de los subsistemas de gestión de riesgos descritos en esta Circular. En este sentido, las notas son un resumen de su situación en materia de la administración de dichos riesgos con información tanto cualitativa como cuantitativa.

### 25.1. LINEAMIENTOS ESPECIFICOS DE LOS SUBSISTEMAS DE ADMINISTRACIÓN DE RIESGOS

El presente capítulo contiene los lineamientos específicos de los Subsistemas de Administración de Riesgos para cada uno de los riesgos prioritarios (salud, actuarial, crédito, liquidez, mercado de capitales, operacional, y finalmente para la gestión del riesgo de grupo), sin perjuicio de los demás riesgos identificados por la entidad.

Para el Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT), los lineamientos específicos se encuentran publicados en la Circular Externa 009 de 2016 (expedida por la SNS) y sus modificatorias, y adaptado en el **manual SARLAFT** de la INSTITUCIÓN.

Para el Riesgo de riesgo de corrupción, opacidad y fraude (SICOF), los lineamientos y modificaciones a las circulares externas 018 de 2015, 009 de 2016, 007 de 2017 y 003 de 2018 se encuentran publicadas en la Circular Externa **2021170000005-5 DE 2021** y adaptado en el **manual SICOF** de la INSTITUCIÓN.

## 26. GESTIÓN DE RIESGO EN SALUD

Se entiende por Riesgo en Salud 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 o la necesidad de requerir más consumo de bienes y servicios que hubiera podido evitarse. El evento, es la ocurrencia de la enfermedad, traumatismos o su evolución negativa, desfavorable o complicaciones de esta; y las causas, son los diferentes factores asociados a los eventos. De esta manera, se incluyen el marco institucional y el ciclo de gestión de riesgo en salud.

## 27. CICLO DE LA GESTION DE RIESGO EN SALUD

### 27.1. IDENTIFICACIÓN DEL RIESGO EN SALUD

- a. Se realiza la identificación de la situación en salud del territorio donde se encuentran habilitados y de la población objeto de la INSTITUCIÓN o afiliada a la EPS con la que existe una relación contractual.
- b. Se caracterizan los servicios ofertados según modalidades de atención y contratación, teniendo en cuenta los grupos de riesgos de la población potencialmente usuaria de estos servicios, que permita una gestión clínica óptima en el marco de un enfoque diferencial.
- c. Caracterización de la demanda de servicios ex-ante, efectiva y agregada propia de la entidad, teniendo en cuenta un enfoque diferencial (género, grupo etario, étnico, curso de vida, territorial, grupos de riesgo, entre otros).
- d. A través del sistema de reporte institucional de incidentes y eventos adversos. (Formatos de identificación y análisis de Eventos e incidentes adversos) y de análisis de análisis realizados por colaboradores a través **las herramientas institucionales para el reporte de eventos adversos para la identificación** y medidas de control para riesgos en salud.
- e. Caracterización de los riesgos existentes en cada uno de los servicios declarados con su respectiva estrategia de prevención. Ver Política de Seguridad del Paciente y Protocolo para la correcta identificación del paciente en procesos asistenciales.

ESE Universitaria del Atlántico debe realizar la evaluación de la capacidad de oferta de los servicios, teniendo en cuenta la capacidad instalada y la oferta de talento humano con respecto a la capacidad de producción, discriminado en cada uno de los servicios.

El desarrollo e implementación de la política de seguridad del paciente es de crucial importancia en la identificación de riesgos en salud, puesto que se tiene en cuenta el diagnóstico de los eventos adversos prevenibles ocurridos y los procesos asistenciales de mayor riesgo.

Es fundamental que la INSTITUCIÓN vele por la disponibilidad y confiabilidad de la información acerca de la exposición al riesgo y de la gestión de los eventos adversos ocurridos. Debe tenerse en cuenta que el reporte de incidentes y eventos adversos no es un medio confiable para conocer la verdadera magnitud del riesgo sino una herramienta para profundizar la cultura de la seguridad mediante el aprendizaje alcanzado con el análisis de eventos y los planes de acción diseñados en conjunto con los interesados.

## 27.2. MEDICIÓN Y EVALUACIÓN DEL RIESGO EN SALUD

Posterior a la identificación de los riesgos en salud se debe realizar la medición y evaluación de los mismos, para determinar el nivel de riesgo la institución se vale de una Matriz de Riesgos, donde se pueden contemplar los posibles riesgos en salud por cada proceso:

- a. Se determina la probabilidad de ocurrencia y la severidad de las consecuencias máximas posibles o impacto, sobre la salud de los usuarios, en caso de presentarse un evento derivado de cada riesgo identificado.
- b. Se establecen costos que representa para la institución en términos de sobrecosto asistencial (susceptible de ser objeto de rechazo o glosa), riesgo jurídico, etc. **Este análisis establece un vínculo entre los riesgos en salud y el riesgo operacional y financiero.**
- c. Se priorizan los riesgos de salud acorde con los criterios de valoración de UNA y armonizados con los lineamientos, pautas e instrumentos en salud expedidos por las autoridades competentes en caso de que aplique, y con las prioridades territoriales y poblacionales.
- d. Se definen límites de tolerancia para cada riesgo o factor de riesgo identificado de forma tal que se establezcan metas de control o mitigación para el sistema de gestión; pero priorizando los recursos sobre aquellos riesgos de mayor importancia teniendo en cuenta la clasificación de riesgo neto de cada riesgo considerado.
- e. Priorizar aquellos riesgos de mayor importancia, sin que eso implique ignorar, dejar de vigilar y no tratar de evitar, otros riesgos que se consideran de menor importancia y que pueden estar presentes en la Institución (Riesgos **BAJOS** o **MODERADOS**).

## 27.3. TRATAMIENTO Y CONTROL DE RIESGOS EN SALUD

Se consideran como elementos mínimos para la selección e implementación de tratamiento y control los siguientes:

- a. Monitorear el logro de metas, acorde con los límites de aceptación y tolerancia para los riesgos en salud identificados, además permite apoyar el replanteamiento de estrategias de intervención en caso de ser necesario para garantizar el cumplimiento de las metas planteadas. Para ello se diseñan e implementan procedimientos y programas en los que se definirán los tratamientos a los riesgos en salud identificados (Deben contener indicadores).
- b. Monitoreo y evaluación de los indicadores de calidad y salud correspondiente a aquellos factores de riesgo que se hayan identificado como **prioritarios**.
- c. Para riesgos en niveles mayores al nivel de tolerancia definido por la organización; se generan planes de acciones que incluyan capacitación, comunicación y revisión periódica de implementación y resultados.
- d. Diseño, implementación, evaluación y seguimiento de los procesos y procedimientos institucionales y su articulación; de tal manera que garanticen el acceso y la calidad de los servicios ofertados.

Recomendable:

- e. Utilizar modelos de contratación y mecanismos de pago con sus proveedores orientados a la obtención de resultados en salud y pago por desempeño e incentivos, los cuales deben ir articulados con el Modelo de Atención en Salud planteado por la entidad.
- f. Implementar jornadas de capacitación a su personal, haciendo énfasis en el procedimiento de evaluación, seguimiento, y adherencia a guías, protocolos de práctica clínica, normas técnicas, lineamientos y orientaciones.

## 28. GESTIÓN DE RIESGO OPERACIONAL

El Riesgo Operacional corresponde a la probabilidad que la institución presente desviaciones en los objetivos misionales, como consecuencia de deficiencias, inadecuaciones o fallas en los procesos, en el recurso humano, en los sistemas tecnológicos, legal y biomédicos, en la infraestructura, por fraude, corrupción y opacidad, ya sea por causa interna o por la ocurrencia de acontecimientos externos, entre otros.

El presente subsistema es desarrollado a fondo en el **manual del Subsistema de Administración de Riesgo Operacional (SARO)**.

Pueden generar pérdidas de **tres** tipos:

- i) Pérdidas en los resultados en salud de los pacientes, los cuales, por su relevancia son tratados como riesgos en salud.
- ii) Pérdidas en los resultados operativos esperados, incluyendo la satisfacción de la población en su área de influencia, que deben ser tratados en el resultado de la gestión de los riesgos operacionales.
- iii) Pérdidas financieras en la entidad, que corresponden a la contabilización de los eventos de riesgo y los riesgos que se materializaron, tratados en la evaluación de los riesgos financieros.

La implementación y seguimiento a estos riesgos van estrechamente ligados a las políticas, principios y valores institucionales establecidos en el Gobierno Organizacional.

## 29. CICLO GENERAL DE GESTIÓN DEL RIESGO OPERACIONAL

### 29.1. IDENTIFICACIÓN DEL RIESGO OPERACIONAL

- a) Para el óptimo desarrollo del **SARO** los siguientes procesos apoyan para el cumplimiento de las funciones de la institución y recopilación de información veraz en cuanto al comportamiento de los riesgos operacionales:
  - Atención de Apoyo Diagnóstico y Terapéutico
  - Referencia y Contrarreferencia
  - Sistemas de información en salud
  - Calidad
  - Gestión del talento humano
  - Gestión Financiera.
  - Gestión administrativa y jurídica.
- b) Identificación de los eventos de riesgo operacional, potenciales y ocurridos, en cada uno de los procesos. (Implementar matriz de riesgos)
- c) Identificación de procesos jurídicos en los que se encuentre la entidad.
- d) Identificación pérdidas en los resultados en salud de sus pacientes, los cuales, por su relevancia son tratados como riesgos en salud.
- e) Determinación de potenciales pérdidas financieras en la entidad causadas por los eventos de riesgo operacional identificados.

La etapa de identificación debe realizarse previamente a la implementación de nuevos procesos o a la modificación de cualquier proceso, así como en los casos de fusión, adquisición, cesión de activos, pasivos y contratos, entre otros.

f) Los riesgos operacionales potenciales se registran en la matriz de riesgo institucional, **de materializarse un riesgo operacional se debe diligenciar el formato de materialización de riesgo operacional** en el que quedara registro de pérdidas ocasionadas, tipo de riesgo, causas y consecuencias del evento en concreto. Ver formato de registro de riesgos operacionales.

#### 29.1.1. MEDICION Y EVALUACION DE RIESGO OPERACIONAL

En esta etapa, el Subsistema de Administración de Riesgo Operacional debe medir la probabilidad de ocurrencia de un evento de riesgo operacional y su impacto en caso de materializarse. Se elabora un plan de ajuste que para la posterior medición cuantitativa del riesgo. Se implementará matriz de riesgo institucional para este fin.

#### 29.1.2. TRATAMIENTO Y CONTROL DE RIESGO OPERACIONAL

Se debe permitir a la INSTITUCIÓN tomar medidas adecuadas para controlar el riesgo operacional inherente al que se ve expuesta en el desarrollo de sus operaciones con el fin de disminuir la probabilidad de ocurrencia y/o impacto en caso de que se materialicen. Para esto:

- a. Diseñar e implementar controles para cada riesgo de manera que se pueda mitigar, ya sea mediante su probabilidad, impacto o ambos.
- b. Incluir los controles diseñados dentro de las políticas y procedimientos de la entidad.
- c. Se formularán acciones preventivas para evitar ocurrencia del evento, controles sobre dichas acciones, así como acciones de contingencia ante la posible materialización del mismo. Se debe implementar un **Plan de Continuidad del Negocio** aprobado por Gerencia.

### 30. PLAN DE CONTINUIDAD DEL NEGOCIO

ESE Universitaria del Atlántico define, implementa, prueba y mantiene un proceso para administrar y asegurar la continuidad del negocio en situaciones de emergencia o desastre, incluyendo elementos como la prevención y la atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal en su **PLAN DE CONTINUIDAD DEL NEGOCIO**.

Este contiene:

- a. Eventos que pueden afectar la operación.
- b. Actividades por realizar cuando se presentan las fallas.
- c. Alternativas de operación.
- d. Proceso de retorno a la actividad normal.

### 30.1. Acreditación con soportes de todas las operaciones, negocios y contratos

Las entidades deben establecer reglas específicas que prohíban la realización de actividades, negocios y contratos sin que exista el respectivo soporte interno y/o externo, debidamente fechado y autorizado por quienes intervengan en ellos o los elaboren. Todo documento que acredite transacciones, negocios o contratos de la entidad, además de constituir el soporte de la negociación y del registro contable, constituye el respaldo probatorio para cualquier investigación que puedan adelantar las autoridades competentes.

## 31. GESTIÓN DE RIESGO ACTUARIAL

Se entiende por riesgo actuarial la posibilidad de incurrir en pérdidas económicas debido a no estimar adecuadamente el valor de los contratos según los diferentes tipos de contratos (cápita, evento, Grupo Relacionado de Diagnóstico, Pago Global Prospectivo entre otros) por venta de servicios, de tal manera que estos resulten insuficientes para cubrir las obligaciones futuras que se acordaron. Estas estimaciones deben realizarse teniendo en cuenta algunos eventos futuros e inciertos que podrían ocurrir como:

- a. Desconocimiento de la demanda efectiva de servicios que van a atender, de la situación en salud de la población y de las frecuencias de uso.
- b. Concentración poblacional, con un enfoque diferencial de género, étnico, grupos etarios, regiones, grupo de riesgo, curso de vida, entre otros.
- c. Atención en zonas de difícil acceso y alta dispersión de la población.
- d. Hechos catastróficos o situaciones similares que afecten un número elevado de la población incluida en los contratos.
- e. Variaciones en las condiciones de morbi-mortalidad de la población incluida en los contratos.
- f. Incrementos inesperados en los costos de proveedores.
- g. Incorporación de tecnología nueva que requiera recursos de inversión considerables.

El presente subsistema es desarrollado a fondo en el **manual del Subsistema de Administración de Riesgo Actuarial**.

## 32. CICLO GENERAL DE GESTIÓN DE RIESGO ACTUARIAL

### 32.1. IDENTIFICACIÓN DEL RIESGO ACTUARIAL

- a. Caracterización y conocimiento de la población que incluirá en los contratos por venta de servicios teniendo en cuenta los aspectos geográficos, etarios, demográficos, la situación de morbi-mortalidad; así como la actualización de novedades.
- b. Particularidades de las diferentes modalidades de pago (por capitación, por evento, por paquete, entre otros).
  - Pago por Capitación: Identificación de las personas incluidas en el contrato e identificación de las actividades, procedimientos, intervenciones, insumos y medicamentos de baja complejidad incluidos en el contrato.
  - Pago por evento: Identificación de las actividades, procedimientos, intervenciones, insumos y medicamentos incluidos en el contrato para el cálculo de las tarifas y precios a ser aplicadas a las tecnologías en salud.
  - Pago por Grupo Relacionado de Diagnóstico: Identificación de las tecnologías en salud incluidas y no incluidas asociadas a la condición o condiciones individuales de salud, comorbilidades, complicaciones o eventos adversos de acuerdo con el grupo de riesgo.
  - Pago Global Prospectivo: Identificación de las tecnologías en salud incluidas y no incluidas asociadas a la condición o condiciones individuales de salud, comorbilidades, complicaciones o eventos adversos de acuerdo con el grupo de riesgo. Además, de tener en cuenta la frecuencia estimada de los episodios de atención y/o de tecnologías en salud a ser prestadas con cargo a la suma global.

- c. Identificación de posibles incrementos en los costos de insumos y medicamentos, entre otros.
- d. Registrar los riesgos identificados en la matriz de riesgo institucional.

### 32.2. MEDICIÓN Y EVALUACIÓN DEL RIESGO ACTUARIAL

Como mecanismos para el control de riesgos actuariales identificados se han de considerar:

- a. Anticipar incrementos inesperados en los índices de morbi-mortalidad y, por ende, en los costos de atención que puedan sobrepasar el valor pactado en los contratos.
- b. Realizar proyecciones que incluyan los posibles impactos y la ocurrencia, entre otros, de los factores de riesgo asociados a la concentración, hechos catastróficos, incrementos en los costos de nueva tecnología y el cambio del perfil sociodemográfico de la población de su área de influencia, que pueden tener efectos sobre la frecuencia y características de la demanda de servicios de salud.
- c. Construcción de modelos de cuantificación que contemplen de manera adecuada, las pérdidas esperadas e inesperadas, a las que se encuentra expuesta la entidad

Los modelos que se adopten para calcular estas pérdidas **deben** contar con los siguientes parámetros teniendo en cuenta las particularidades de cada tipo de contrato:

- e. La probabilidad de ocurrencia del evento (materialización del riesgo) en la unidad de tiempo (frecuencia).
- f. Los asociados con cada distribución de pérdida que mejor defina la cuantía de la pérdida (impacto). Es decir, el cálculo del costo promedio del servicio.
- g. El nivel de exposición del riesgo en la unidad de tiempo.

### 32.3. TRATAMIENTO Y CONTROL DE RIESGO ACTUARIAL

El Subsistema de Administración del Riesgo Actuarial debe permitir a la entidad tomar medidas adecuadas para controlar el riesgo actuarial, entre ellas:

- a. Establecer y actualizar periódicamente las políticas y las estimaciones actuariales para cada tipo de contrato, teniendo en cuenta los cambios que se presenten en el sector.
- b. Hacer una traza de las medidas tomadas por la administración, en respuesta a los problemas identificados y a las recomendaciones efectuadas.
- c. Realizar pruebas de estrés (Stress-Testing) y ejercicios de auto comprobación (Back-Testing) sobre los modelos actuariales utilizados para establecer los valores de los contratos, y de esta manera realizar los ajustes correspondientes.
- d. Realizar controles de calidad a los sistemas de información de la entidad.

## 33. GESTIÓN DEL RIESGO DE CRÉDITO

El Riesgo de Crédito corresponde a la posibilidad que una entidad incurra en pérdidas como consecuencia del incumplimiento de las obligaciones por parte de sus deudores en los términos acordados, como, por ejemplo, monto, plazo y demás condiciones.

Teniendo en cuenta la anterior definición, las entidades deben evaluar permanentemente el riesgo inherente que sus activos pierdan valor, como consecuencia de que un deudor o contraparte incumpla sus obligaciones. Es así como dentro de esta evaluación debe incorporar oportunamente los cambios significativos de las condiciones de cumplimiento de sus deudores.

El presente subsistema es desarrollado a fondo en el **manual del Subsistema de Administración de Riesgo de Crédito (SARC)**.

### 33.1. CICLO DE GESTIÓN DE RIESGO DE CRÉDITO

Para riesgos de crédito es necesario:

- a. Una evaluación de riesgo por contraparte (incluyendo los instrumentos financieros, tratándose de inversiones de renta fija), teniendo en cuenta los límites de exposición por contraparte asociadas a la evaluación de riesgos realizada. Se realiza una evaluación agrupando activos con características y perfiles de riesgo similares, pero deberá realizar esta evaluación en forma individual si el activo es significativo.
- b. Un modelo de cálculo de deterioros/provisiones por riesgo de crédito que sea adecuado para reflejar las potenciales pérdidas a las que está expuesta la entidad por el incumplimiento de las contrapartes y que se ajuste a la normatividad vigente.
- c. Procedimientos específicos de seguimiento, cobranza de las deudas y el establecimiento de mecanismos apropiados de negociación y recuperación de deudas que se encuentren en incumplimiento, han de diseñarse e implementarse.
- d. Una estrategia de gestión de glosas ante las EPS, la ADRES (o la entidad que ejerza sus funciones) o ante las Entidades Territoriales según sea el caso. La definición de la estrategia de gestión de glosas se debe formular en función del análisis histórico y su consecuente caracterización para determinar procesos específicos de actuación ante cada tipo de glosa.
- e. La verificación de los literales anteriores se debe realizar por lo menos una vez al año, para evaluar su funcionamiento y monitorear efectivamente la exposición a este riesgo.
- f. Las bases de datos utilizadas en el proceso de diseño de los modelos para la administración del riesgo crediticio deben tener una historia **mínima de tres (3) años**.

### 33.2. IDENTIFICACIÓN DE RIESGO DE CRÉDITO

Para la **identificación** de este riesgo, los aspectos mínimos a considerar por parte de la entidad parten de definir los tipos de activos expuestos a este riesgo, **como mínimo las cuentas por cobrar y los instrumentos financieros**. Estos últimos incluyen:

- a. Cuentas de Bancos y Fondos de Inversión Colectivas (FIC, antes Carteras Colectivas) tales como: cuentas corrientes; cuentas de ahorros; cuentas maestras de recaudo; FIC abiertos, del mercado monetario; carteras colectivas cerradas; y otros tipos de encargos fiduciarios o fondos de inversión fideicomisos, fondos de inversión colectiva inmobiliarios y/o fondos de capital privado, entre otros, siendo locales o extranjeros.
- b. Instrumentos inscritos en el Mercado de Valores de Colombia, tales como títulos de deuda pública emitidos o garantizados por la Nación o por el Banco de la República; títulos de renta fija emitidos, aceptados, garantizados o avalados por entidades vigiladas por la Superintendencia Financiera de Colombia, FOGAFIN y FOGACOOP.
- c. Todas las inversiones en títulos o valores de renta fija emitidos por entidades nacionales o extranjeras.
- d. Registrar en matriz de riesgo el riesgo de pérdida de valor de los activos por incumplimientos de deudores.

### 33.3. EVALUACIÓN Y MEDICIÓN DE RIESGO DE CRÉDITO

El Subsistema de Administración de Riesgo de Crédito ha de evaluar las pérdidas estimadas como resultado del incumplimiento de sus contrapartes. Dentro del Subsistema, la institución puede diseñar modelos para diferentes tipos de activos expuestos a este riesgo, dentro de los cuales deberá como mínimo contemplar la estimación de los siguientes elementos:

- a. La probabilidad de incumplimiento de los deudores dentro de un periodo de tiempo de 12 meses.
- b. Al interior de cada tipo de activo se deben generar categorías de calidad del deudor/contraparte que orienten una posterior asignación de factores de riesgo diferenciales según dicha categorización.
- c. La estimación de la pérdida esperada en que incurriría la entidad dado el incumplimiento. En este elemento se debe considerar tanto el valor expuesto del activo (saldo de la obligación o valor neto del activo) en el momento del incumplimiento, como la tasa de recuperación del valor del activo una vez se ha materializado el incumplimiento, la cual debe contemplar las recuperaciones efectivas que se han realizado sobre estos incumplimientos en los últimos 3 años y la existencia e idoneidad de las garantías, si las hubiese.

Para estimar la probabilidad que el deudor / contraparte no cumpla con sus obligaciones en los términos acordados, se recomienda como mínimo considerar los siguientes aspectos:

❖ **En el caso de los deudores/cuentas por cobrar:**

- a) Análisis históricos de las cuentas por cobrar de cada deudor según plazos y cumplimiento de pago, teniendo en cuenta los acuerdos de voluntades.
- b) La calidad del deudor y el plazo de la cartera (a mayor concentración de las deudas de mayor plazo, mayor el riesgo asociado al deudor).
- c) Adicional al análisis individual por deudor, se recomienda realizar un análisis segmentado por líneas de negocio (en los casos en que la entidad desarrolle varias actividades dentro del sector como aseguramiento obligatorio, voluntario, prestación de servicios de salud) y el concepto generador de la obligación, en el caso de las cuentas por cobrar.
- d) Estimar las posibles pérdidas que resulten de incumplimientos de pago frente a prestaciones realizadas u obligaciones generadas, las cuales involucran entre otros elementos, la evaluación de deterioros o posteriores valoraciones de acuerdo con las políticas contables que sobre los instrumentos financieros haya escogido la entidad, específicamente en las cuentas por cobrar.

❖ **En el caso de los instrumentos financieros:**

- a) Clasifique la seguridad del activo con fundamento en la calificación de crédito emitida por agencias calificadoras de riesgo tanto para el activo de renta fija como para el emisor, ya que estas calificaciones reflejan las probabilidades de incumplimiento de los activos en cada categoría de calificación.
- b) Asigne factores de riesgo en función de las probabilidades de incumplimiento para cada categoría de seguridad del activo. De no disponer de estudios propios que evalúen estas probabilidades de incumplimiento para los diferentes emisores y tipos de instrumentos financieros, se puede tomar como referencia los ponderadores que se mencionan en el Decreto 2954 de 2010 del Ministerio de Hacienda y Crédito Público y sus modificatorias.

Ver procedimiento de evaluación de incumplimiento de **proveedores y contrapartes**.

### 33.4. TRATAMIENTO Y CONTROL DE RIESGO DE CRÉDITO

La INSTITUCIÓN contempla dentro de este Subsistema de Administración y Gestión de Riesgo mecanismos de tratamiento y control del riesgo de crédito, los cuales deben ser aplicados de forma continua. Su frecuencia y criterios deberán definirse de acuerdo con lo pactado y observado en la matriz de riesgos.

Los **seguros de riesgo financiero** son un sistema empleado para proteger a las empresas frente a los posibles riesgos de carácter financiero que le puedan acontecer. Dentro de este tipo de riesgos podríamos destacar diversos tipos de actos fraudulentos, tales como robo, fraude, así como posibles decisiones administrativas que no reporten los datos esperados.

Para la Gestión exitosa de Riesgo de Crédito se debe tener en cuenta los siguientes aspectos:

- Retos para la gestión exitosa del riesgo del crédito
- Gestión de datos ineficiente. La imposibilidad de acceder a los datos correctos cuando se necesitan provoca retrasos problemáticos.
- Trabajo repetido constante. Los analistas no pueden cambiar los parámetros de los modelos con facilidad, lo que genera demasiada duplicación del esfuerzo y afecta negativamente el índice de eficiencia de un banco.
- Herramientas insuficientes para gestionar el riesgo.
- Reportes complicados. Los procesos de generación de reportes manuales basados en hojas de cálculo generan una sobrecarga en los analistas.

## 34. GESTIÓN DEL RIESGO DE LIQUIDEZ

### 34.1. CICLO DE GESTIÓN DE RIESGO DE LIQUIDEZ

El Riesgo de Liquidez corresponde a la posibilidad que una entidad no cuente con recursos líquidos para cumplir con sus obligaciones de pago tanto en el corto (riesgo inminente) como en el mediano y largo plazo (riesgo latente).

Como consecuencia de las actividades y operaciones diarias, las entidades se ven expuestas a este riesgo de liquidez. La gestión de liquidez de la entidad está relacionada con:

- a. Una adecuada recuperación de cartera (gestión de riesgo de crédito),
- b. Una adecuada modelación y monitoreo a las volatilidades del mercado financiero (gestión de riesgo de mercado de capitales).
- c. Una adecuada modelación y gestión de la razón combinada entre costos e ingresos por venta de servicios de salud contratados bajo modalidades diferentes al pago por evento (gestión de riesgo actuarial), dado que los flujos esperados de ingresos se ajustarían a las proyecciones de la entidad para cubrir con sus obligaciones.

La materialización de un riesgo de liquidez genera necesidades de recursos líquidos por parte de las entidades, las cuales pueden verse limitadas para realizar los pagos a terceros como pueden ser a proveedores, empleados y demás acreedores, lo que podría conllevar, entre otras consecuencias, a deficiencias en la prestación de los servicios de salud. Lo expuesto, puede generar un riesgo sistémico y afectar la percepción de los usuarios al servicio de salud y la viabilidad financiera de las entidades del sector.

El presente subsistema es desarrollado a fondo en el **manual del Subsistema de Administración de Riesgo de Liquidez (SARL)**.

### 34.2. IDENTIFICACIÓN DE RIESGOS DE LIQUIDEZ

Se tendrá en cuenta lo siguiente para el correcto análisis de riesgo de liquidez:

#### 34.2.1. ACTIVOS

a) Identificar los activos considerados como líquidos (aquellos que proveen a la entidad de liquidez inmediata). Se recomienda incluir dentro de estos como mínimo, el disponible que esté consignado en bancos y/o inversiones en Fondos de Inversión Colectiva (FIC) en las siguientes modalidades: cuentas corrientes, cuentas de ahorros (cuentas maestras de recaudo), FIC abiertos, del mercado monetario y cualquier otro tipo de encargo fiduciario o fondo de inversión, fideicomisos, fondos de inversión colectiva de inmobiliarios y fondos de capital privado que no tengan restricciones para el retiro inmediato de recursos

(sin pacto de permanencia). Asimismo, se deben identificar todas las inversiones en títulos o valores, sean de renta fija o renta variable, emitidos por entidades nacionales o extranjeras, públicas o privadas, que considere de fácil realización.

**b)** Identificar los recursos y plazos de recuperación de cartera (cuentas por cobrar). Tener en cuenta el comportamiento histórico de cartera vencida para aplicar factores de descuento o de castigo, en los casos que considere necesario para obtener una aproximación mucho más cercana a la realidad.

**c)** Identificar los ingresos causados y recibidos por venta o prestación de servicios de salud.

**d)** Proyectar cualquier movimiento de entradas futuras de efectivo por cualquier concepto, entre los cuales puede estar el portafolio de inversiones: vencimiento de títulos de renta fija o de operaciones, cobro de cupones, rendimientos de un CDT, dividendos en efectivo, entre otros flujos que se esperan recibir.

#### **34.2.2. PASIVOS**

**a)** Identificar y caracterizar las cuentas por pagar bajo cualquier concepto (insumos y medicamentos; dispositivos médicos o equipo biomédico; salarios; gastos operativos y administrativos; entre otros).

**b)** Identificar el valor causado y pagado de los costos y gastos de la operación de la entidad.

**c)** Proyectar cualquier movimiento de salidas futuras de efectivo bajo cualquier concepto, los cuales pueden presentarse por la emisión de instrumentos financieros, el pago de cupones de emisiones de deuda por renta fija y el pago de dividendos por acciones emitidas, entre otros flujos a entregar.

#### **34.2.3. EVALUACIÓN Y MEDICIÓN DE RIESGO DE LIQUIDEZ**

El Subsistema de Administración de Riesgo de Liquidez debe permitir a las entidades cuantificar el nivel mínimo diario de efectivo o equivalentes de efectivo requerido, en moneda nacional y/o extranjera, de acuerdo con la normatividad vigente, que le permita cumplir de manera oportuna con sus obligaciones de pago.

Para la medición del riesgo de liquidez se requiere que la entidad aplique una "prueba de liquidez" periódicamente con el fin de identificar potenciales necesidades de liquidez o recursos líquidos para cubrir sus flujos de pago y las causas de potenciales situaciones de iliquidez.

#### **34.2.4. TRATAMIENTO Y CONTROL DE RIESGO DE LIQUIDEZ**

Se ha de realizar un seguimiento continuo de la exposición de la INSTITUCIÓN al riesgo de liquidez mediante las alertas tempranas, los límites de exposición y los indicadores de liquidez que la entidad haya elaborado con el fin de monitorear y realizar los controles adecuadamente y a tiempo para evitar que el riesgo de liquidez pueda llegar a materializarse e impactar negativamente en los objetivos de la entidad. En caso de que se materialice el riesgo, la entidad deberá tomar las medidas correctivas para mitigar dicho impacto.

Dicho seguimiento debe permitir la elaboración de reportes gerenciales y de monitoreo del riesgo de liquidez que evalúe los resultados de las estrategias de la entidad e incluyan el resumen de las posiciones que contribuyen significativamente a dicho riesgo.

Para mejorar el flujo de recursos se requiere disponibilidad de información necesaria para diseñar el flujo de efectivo se requiere como mínimo:

- a. Sistema de información que permita la identificación y gestión del recaudo de los ingresos y egresos de la entidad acorde con los diferentes rubros.
- b. Registro oportuno, de preferencia en tiempo real, de los costos de la entidad.
- c. Implementación de procesos orientados a garantizar el pago oportuno de las obligaciones a los diferentes acreedores de la entidad.
- d. Sistema que permita la radicación oportuna de las facturas, de preferencia en línea, por parte de los proveedores de cada entidad y la trazabilidad de estas.

### 35. GESTIÓN DEL RIESGO DE MERCADO DE CAPITALES

El Riesgo de Mercado de Capitales corresponde a la posibilidad de incurrir en pérdidas derivadas de un incremento no esperado, de sus obligaciones con acreedores tanto internos como externos, o la pérdida en el valor de sus activos, por causa de las variaciones en los parámetros del mercado tales como la tasa de interés, la tasa de cambio o cualquier otra variable de referencia que afecte los precios del mercado financiero y asimismo los estados financieros de la entidad.

El presente subsistema es desarrollado a fondo en el **manual del Subsistema de Administración de Riesgo de Mercados Capitales (SARM)**.

La adopción del Subsistema de Administración de Riesgo de Mercado de Capitales debe cumplir como mínimo con lo siguiente:

#### 35.1. CICLO DE GESTIÓN DE RIESGOS DE MERCADO CAPITAL

##### 35.1.1. IDENTIFICACIÓN DEL RIESGO DE MERCADOS CAPITALES

Para identificar el riesgo se considera:

- i) Se consideran las tasas de interés, el precio de las acciones, el precio de bienes inmuebles y la tasa de cambio.
- ii) Los activos expuestos a la volatilidad de estas variables, como:
  - a) Respecto a los activos expuestos a la tasa de interés (instrumentos de renta fija principalmente) considerar al menos los siguientes: bonos ordinarios, bonos subordinados, bonos opcionalmente convertibles en acciones, bonos obligatoriamente convertibles en acciones, Certificados de Depósito a Término (CDT), Títulos de Deuda Pública (TES), bonos de capitalización, y demás inversiones que estén expuestos a este factor de riesgo, ya sea que estén inscritos o no en la Bolsa de Valores de Colombia (BVC).
  - b) Al considerar los activos expuestos al precio de las acciones (instrumentos de renta variable) por lo menos tener en cuenta acciones ordinarias, acciones preferenciales y demás inversiones que estén expuestos a este factor de riesgo, que estén inscritos en la BVC.
  - c) Entre los activos no monetarios que estarían expuestos a la variabilidad en el precio de los bienes inmuebles, contemplar los terrenos, así como las construcciones y edificaciones de la entidad.
  - d) Por último, considerar los activos y pasivos denominados en moneda extranjera a efectos de abordar la volatilidad de la tasa de cambio.

### 35.1.2. EVALUACIÓN Y MEDICIÓN DEL RIESGO DE MERCADO DE CAPITALES

- a) Se detalla la correspondiente valoración de los activos y pasivos (el precio o valor de mercado) expuestos a los factores de riesgos identificados por la entidad y mencionados en el numeral anterior como mínimo, aplicando de manera adecuada las mediciones, reconocimiento, presentación y revelación en aplicación del respectivo marco técnico normativo de información financiera y contable.
- b) Escoger y aplicar una metodología para valorar la exposición de cada factor ante el riesgo de mercado de capitales, analizando de manera independiente las variaciones en la tasa de interés, tasa de cambio, precio de las acciones y precio de bienes inmuebles, como mínimo.
- c) La entidad debe escoger la metodología que considere más apropiada para la medición, en función de la información disponible, el personal encargado de la estimación y las políticas establecidas por la entidad en la gestión de este riesgo. Para ello, se recomienda analizar la información histórica de las variables que generan exposición al riesgo de mercado de capitales para un periodo de observación efectivo de por lo menos un (1) año.
- d) Calcular el capital expuesto que guarde correspondencia con los niveles de riesgo asumidos por cada entidad de acuerdo con las posibles pérdidas calculadas para cada uno de los factores de riesgo del mercado de capitales (tasa de interés, tasa de cambio, precio de las acciones y precio de bienes inmuebles, como mínimo).
- e) Agregar los resultados del capital expuesto de los diferentes factores de riesgo del mercado de capitales aplicando la correlación entre los mismos. De no disponer de información propia que le permita cuantificar esta correlación, podrá utilizar los coeficientes de correlación propuestos por la literatura internacional, las disposiciones de Basilea, lo normado por la Superintendencia Financiera de Colombia, entre otras.

### 35.1.3. TRATAMIENTO Y CONTROL DE RIESGO DE MERCADOS CAPITALES

- a) Se identifican los criterios utilizados para calcular los niveles de exposición al riesgo, los factores de riesgo, la periodicidad de evaluación y las fuentes de información. Debe haber correspondencia entre el modelo y las características particulares de la INSTITUCIÓN, teniendo en cuenta el grado de complejidad y el volumen de las operaciones expuestas a este riesgo. Dicho modelo debe estar en la capacidad de realizar mediciones que incorporen escenarios extremos (stress testing) en los diferentes factores de riesgo. Se usa como referencia el que se contempla en el Sistema de Administración de Riesgo de Mercado (SARM) de la Superintendencia Financiera de Colombia.
- b) Permitir el control de los niveles de exposición a los diferentes factores de riesgo de mercado de capitales y especificar los límites máximos de exposición permitidos por la INSTITUCIÓN y los planes de contingencia para los casos en los que se superen dichos límites. Ver matriz de riesgos.

## 36. GESTIÓN DE RIESGO DE GRUPO

El Riesgo de Grupo corresponde a la posibilidad de pérdida que surge como resultado de participaciones de capital o actividades u operaciones con entidades que forman parte del mismo grupo empresarial. Este se deriva de la exposición afuentes de riesgo adicionales a las propias del negocio de la entidad, dentro de las que se encuentran, por ejemplo: i) riesgo de contagio financiero, ii) detrimentos patrimoniales por filtración de flujos o concentración de pasivos y/o; iii) posibles conflictos de intereses, que generen condiciones desfavorables en las transacciones de la entidad. La exposición a las fuentes de riesgo puede ser directa, mediante exposición financiera u operativa, o indirecta, mediante daño a la reputación.

### 36.1. CICLO GENERAL DE GESTIÓN DEL RIESGO DE GRUPO

Para la gestión del riesgo de grupo inherente aplican todos los lineamientos generales presentados en esta Circular. Sin embargo, en atención a la anterior definición y para plantear las políticas específicas de gestión de este riesgo, el Subsistema de Administración de Riesgo de Grupo que implementen las entidades, debe contener los siguientes lineamientos específicos como mínimo:

### 36.1.1. IDENTIFICACIÓN DEL RIESGO DE GRUPO

Para la identificación de este riesgo la entidad debe determinar si ésta hace parte de un grupo empresarial e identificar todos los miembros de su grupo definido en los términos legales de los artículos 260 y 261 del código de comercio, la Ley 222 de 1995 y sus modificatorias. Asimismo, debe tener en cuenta lo establecido en el marco de las normas Internacionales de Información Financiera.

Adicionalmente, la entidad debe identificar las transacciones de índole financiera y administrativa que involucran de forma directa o indirecta con los miembros de su grupo empresarial o partes vinculadas, con el fin de poder evaluar el impacto y probabilidad de ocurrencia de estos.

### 36.1.2. EVALUACIÓN Y MEDICIÓN DEL RIESGO DE GRUPO

La entidad debe establecer mecanismos para la medición y evaluación del riesgo de grupo teniendo en cuenta que, por el hecho de pertenecer a un grupo puede estar expuesta, entre otros, a:

- Riesgo de contagio, donde resultados negativos en el ámbito financiero, calidad del servicio, entre otros, de los miembros del grupo empresarial y/o de las partes vinculadas impliquen algún estrés al interior de la entidad. Para tal fin, se debe tomar en consideración el seguimiento a las tendencias financieras del grupo y de los estados financieros separados que apliquen.
- Concentración del riesgo, donde un mismo tipo de riesgo se puede materializar en la entidad y otro miembro del grupo y/o parte vinculada al mismo tiempo. Esto teniendo en cuenta el nivel de concentración de transacciones y la participación de unos miembros en los otros.
- Posibles conflictos de intereses, especialmente en los procedimientos de compras y pagos de la entidad.
- Para la medición del impacto debe tenerse en cuenta los efectos sobre la fijación de precios, el flujo de Información, la calidad en la atención en salud, la gestión contractual, entre otros.

### 36.1.3. TRATAMIENTO Y CONTROL DEL RIESGO DE GRUPO

Teniendo en cuenta la probabilidad e impacto de las diferentes transacciones de la entidad con los miembros del grupo empresarial al cual pertenece sobre las pérdidas de la entidad, se recomiendan las siguientes medidas:

- Incluir políticas en la entidad asociadas a la gestión y auditorías de transacciones con los miembros del grupo empresarial al cual pertenece o sus partes vinculadas.
- Implementar mecanismos de resolución de conflictos de interés activados en virtud de la gestión del riesgo de grupo y realizar seguimiento.
- Velar por la inscripción del grupo empresarial, al cual pertenece, en el registro mercantil de acuerdo con lo establecido en el artículo 30 de la Ley 222 de 1995.

- Participar de forma activa revelando al Máximo Órgano Social del grupo empresarial al cual pertenece, la identificación, evaluación e impactos estimados por el riesgo de grupo, a efectos de que tanto el Marco de Referencia de la regulación de las relaciones institucionales entre las empresas del grupo, como las mejores prácticas con relación a proveedores aborden, de manera informada y documentada las necesidades de mitigación del riesgo de grupo de la entidad.

Adicional a las políticas individuales, se debe verificar que la entidad controlante asegure la existencia de políticas internas del grupo empresarial y mecanismos de control y gestión de riesgos adecuados conforme la estructura, negocios y perfil riesgos del grupo empresarial.

## 37. OTROS RIESGOS

### 37.1. RIESGO DE FALLAS DE MERCADO

El Riesgo de Fallas de Mercado corresponde a la posibilidad que la estructura del mercado de salud genere pérdidas en el bienestar y beneficios de la entidad.

Ejemplos: mercado monopólico u oligopólico; prácticas de competencia desleal (como lo son la selección de riesgo, barreras de acceso a los servicios, entre otros).

Ejemplo de riesgos de falla de mercado:

- a. Fallos de la competencia, presencia de monopolios y oligopolios, así como problemas de comportamiento de los agentes que impliquen, por ejemplo, colusiones orientadas a generar acuerdos de precios (proveedores o aseguradores).
- b. Asimetrías de información (información incompleta o imperfecta) que impidan hacer el seguimiento al cumplimiento contractual con los proveedores o impidan hacer gestión del riesgo individual de la población de su área de influencia.
- c. Existencia de integraciones verticales y horizontales, y grupos empresariales.
- d. Externalidades, generadas por personas o entidades que provocan impactos negativos afectando la eficiencia del mercado.
- e. Mercados incompletos.

La INSTITUCIÓN debe contar con una base de datos completa y oportuna de composición de la oferta y precios de los servicios, medicamentos y otros insumos que contrata con terceros, así como el análisis de la demanda.

Asimismo, debe contar con información que le permita calcular indicadores de gestión que le faciliten la comparación de mercados y evaluación del efecto de las fallas de mercado.

### 37.2. GESTIÓN DE RIESGO REPUTACIONAL

El Riesgo Reputacional corresponde a la posibilidad de toda acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de una entidad, tales como el impacto de la publicidad negativa sobre las prácticas comerciales, conducta o situación financiera de la entidad. Tal publicidad negativa, ya sea verdadera o no, puede disminuir la confianza pública en la entidad, dar lugar a litigios costosos, a una disminución de su base de usuarios, clientes, negocios o los ingresos, entre otros. Estos pueden ser desagregados, en situacional o previsto, de acuerdo con la capacidad de prevención-mitigación:

→ **Riesgo reputacional situacional:** Riesgo reputacional inmediato derivado de una acción imposible de anticipar.

➔ **Riesgo reputacional previsto:** Riesgo reputacional derivado de eventos a los cuales la organización puede anticiparse con una gestión adecuada de los riesgos en salud, financieros, y operativos, así como mediante estrategias de comunicación.

Para la identificación de este riesgo, la INSTITUCIÓN constituye un inventario de eventos que tengan posibles efectos sobre la reputación de esta. Para ello, se debe realizar la selección de los procesos, servicios y acciones que sean considerados estratégicos en formar reputación que sean cuantificables y que permitan la comparabilidad frente al sector. Estos se verán reflejados en la matriz de riesgos y se les hará su respectiva valoración y seguimiento.

Para control del nivel reputacional de la empresa se considerarán las **encuestas de satisfacción y el contenido en medios**.

Para correcto control de este riesgo, es necesaria la socialización del código de conducta y buen gobierno, la implementación de un protocolo de manejo de comunicaciones públicas y valoración de su posición reputacional a través de rankings o de rastreo de medios.

### 38. RESPONSABILIDADES POR SUBSISTEMA (INTEGRANTES DE COMITÉ DE RIESGO)

Los **integrantes del comité de riesgo**, encargado de velar por el efectivo, eficiente y oportuno cumplimiento de todas las fases del ciclo de gestión de los riesgos, responderán por la puesta en marcha de los planes y procedimientos asignados a cada subsistema. Para el cumplimiento de todos los requerimientos y recomendaciones presentes en las circulares externas **009 de 2016, 2021170000004-5 y 5-5 de 2021**, los líderes proveerán al proceso de Planeación estratégica de calidad y gestión del riesgo información en forma de indicadores, análisis, e incorporación de procedimientos con enfoque en riesgos en sus áreas.

A continuación, en Anexo 6, tabla de áreas responsables por subsistema y el proceso líder (encargado del cumplimiento de los lineamientos específicos por Subsistema impartidos por la Super Intendencia):

SUBSISTEMA	NORMA	PROCESO RESPONSABLE	LIDER (INTEGRANTE DE COMITE)
Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo / Proliferación de armas de Destrucción Masiva (SARLAFT / FPADM)	CE 009 de 2016, Modificada por Circular externa 2021170000005-5 de 2021	Planeación Estratégica Subgerencia corporativa <b>Oficial de Cumplimiento (líder)</b> Gestión Contractual Gestión del Talento Humano Planeación Estratégica de calidad y Gestión del Riesgo	Oficial de cumplimiento  Subgerente corporativo
Sistema de Administración de Riesgos de Corrupción, Opacidad y Fraude (SICOF)	Circular externa 2021170000005-5 de 2021	Planeación Estratégica Subgerencia corporativa <b>Oficial de Cumplimiento (líder)</b> Dirección de planeación Planeación Estratégica de calidad y Gestión del Riesgo	Asesor subgerencia corporativa

Sistema de Administración de Riesgo Operativo (SARO)	Circular externa de 2021 20211700000004-5	<b>Planeación Estratégica de calidad y Gestión del Riesgo (líder)</b> Subgerencia corporativa Subgerencia Científica Planeación financiera Líderes Procesos de apoyo	Líder de proceso de gestión de riesgo Coordinación de calidad Dirección de Talento Humano Dirección jurídica
Sistema de Administración de Riesgo de Liquidez (SARL)	Circular externa de 2021 20211700000004-5	Subgerencia corporativa <b>Dirección Financiera (líder)</b> Planeación Estratégica de calidad y Gestión del Riesgo	Director financiero
Sistema de Administración de Riesgo de Crédito (SARC)	Circular externa de 2021 20211700000004-5	Subgerencia corporativa <b>Dirección Financiera (líder)</b> Planeación Estratégica de calidad y Gestión del Riesgo	
Sistema de Administración de Riesgo de Mercados Capitaes (SARM)	Circular externa de 2021 20211700000004-5	Subgerencia corporativa <b>Dirección Financiera (líder)</b> Planeación Estratégica de calidad y Gestión del Riesgo	
Sistema de Administración de Riesgo de Salud (SARS)	Circular externa de 2021 20211700000004-5	<b>Subgerencia Científica / gestión del riesgo de salud (líder)</b> Planeación Estratégica de calidad y Gestión del Riesgo	Subgerente científico Dirección de seguridad del paciente
Sistema de Administración de Riesgo Actuarial	Circular externa de 2021 20211700000004-5	Planeación Estratégica de calidad y Gestión del Riesgo <b>Gestión Contractual (líder)</b>	Dirección de contratación
Sistema de Administración de Riesgo de Grupo	Circular externa de 2021 20211700000004-5	Planeación Estratégica de calidad y Gestión del Riesgo	Subgerente corporativo
Programa de Transparencia y Ética Empresarial /	CE 003 de 2018, modificada y expandida por Circular externa	Planeación Estratégica de calidad y Gestión del Riesgo	Director de planeación

Implementación Código de Conducta	de	<b>2021170000003-5</b> <b>2021</b>	de	<b>Dirección de Planeación</b> <b>(líder)</b>	
--------------------------------------	----	---------------------------------------	----	--	--

### 39. COMPROMISOS INSTITUCIONALES

Para garantizar el cumplimiento de las políticas y procedimientos aquí descritos, la ESE UNIVERSITARIA DEL ATLANTICO implementará las siguientes estrategias:

- Promover la cultura de autocontrol hacia una administración basada en riesgos.
- Formular, desplegar, implementar y evaluar un programa de gestión de riesgos que incluya las etapas descritas en la circular en la que se basa el presente manual
- Documentar y actualizar anualmente la matriz de riesgos para cada uno de los procesos asistenciales y administrativos, siendo ésta la herramienta conceptual y metodológica para la identificación, evaluación, tratamiento y seguimiento de los riesgos en la institución. La elaboración de la matriz de riesgos estará a cargo de los responsables de cada uno de los procesos con el acompañamiento del proceso de gestión del riesgo de la ESE UNIVERSITARIA DEL ATLANTICO.
- Formular un plan de trabajo para implementar los controles definidos en las matrices de riesgos, teniendo en cuenta que los responsables de los procesos serán los encargados de implementar los controles para cada uno de los riesgos, verificar su efectividad, proponer cambios y velar por su adecuada documentación, socialización y aplicación en su respectivo proceso.
- Monitorizar el impacto de los Sistemas de gestión de riesgos, mediante la variación en el riesgo residual.
- Fortalecer la supervisión a través del autocontrol, las auditorías internas y el aprovechamiento de los hallazgos de las auditorías externas, con el fin de consolidar el ambiente de control y la eficacia de la gestión de riesgos en la institución.

### 40. REPORTES Y FUENTES DE INFORMACIÓN

Tanto el código de conducta y de buen gobierno, como las políticas, el manual de procesos y procedimientos de la entidad, las bases de datos utilizadas para la modelación de los riesgos, y demás información, documentación y lineamientos que estén referenciados en esta Circular, deben estar a disposición de la Superintendencia Nacional de Salud, la cual, en virtud de sus funciones de IVC podrá requerir dicha información o información adicional en cualquier momento.

La información requerida para el IVC frente a la medición y exposición de riesgos prioritarios se obtendrá de la información reportada en la Circular Única y otras fuentes de información pública reportada.

- Ver circular externa **2021170000004-5 de 2021** para reportes obligatorios → FT018 Datos para cálculo de posición de liquidez.
- Ver circular externa **0003 de 2016** para reporte obligatorio → ARCHIVO TIPO GTOOI para Reporte de Implementación de Código de Conducta y Buen Gobierno.

### 41. CONTROL DEL CUMPLIMIENTO DEL MANUAL

De conformidad con lo establecido en la Ley 1438 de 2011 artículos 130 y 131, modificados por el artículo 2 de la Ley 1949 de 2019, la inobservancia e incumplimiento de las instrucciones impartidas en este manual (adaptado de la circular 20211700000045), dará lugar a la imposición de multas hasta de 8000 Salarios Mínimo Legales Mensuales Vigentes (SMLMV), así como a título personal hasta 2000 SMLMV a Representantes Legales, directores o secretarios de salud o quienes hagan sus veces, jefes de presupuesto, los revisores fiscales, tesoreros y demás funcionarios responsables de la administración y manejo de los recursos de la INSTITUCIÓN, o a la revocatoria del certificado de habilitación de las entidades vigiladas, si a

ello hubiere lugar, sin perjuicio de las acciones que le correspondan a otras autoridades competentes y demás facultades sancionatorias que esta Superintendencia tiene bajo el ámbito normativo.

#### 42. FICHA DE CONTROL DE CAMBIOS

FICHA DE CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
01	12/09/2024	Creación del documento.

#### 43. APROBACIÓN DEL DOCUMENTO

APROBACIÓN DEL DOCUMENTO		
ELABORO	REVISO	APROBÓ
<b>Nombre:</b> Armando Zabarain Lara	<b>Nombre:</b> Aura Cortizo Cabana	<b>Nombre:</b> Rafael Fernández De Castro Riascos
<b>Cargo:</b> Gestión de Riesgos en Salud	<b>Cargo:</b> Coordinador(a) de calidad	<b>Cargo:</b> Subgerente Corporativo
<b>Fecha:</b> 12/09/2024	<b>Fecha:</b> 21/10/2024	<b>Fecha:</b> 22/10/2024
<b>Firma:</b>	<b>Firma:</b>	<b>Firma:</b>