MANUAL INTEGRAL PARA LA GESTIÓN DEL RIESGO

Diagnóstico Cedimed

HOMOLOGADO PARA TODAS LAS COMPAÑÍAS DEL GRUPO EN COLOMBIA

Contenido

I LINEAMIENTOS GENERALES

1. Introducción

El gobierno nacional ha impulsado una serie de normas dirigidas al fortalecimiento técnico, operativo, financiero y administrativo de los agentes participantes del sistema general de salud, el cual comprende la implementación del Sistema de Gestión Integral de los riesgos en salud de las instituciones. Pues la institución se enfrenta a factores e influencias internas y externas que hacen incierto saber si y cuando conseguirá sus objetivos; la incidencia que esta incertidumbre tiene sobre la consecución de los objetivos constituye el "riesgo".

La institución, a través de todos sus colaboradores, debe gestionar el riesgo mediante la identificación, evaluación, medición y análisis del riesgo y el control y monitoreo eficaz como mínimo de los riesgos prioritarios los que está expuesto en desarrollo de sus operaciones. Lo anterior permitirá a la Administración establecer un tratamiento que satisfaga los criterios de riesgo, apoyada en una cultura de autocontrol y un adecuado Sistema

2. Objetivo

Establecer de forma integral los lineamientos generales para la gestión de riesgos en la institución, con el fin de asegurar el logro de los objetivos estratégicos tomando como referencia la norma ISO 31000 - Gestión de Riesgos y la normativa vigente.

3. Alcance

El presente manual aplica para todos los procesos, proyectos, planes y programas, de acuerdo con cada tipo y clasificación del riesgo. Inicia con la identificación, valoración, control y finaliza con el seguimiento y /o monitoreo de los planes de acción para mitigación de cada uno de los riesgos.

4. Definiciones

- **Alta Gerencia:** Personas del más alto nivel jerárquico en el área administrativa (denominados administradores) u organizacional de la entidad. La Junta Directiva la hace responsable del giro ordinario del negocio de la sociedad y la encarga de idear, ejecutar y controlar los objetivos y estrategias de la misma.
- **Análisis de impacto en el negocio:** Dentro de la gestión de la continuidad del negocio, es la tarea que identifica las funciones vitales del negocio y sus dependencias. Estas dependencias pueden incluir proveedores, personas, otros procesos de negocio, servicios TIC, etc.
- **Apetito de riesgo:** Es el nivel de riesgo que la empresa quiere aceptar y lo define la Junta Directiva.
- **Causa del riesgo:** Elemento que por sí solo o en combinación con otros, presenta el potencial intrínseco de ocasionar un riesgo.
- **Comité de Riesgos y/o sus equivalentes:** Encargado de liderar la implementación y desarrollar el monitoreo de la política y estrategia de la gestión de riesgos de la Institución.
- **Consecuencia:** Resultado de un suceso que afecta a los objetivos.
- **Control:** 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.

- **Criterios de riesgo:** Términos de referencia respecto a los que se evalúa la importancia de un riesgo.
- **Líder del proceso:** Persona que tiene la responsabilidad y autoridad para gestionar un riesgo.
- **Efecto:** Es una desviación, positiva y/o negativa, respecto a lo previsto.
- **Equipo funcional:** Colaboradores integrantes del proceso.
- **Evaluación del riesgo:** Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.
- **Evento:** Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.
- **Evento de interrupción:** Un evento que impacta la capacidad de una organización para continuar sus operaciones.
- **Factores de Riesgos:** 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.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.
- **Incertidumbre:** Es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.
- **Mapa de riesgos:** Representación gráfica donde se sitúan cada uno de los riesgos más representativos de la Institución.
- **Nivel de riesgo:** Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad.
- **Objetivos:** Pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como, nivel estratégico, nivel de un proyecto, de un producto y de un proceso).
- **Perfil de riesgo:** Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.
- **Plan de contingencia:** Es un plan de respuesta de emergencia. Son las operaciones de backup y recuperación post-desastre gestionada por una organización como parte de su programa de seguridad que garantice la disponibilidad de recursos críticos y facilitar la continuidad de las operaciones en una situación de emergencia.
- **Plan de continuidad del negocio:** Recopilación documentada de los procedimientos y la información que se preparan para su uso en caso de incidente grave, con el objetivo de poder continuar prestando sus servicios críticos en un nivel aceptable predefinido.
- **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. De esta manera se pueden identificar y ajustar los supuestos, parámetros y demás elementos que hacen parte del modelo de cálculo.
- **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. Busca identificar fortalezas y vulnerabilidades de los Subsistemas de Administración de Riesgos de manera individual para cada riesgo, y así cada entidad pueda comprender mejor sus propios perfiles de riesgo y validar los límites establecidos.

- **Probabilidad:** Posibilidad de que algún hecho se produzca.
- **Proceso de gestión del riesgo:** Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.
- **Riesgo:** Efecto de la incertidumbre sobre la consecución de los objetivos.
- **Riesgo inherente:** Cualquier nivel de riesgo propio de la actividad, cuya evaluación se efectúa sin considerar el efecto de los mecanismos de mitigación y de control.
- **Riesgo residual**: Es el nivel de riesgo que resulta luego de la aplicación de las medidas de control o mitigación existentes a los riesgos inherentes.
- **Suceso:** Ocurrencia o cambio de un conjunto particular de circunstancias.
- **Tratamiento del riesgo:** Proceso destinado a modificar el riesgo.
- **Valoración del riesgo:** Proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo.

5. Normatividad Vigente

- **Circular Externa 09 de 2016:** Por la cual se imparten instrucciones relativas al sistema de administración del riesgo de lavado de activos y la financiación del terrorismo (SARLAFT)
- **Circular Externa número 000003 de 24 mayo 2018:** Instrucciones generales para la implementación de mejores prácticas organizacionales - código de conducta y de buen gobierno IPS del grupo C1 y C2.
- **ISO 31000 de 2018:** Gestión de Riesgos de las Organizaciones.
- **Circular Externa 20211700000005-5 de 2021:** Subsistema de administración del riesgo de corrupción, opacidad y fraude (SICOF)
- **Circular Externa 20211700000004-5 de 2021:** Código de Conducta y de Buen Gobierno Organizacional, y sistema integrado de gestión de riesgos y sus subsistemas de administración de riesgos.
- **Circular Externa 2022151000000053-5 de 2022 05-08-2022:** Lineamientos respecto al programa de transparencia y ética empresarial, modificaciones a las circulares externas 007 de 2017 y 003 de 2018 en lo relativo a la implementación de mejores prácticas organizacionales – código de conducta y de buen gobierno.

6. Principios

Para que la gestión del riesgo sea eficaz, la Institución cumplirá en todos sus niveles los siguientes principios cuyo propósito es la creación y protección de valor.

- **Es Integrada:** La gestión del riesgo es parte integral de todas las actividades de la Institución.
- **Es Estructurada y exhaustiva:** Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.
- **Se Adapta:** El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.

- **Es Inclusiva:** La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
- **Es Dinámica:** Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
- **Se basa en la mejor información disponible:** Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras.
  La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
- **Toma factores humanos y culturales:** El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
- **Mejora continua:** La gestión del riesgo mejora continuamente con el aprendizaje y experiencia.

7. Clasificación de los riesgos

La Administración de la Institución debe gestionar los riesgos que se presenten dentro de su operación, para ello, diseñará políticas y procedimientos para cada uno de ellos basadas en la normativa vigente y en las mejores prácticas.

La clasificación de los riesgos son los siguientes:

- **Riesgos en Salud.**

Es el efecto 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.

- **Riesgos Operacional.**

Corresponde al efecto que una entidad 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.

- **Riesgo Actuarial.**

Es el efecto que se puede generar por no estimar adecuadamente el valor de los contratos según los diferentes tipos de contratos relacionados con la venta de servicios, de tal manera que estos resulten insuficientes para cubrir las obligaciones futuras que se acordaron.

- **Riesgo de crédito.**

Corresponde al efecto que se puede generar como consecuencia del incumplimiento de las obligaciones por parte de sus deudores en los términos acordados (monto, plazo y demás condiciones).

- **Riesgo de liquidez.**

Es el efecto que se puede generar por no contar 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).

- **Riesgo de Mercado de Capitales.**

Es el efecto que se puede generar por un incremento no esperado, de las obligaciones con acreedores tanto internos como externos, o la pérdida en el valor de los 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 Institución.

- **Riesgo de Grupo.**

Es el efecto que se puede generar 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 a fuentes 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.

- **Riesgo de Fallas de Mercado.**

Es el efecto que se puede generar por la composición de la estructura del mercado de salud: Mercado monopólico u oligopólico; prácticas de competencia desleal (como lo son la selección de riesgo, barreras de acceso a los servicios, entre otros).

- **Riesgo Reputacional.**

Es el efecto que se puede generar por toda acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de la Institución.

- **Riesgo de lavado de activos y financiación del terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM).**

Es el efecto que la Institución puede tener al ser utilizada por organizaciones criminales como instrumento para ocultar, manejar, invertir o aprovechar dineros, recursos y cualquier otro tipo de bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos de recursos vinculados con las mismas. También se incluye en este riesgo el Riesgo de contagio que es el efecto que la Institución puede tener, directa o indirectamente, por una acción o experiencia de un vinculado. El vinculado es el relacionado o asociado e incluye personas naturales o jurídicas que tienen posibilidad de ejercer influencia sobre la entidad.

- **Riesgos de Corrupción, Opacidad, Fraude y Soborno (COFS).**

Es el efecto que se puede generar por cualquier acto intencional o deliberado de privar los recursos o activos de la Institución o cualquier actuación, que, sin privar los recursos o activos de la Institución, sea utilizada para beneficios personales.

- **Riesgos de Protección de datos personales.**

Es el efecto que se puede generar por no proteger la información privada y confidencial de las personas naturales con las que interactúa la Institución.

8. Ciclo General de Gestión de Riesgos

Estructura, roles y responsabilidades

Estructura: La institución adopta el siguiente esquema de "3 líneas de defensa" para estructurar funciones y responsabilidades dentro de la empresa.

Primera Línea de Defensa: Responsables de cada proceso.

Dentro de sus funciones están la de gestionar los riesgos e implementar acciones correctivas para abordar el proceso y las deficiencias de control, para ello, deben identificar, evaluar, controlar y mitigar los riesgos, orientan el desarrollo e implementación de políticas y procedimientos internos y aseguran que las actividades sean compatibles con las metas y objetivos de la Institución. Igualmente, realizan el registro de eventos de riesgo presentados en la organización y establecen los planes de acción.

Segunda Línea de Defensa: Responsable: Administrador de Riesgos
Las funciones específicas de la segunda línea de defensa son:

- Diseña el manual de gestión del riesgo y da soporte a la primera línea de defensa para la implementación de las políticas.
- Monitorea el diseño y ejecución de los controles de manera priorizada.
- Da seguimiento a la base de eventos de riesgos y a la implementación de los planes de acción establecidos por la primera línea de defensa.

Tercera Línea de Defensa: Responsable: Auditoría Interna o quien haga sus veces.
A través de las pruebas de auditoría se proporcionará el aseguramiento sobre la eficacia del sistema de control interno, gestión de riesgos y de los procesos a la alta dirección de la organización, incluida las maneras en que funciona la primera y segunda línea de defensa.

Dependiendo de la estructura de la compañía, la segunda y tercera línea de defensa se podrá integrar en una sola velando por la independencia y objetividad.

9. Proceso de gestión del riesgo.

El proceso de gestión del riesgo es una parte integrante de la gestión de la Administración y se integra en la cultura y en las prácticas de la Institución adaptándose a los procesos de negocio de la organización y comprende las siguientes actividades *(tomado de la norma ISO 31000 – Gestión del riesgo).*

9.1 Comunicación y Consulta

En esta etapa se asiste a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo. La consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.

La comunicación y consulta se realizará en todas y cada una de las etapas del proceso de la gestión del riesgo.

9.2 Alcance, contexto y criterios

El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo.

9.2.1 Alcance

Al interior de la Institución, la gestión del riesgo se aplica a niveles estratégicos, operacionales (procesos), de proyectos u otras actividades que puedan surgir, tomando como consideración entre otros aspectos los objetivos y las decisiones que se necesitan tomar, así como los resultados esperados de las etapas a ejecutar en el proceso.

9.2.2 Contexto Externo e Interno

Los contextos externo e interno son el entorno en el cual la organización busca definir y lograr sus objetivos.

En el contexto externo se incluye entre otros aspectos sin limitarse a ellos:

- Entorno social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo.
- Factores y las tendencias claves que tengan impacto en los objetivos de la organización.
- Relaciones con las partes interesadas externas, sus percepciones y sus valores.

En el contexto interno constituye todo aquello al interior de la Institución que puede influir en la manera en la que la organización gestiona el riesgo. Incluye entre otros aspectos sin limitarse a ellos:

- El gobierno, la estructura, las funciones y las responsabilidades.
- Las políticas, los objetivos y las estrategias que se establecen para conseguirlo.
- Las aptitudes, entendidas en términos de recursos y conocimientos (capital, tiempo, personas, procesos, sistemas y tecnologías).
- La cultura de la organización.
- Los sistemas de información, los flujos de información y los procesos de toma de decisiones (tanto formales como informales).

9.2.3 Criterios del riesgo

Los criterios del riesgo reflejan los valores, objetivos y recursos de la organización y son coherentes con las políticas y declaraciones acerca de la gestión del riesgo. En el documento "**Anexo A – Definiciones de criterios de riesgo"** se encuentra el nivel de detalle de los criterios tanto del impacto como de la probabilidad.

9.2.4 Apetito / Tolerancia del Riesgo

El apetito/tolerancia al riesgo estará alineado con los límites de la matriz de impacto x probabilidad y por las directrices de Casa Matriz. La organización tratará que el apetito/tolerancia sea categoría "BAJO" en sus riesgos residuales, sin embargo, por el modelo de negocio puede estar en otra calificación superior.

9.3 Evaluación del Riesgo:

La evaluación del riesgo es el proceso global de identificación del riesgo, análisis del riesgo y valoración del riesgo. Se lleva a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas y utiliza la mejor información disponible, complementada por investigación adicional, si fuese necesario.

9.3.1 Identificación

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a la Institución lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

Para la identificación se deben tener en cuenta los siguientes factores, sin limitarse a ellos así estén o no bajo su control

- Las fuentes de riesgo tangibles e intangibles
- Las causas y los eventos
- Las amenazas y las oportunidades.
- Las vulnerabilidades y las capacidades.
- los cambios en los contextos externo e interno.
- los indicadores de riesgos emergentes.
- las consecuencias y sus impactos en los objetivos.
- las limitaciones de conocimiento y la confiabilidad de la información;
- los sesgos, los supuestos y las creencias de las personas involucradas.

Ver "Anexo A – Definiciones de criterios de riesgo"

La técnica a utilizar será la lluvia de ideas, pero se podrá seleccionar cualquiera de las técnicas de la ISO 31010.

9.3.2 Análisis del riesgo: Evaluación y Medición

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. La Institución efectuará este análisis de riesgo tanto para el riesgo inherente (calificación del riesgo antes de controles) como para el riesgo residual (calificación del riesgo después de que se ha implementado los controles y se encuentran en funcionamiento). **Ver "Anexo A – Definiciones de criterios de riesgo"**

Realiza el análisis de los riesgos de forma inherente como residual, permite determinar la madurez de los controles al interior de la organización.

9.3.2.1 Metodología de calificación de los riesgos

Tanto el riesgo inherente como el riesgo residual se calificarán bajo la metodología "IMPACTO y PROBABILIDAD" los lineamientos para cada calificación estarán descritos en el documento **"Anexo A – Definiciones de criterios de riesgo"**

Impacto	Probabilidad
Severo	Casi Seguro
Alto	Probable
Medio	Posible
Bajo	Raro/Remoto

9.3.2.2 Severidad de los riesgos

Las siguientes son las calificaciones de los niveles de severidad establecidos en la Institución y las acciones que se deben seguir para cada uno de ellos:

Extremo
Alto
Moderado
Bajo

9.3.2.3 Mapa de riesgos

El mapa de riesgo se construye ubicando en la matriz 4x4 las calificaciones de la probabilidad y del impacto. El mapa de riesgo para la Institución es el siguiente:

4 - Severo	4	8	12	16
3 – Alto	3	6	9	12
2 – Medio	2	4	6	8
1 - Bajo	1	2	3	4
IMPACTO / PROBABILIDAD	1 – Raro/remoto (0-10 %)	2 – Posible (11-50 %)	3 – Probable (50 - 90%)	4 – Casi seguro (>90%)

Para los riesgos en salud se podrá trabajar bajo la metodología AMEF/AMFE

Los Riesgos se registrarán en el aplicativo institucional definido. **Ver Anexo B - Instructivo de Registro de Riesgos.**

9.3.2.4 Calificación del Riesgo Inherente

Es aquel que puede existir de manera intrínseca en toda actividad. No tiene en cuenta el efecto de los controles.

Las calificaciones las asignará el líder del proceso de acuerdo con el nivel de criticidad de las variables, las cuales se encuentran definidas en el documento **"Anexo A – Definiciones de criterios de riesgo".** Los riesgos no se promedian: La calificación estará determinada por la mayor exposición del riesgo en cualquiera de los factores.

9.3.2.5 Calificación del Riesgo Residual

Es el riesgo que resulta tras la aplicación de los oportunos controles que hayan sido considerados por la organización.

La calificación del riesgo residual estará a cargo de cada líder de proceso, después de haber calificado los riesgos inherentes y aplicar los controles. La calificación del riesgo residual está basada en un juicio cualitativo teniendo en cuenta el diseño y la ejecución de los controles.

Los controles para que sean eficaces deben tener las siguientes características tanto en diseño como ejecución:

9.3.2.6 Diseño del Control

Responsabilidad del control: Estar asignados a un responsable con una adecuada segregación de funciones.
Tipo de Control: Se refiere a si el control es manual o automático. Se considera más fuerte el control cuando es automático.
Naturaleza del control: Preventivo o Detectivo. Se considera más fuerte el control cuando es Preventivo.
Frecuencia del control: Cada cuanto se ejecuta el control. Se considera más fuerte el control si la periodicidad de ejecución es la más apropiada para prevenir el riesgo.
Documentación: Se considera más fuerte el control cuando el mismo se encuentra documentado en una política, procedimiento, etc. en la plataforma habilitada para ello.

Los riegos residuales administrativos calificados en "EXTREMO" y "ALTO" serán monitoreados por la Auditoría Interna o quien haga sus veces y presentados en el Comité de Riesgos y/o su equivalente mínimo cada 6 meses. Para los riesgos asistenciales calificados en esta categoría serán monitoreados por la Dirección de Calidad o quien haga sus veces.

9.3.2.7 Ejecución del Control

Un control puede estar adecuadamente diseñado, pero sino se ejecuta por parte de los responsables el riesgo tiene más probabilidad de materializarse. La evaluación del riesgo residual será calificada de forma cualitativa basado en los argumentos anteriores.

Las siguientes serán las calificaciones de la ejecución del control:

Alto: El control está diseñado y funciona eficazmente según lo previsto y puede ser probado y evidenciado.
Medio: El control existe y está implementado, pero hay deficiencias en su diseño y/o eficacia operativa.

Bajo: El control está establecido, pero es ineficaz, debido a un diseño inadecuado y/o a un funcionamiento incoherente que ha sido identificado o el control no está funcionando.

La evidencia de la ejecución del control estará a cargo del líder del proceso quién deberá demostrar el cumplimiento de estos por cualquiera de los mecanismos que considere adecuado.

Un control se considera no satisfactorio cuando no se cumplan todos o alguno de los elementos mencionados anteriormente, para ello, cada líder de proceso deberá tomar las acciones necesarias para garantizar el cumplimiento de estos elementos.

9.3.3 Valoración del Riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones.
La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecido para determinar las acciones a seguir. Al interior de la Institución las siguientes acciones se deberán realizar según la severidad del riesgo residual:

Resultado del Riesgo Residual	Acción a seguir
Extremo	Debe ser puesto en conocimiento de la Gerencia, la Junta Directiva y el Comité de Riesgos y/o su equivalente y ser objeto de tratamiento inmediato.
Alto	Exige la atención del Gerente, debe ser tratado y monitoreado. Debe ser informado a la Junta Directiva y Comité de Riesgos y/o su equivalente.
Moderado	Debe ser gestionado adecuadamente por los líderes de los procesos y ser objeto de monitoreo continuo. Debe informarse a la Gerencia.
Bajo	Debe continuar gestionándose con los controles actuales existentes en la organización.

Los líderes de los procesos implementarán los controles necesarios para que sus riesgos residuales sean BAJOS basados en la premisa costo/beneficio donde el control no puede ser más costoso que la materialización del riesgo. No obstante, los riesgos residuales pueden estar en un nivel de severidad mayor justificando los motivos de los mismos.

Los niveles de tolerancia de riesgos estarán determinados por la organización con base en sus indicadores de gestión (KPI) e indicadores de riesgo (KRI) establecidos en cada proceso.

9.4 Tratamiento del Riesgo

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo.
El tratamiento del riesgo implica un proceso iterativo de: Formular y seleccionar opciones para el tratamiento del riesgo; — planificar e implementar el tratamiento del riesgo; — evaluar la eficacia de ese tratamiento; — decidir si el riesgo residual es aceptable; — si no es aceptable, efectuar tratamiento adicional.

Las opciones de tratamiento de riesgo son los siguientes:

Tratamiento	Descripción
Evitar	Consiste en no realizar la actividad que genera el riesgo. Evitar supone salir de las actividades que generen riesgos, puede incluir acciones como: • Retirar la fuente de riesgo. • Prescindir de una unidad de negocio, línea de producto o segmento geográfico. • Decidir no emprender nuevas iniciativas/ actividades que podrían dar lugar a riesgos
Reducir	Implica llevar a cabo acciones para reducir la probabilidad o el impacto del riesgo o ambos conceptos a la vez.
Transferir	La probabilidad o el impacto del riesgo se reduce trasladando, o compartiendo el riesgo con una o varias de las partes. • Adquirir seguros contra pérdidas inesperadas y significativas. • Entrar en sociedad compartida (joint venture). • Establecer acuerdos con otras empresas. • Establecer contratos de servicio • Utilizar instrumentos de mercado de capital. • Tercerizar procesos de negocio.
Aceptar	Consiste en retener el riesgo para perseguir una oportunidad y establecer un plan apropiado de financiación del riesgo • Provisionar las posibles pérdidas. • Confiar en las compensaciones naturales existentes dentro de un portafolio. • Aceptar el riesgo si se adapta a la tolerancia al riesgo existente.

La selección de la opción más apropiada de tratamiento del riesgo implica obtener un análisis de los costos/beneficios.
El tratamiento de los riesgos estará a cargo de cada Líder de proceso y debe ser revisada por la Gerencia y en el comité que corresponde, para cumplir con los siguientes objetivos:

- Tener un mejor conocimiento de los controles establecidos y determinar si dichos controles mitigan los riesgos de su proceso.
- Validar que el costo de la implementación de los controles es menor que los beneficios recibidos.
- Adicionar o eliminar nuevos controles o cambiar el tratamiento.

Un plan de acción debe realizarse en los siguientes escenarios:
- Cuando el riesgo no tiene un control asociado.
- Cuando el control no es efectivo.
- Cuando se deba robustecer el control.

Los planes de tratamiento deben incluir por lo menos los siguientes aspectos:

- Las razones que justifican la selección del tratamiento, incluyendo los beneficios previstos.
- Las personas responsables de la aprobación del plan y de la implementación del plan.
- Las acciones propuestas.
- Las necesidades de recursos, incluyendo las contingencias.
- Las medidas del desempeño y las restricciones.
- Los requisitos en materia de información y de seguimiento.
- El calendario y la programación.

La aceptación del riesgo estará a cargo de la Gerencia y/o de la Junta Directiva según su nivel de criticidad y exposición para la organización.

Adicional a lo anterior, la institución cuenta con los siguientes controles:

➢ **Controles estratégicos**

La alta dirección realiza revisiones de alto nivel a los asuntos de alta criticidad para la organización, tales como:

- Seguimiento a los indicadores de calidad y salud.
- Seguimiento al cumplimiento de la estrategia corporativa.
- Revisión de los niveles de cumplimiento, avance de los indicadores y planes de acción en caso de incumplimiento.

➢ **Controles del recurso humano**

El proceso de Gestión Humana o quien haga sus veces debe garantizar la implementación de controles efectivos en los procesos de selección, vinculación y promoción del recurso humano, tales como:

- Adecuación de competencias, verificación de títulos de los profesionales y personal en salud.
- Monitoreo de la rotación interna y externa.
- Valoración del clima laboral

➢ **Auditoría de controles**

A través del Proceso de Calidad, Auditoría Interna o quien haga sus veces realiza la validación del funcionamiento de los controles implementados por los líderes de los procesos.

Monitoreo de las señales de alerta se encuentra detallado en un documento aparte. Ver **Anexo D- Metodología para el monitoreo de las señales de alertas tempranas.**

9.5 Seguimiento y Revisión (Monitoreo)

El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso.

La revisión de los riesgos se realiza por lo menos cada año y es realizada por el Administrador de los riesgos, los líderes de los procesos y los órganos de control.

Este manual se revisará anualmente por parte del administrador de riesgos o persona responsable para esta función. Cualquier modificación al mismo debe presentarse al Comité de Riesgos y/o su equivalente para su revisión y aprobación.

Lo anterior no exime a que si antes de esta periodicidad se identifica un riesgo el mismo debe ser analizado con lo indicado en la política.

Cada líder de proceso implementará indicadores de ejecución (KPI) que tienen como finalidad informar, controlar, evaluar y ayudar a tomar las decisiones y deberán estar alineados a la estrategia de la organización. Para cada indicador se deberá establecer los niveles “Meta” de cumplimiento, así como los niveles de “precaución” y “críticos”. Estos dos últimos niveles serán considerados como señales de alerta (KRI).

Los KPI hacen parte de los pilares estratégicos de la organización y soportan las iniciativas estratégicas. El seguimiento se efectúa mensualmente en las reuniones Gerenciales y se reportarán a Casa Matriz.

De llegarse a presentar desviaciones o que se incumplan los indicadores “Meta”, los líderes de los procesos se deben establecer planes de contingencia para intervenir y tratar los diferentes riesgos, teniendo en cuenta la variabilidad de los riesgos identificados, con el propósito de ajustar las desviaciones lo más pronto posible.

Cada líder será responsable y establecerá los plazos, periodicidad, reportes de avance y de evaluaciones periódicas sobre las estrategias seleccionadas.

Los incumplimientos a los límites serán presentados en el Comité de Riesgos y/o equivalente, donde se informará los planes de contingencia adoptados respecto de cada escenario extremo presentado.

El proceso de seguimiento y revisión abarcan todos los aspectos del proceso de gestión del riesgo, con la finalidad de:

- Asegurar que los controles son eficaces y eficientes tanto en su diseño como en su utilización.
- Obtener la información adicional para mejorar la valoración del riesgo.
- Analizar y sacar conclusiones de los sucesos (incluyendo los cuasi-accidentes), cambios, tendencias, éxitos y fallos.
- Detectar los cambios en el contexto interno y externo, incluidos los cambios en los criterios de riesgo y en el propio riesgo, que puedan requerir la revisión de los tratamientos de riesgo y de las prioridades.
- Identificar los riesgos emergentes.

9.6 Registro e Informe

La Alta Dirección de la Institución proporcionará comunicaciones específicas y orientadas que se dirigirán a las expectativas de comportamiento y las responsabilidades del personal, incluyendo una clara exposición de su filosofía y enfoque de gestión de riesgos, su delegación y autoridad.

9.6.1 Divulgación de la Información Interna

Como resultado del monitoreo y control de cada uno de los riesgos identificados y especialmente los prioritarios, la Institución elaborará reportes semestrales como mínimo, que permitan establecer el perfil de riesgo de éstas.

Asimismo, al cierre del ejercicio contable informará 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 ven expuestas las entidades 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 de la Institución.

Estos informes se presentan al Representante Legal, a la Junta Directiva y los líderes de los procesos involucrados, los cuales quedan plasmados en acta donde se socializan estos informes.

9.6.2 Divulgación de la Información Externa

El Representante Legal, en el informe de gestión anual incluirá en las notas a los estados financieros un apartado sobre la gestión adelantada en materia de administración de los diferentes subsistemas de gestión de riesgos el contendrá un resumen de su situación en materia de la administración de dichos riesgos con información cualitativa y cuantitativa.

En la información cualitativa se informará sobre los objetivos, estrategias y filosofía en la gestión de riesgos y los controles implementados en cada uno para mitigarlos, así como los cambios potenciales en los niveles de riesgo, cambios materiales en las estrategias y límites de exposición para cada uno de los Subsistemas de Administración de Riesgos.

En la información cuantitativa sobre la gestión integral de los riesgos se informará el resultado de las políticas y metodologías internas aplicadas prevaleciendo el carácter privilegiado, confidencial o reservado de la información.

10. Políticas para la gestión de riesgos

- **Riesgos en Salud**
  - ✓ Preservamos la salud y la vida entregando una atención humanizada y de excelencia.
  - ✓ La Institución se rige por el modelo de gestión del servicio farmacéutico contenida en las disposiciones legales y de mejores prácticas en la selección de proveedores para la compra de insumos y medicamentos.
  - ✓ La Institución podrá prestar sus servicios en cualquiera los diferentes mercados existentes basados en la normativa vigente.
  - ✓ Periódicamente se generan y revisan los reportes de gestión a la atención de pacientes, así como los reportes de peticiones, quejas, reclamos y solicitudes.

- **Riesgos Operacional**
  - ✓ Generamos confianza al trabajar bajo los más altos estándares de calidad y seguridad para lograr los mejores resultados.
  - ✓ Fortalecemos el talento humano mediante la capacitación, el desarrollo de las habilidades técnicas, el crecimiento emocional y espiritual para fomentar el compromiso, la creatividad y la participación de los colaboradores en el mejoramiento continuo y la excelencia organizacional.
  - ✓ Aseguramos una cultura de gestión integral y de mejoramiento continuo en los procesos, incorporando la filosofía corporativa a las actividades diarias, teniendo como referencia el marco normativo y operativo para el logro de la eficiencia organizacional.

Mantiene un plan para administrar y asegurar la continuidad del negocio en situaciones de emergencia o desastre. (Ver. **Manual plan de continuidad del negocio**).

- **Riesgo Actuarial**
  - ✓ Aseguramos los recursos necesarios y suficientes para garantizar la operación eficiente y eficaz de los procesos asistenciales y administrativos.
  - ✓ Cada tipo de contrato para la generación de ingresos será revisado para determinar su viabilidad y rentabilidad.
  - ✓ Se revisan las rentabilidades de los diferentes contratos de generación de ingresos para determinar el cumplimiento de las metas establecidas.

- **Riesgo de crédito**
  - ✓ La Administración debe asegurar en todo momento, que las atenciones de los pacientes cuenten con las autorizaciones por parte de las aseguradoras.
  - ✓ Cualquier inversión debe ser aprobada por la Alta Dirección.
  - ✓ Se analizan los cumplimientos de plazos, pagos, glosas, devoluciones y condiciones contractuales para determinar las acciones a seguir con las aseguradoras.
  - ✓ Para aquellos casos donde se requieran atención de pacientes con aseguradoras sin contrato, la administración deberá solicitar las garantías o anticipos respectivos para evitar la no recuperación de la cartera.
  - ✓ Se evalúa la morosidad de la cartera para la constitución de provisión.

- **Riesgo de Liquidez**
  - ✓ La Administración debe asegurar la calidad de la facturación y la oportunidad en la radicación de estas, con el fin de garantizar el pago oportuno de la cartera.
  - ✓ Se revisa de forma periódica el flujo de caja de la Institución.
  - ✓ Cuando se presenten necesidades de liquidez se apoyarán con recursos internos con las demás filiales.

- **Riesgo de Mercado de Capitales**
  - ✓ La Administración requerirá autorización de la Junta Directiva y de la Controlante para realizar operaciones o transacciones asociadas a cualquier tipo de tasas o cualquier variable de referencia.

- **Riesgo de Grupo**
  - ✓ La Administración requerirá autorización de la Junta Directiva y de la Controlante para realizar negociaciones.
  - ✓ Las transacciones realizadas entre empresas del mismo grupo empresarial serán objeto de revelación en las notas a los estados financieros.

- **Riesgo de Fallas de Mercado**
  - ✓ La Administración tratará de no realizar operaciones con entidades que conforman mercado monopólico u oligopólico.
  - ✓ La Institución no participará en prácticas de competencia desleal.

- **Riesgo Reputacional**
  - ✓ La Administración realizará seguimiento permanente a las NPS, PQRS, redes sociales y línea de transparencia para determinar comentarios negativos de la Institución y tomará acciones inmediatas para evitar un mayor impacto.

- **Riesgo de lavado de activos, financiación del terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM)**
  - ✓ Las políticas se encuentran definidas en el manual del SARLAFT/FPADM.

- **Riesgo de Corrupción, Opacidad, Fraude y Soborno (COFS)**
  - ✓ Las políticas se encuentran definidas en el Manual de SICOF.

- **Riesgos de Protección de datos personales**
  - ✓ Las políticas se encuentran definidas en el Manual de políticas de Protección de Datos Personales.

11. Procesos y procedimientos para la gestión de riesgos

La Institución establecerá los procesos y procedimientos para instrumentar la Política de Gestión de Riesgo, para ello, se tendrán en cuenta los siguientes subsistemas de gestión de riesgos. El sistema de riesgos de prevención de corrupción, opacidad, fraude y soborno estará en un documento separado y hace parte integral de este manual.

12. Documentación

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

Esta documentación contendrá como mínimo lo siguiente:

- ➢ Las políticas para la administración de cada uno de los riesgos.
- ➢ 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.
- ➢ 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.

- Los roles y responsabilidades de quienes participan en la gestión de los diversos riesgos identificados, especialmente los prioritarios.
- Las medidas necesarias para asegurar el cumplimiento de las políticas y objetivos de cada uno de los Subsistemas de Administración de Riesgos.
- Roles, responsabilidades y acciones de los órganos de control frente a cada uno de los Subsistemas de Administración de Riesgos.
- Las estrategias de capacitación y divulgación de cada uno de los Subsistemas de Administración de Riesgos.

Igualmente hacen parte de la documentación:

- Las actas del máximo órgano de administración o quien haga sus veces, donde conste la aprobación, ajustes o modificaciones a las políticas de los Subsistemas de Administración de Riesgos.
- Los instructivos o manuales que contengan los procesos y procedimientos a través de los cuales se llevan a la práctica las políticas aprobadas para cada uno de los Subsistemas de Administración de Riesgos.
- El Código de Conducta y Buen Gobierno.
- Los informes presentados por la Junta Directiva o quien haga sus veces, el Representante Legal y el Comité de Riesgos en caso de que aplique. Entre estos debe encontrarse un reporte sobre el cumplimiento de los límites y del nivel de exposición de los diferentes riesgos establecidos por la entidad, particularmente los prioritarios.
- Los informes presentados por los órganos de control, sobre el funcionamiento y resultados de la implementación de cada uno de los Subsistemas de Administración de Riesgos.
- Las actas de Junta Directiva en donde conste la presentación del informe del Comité de Riesgos y del Revisor Fiscal, en los casos que aplique.
- Las actas del Comité de Riesgos, del Comité de Contraloría Interna, y los reportes a la Junta Directiva y al Representante Legal, en los casos que aplique.
- Las constancias de las capacitaciones impartidas a todos los empleados, socios, directivos, administradores y cualquier otra persona que tenga vinculación con la entidad sobre el Sistema Integrado de Gestión de Riesgos, con el fin de asegurar que sean entendidas e implementadas en todos los niveles de la organización.
- Los documentos y registros que evidencien el funcionamiento oportuno, efectivo y eficiente de cada uno de los Subsistemas de Administración de Riesgos.
- Las metodologías, parámetros, fuentes de información y demás elementos utilizados para la medición de cada uno de los riesgos.
- El procedimiento a seguir en caso de incumplimiento a los límites preestablecidos en cada uno de los Subsistemas de Administración de Riesgos.
- Disponer de un respaldo físico o en medio magnético de la documentación mencionada en este numeral.
- Establecer requisitos de seguridad, de forma tal, que se permita la consulta a información sensible, únicamente por parte de funcionarios autorizados.
- Determinar criterios y procesos de manejo, guarda y conservación de la información.

Toda la información anteriormente mencionada se encuentra a disposición de la Super Intendencia Nacional de Salud.

13. Estructura Organizacional

13.1 Junta Directiva

- ✓ Identifica, mide y gestiona las diversas clases de riesgos (de salud, económicos, reputacionales, de lavado de activos, entre otros) y establecer las políticas asociadas a su mitigación.
- ✓ Aprueban la política de Gestión de Riesgos, sus modificaciones y actualizaciones.
- ✓ Aprueban el apetito de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo de la entidad.
- ✓ Garantizan los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente del sistema de Gestión de Riesgo.
- ✓ Revisan el desempeño de la gestión de riesgos.

13.2 Comité de Riesgos y/o su equivalente.

- ✓ Establece estrategias para prevenir y mitigar los riesgos en salud y operativos.
- ✓ Identifica, mide, caracteriza, supervisa y anticipa, mediante metodologías adecuadas, los diversos riesgos (de salud, económicos, operativos, de grupo, lavado de activos, reputacionales, entre otros) asumidos por la entidad, propios de su función en el SGSSS.
- ✓ Hace seguimiento y evalúa periódicamente el funcionamiento de los Comités internos de la institución relacionados con asuntos de salud.
- ✓ Vela por el cumplimiento y mejoramiento progresivo de los procesos y estándares relacionados con la seguridad del paciente.
- ✓ Supervisa los procesos de atención al paciente, velan por una atención humanizada, miden y evalúan indicadores de atención (seguimiento y análisis de quejas y reclamos, orientación al usuario, tiempos de espera, etc.).

13.3 Representante Legal

- ✓ Implementa la política aprobada por la Junta Directiva.
- ✓ Comunica la política y decisiones adoptadas por la Junta Directiva a todos y cada uno de los funcionarios dentro de la entidad, quienes en desarrollo de sus funciones y con la aplicación de procesos operativos apropiados deben procurar el cumplimiento de los objetivos trazados por la dirección, siempre sujetos a los lineamientos por ella establecidos.
- ✓ Implementa los diferentes informes, protocolos de comunicación, sistemas de información y demás determinaciones de la Junta Directiva relacionados con la gestión de riesgos.
- ✓ Fija los lineamientos tendientes a crear la cultura organizacional de control, mediante la definición y puesta en práctica de las políticas y los controles suficientes, de tal forma que el personal de todos los niveles comprenda la importancia del control interno e identifique su responsabilidad frente al mismo.
- ✓ Proporciona a los órganos de control internos y externos, toda la información que requieran para el desarrollo de su labor.
- ✓ Proporciona los recursos que se requieran para el adecuado funcionamiento de la gestión del riesgo, de conformidad con lo autorizado por la Junta Directiva.
- ✓ Apoya y garantiza el efectivo cumplimiento de las políticas definidas por la Junta Directiva.
- ✓ Adelanta un seguimiento permanente del cumplimiento de las funciones del Comité de Riesgos u Órgano equivalente, en los casos que aplique y mantiene informada a la Junta Directiva.

- ✓ Conoce y discute 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.
- ✓ Hace seguimiento y se pronuncia respecto a los informes periódicos que presente el Comité de Riesgos u Órgano equivalente 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.
- ✓ Realiza monitoreo y revisión de las funciones del control interno de la Institución.
- ✓ Vela 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.
- ✓ Vigila 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.
- ✓ Informa 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.

13.4 Administrador de Riesgos

- ✓ Define los instrumentos, metodologías y procedimientos tendientes a que la Institución administre efectivamente los riesgos.
- ✓ Desarrolla e implementa el sistema de reportes.
- ✓ Administra el registro de eventos de riesgo.
- ✓ Coordina la recolección de la información para alimentar el registro de eventos de riesgo operativo.
- ✓ Establece y monitorea el perfil de riesgo e informarlo al Comité de Riesgos.
- ✓ Desarrolla los programas de capacitación relacionados con la gestión del riesgo.
- ✓ Realiza seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.
- ✓ Apoya 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.
- ✓ Sugiere al Comité de Riesgos y/o quien haga sus veces, los ajustes o modificaciones necesarios a las políticas de los diferentes Subsistemas de Administración de Riesgos.
- ✓ Propone al Comité de Riesgos y/o quien haga sus veces, 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.
- ✓ 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.

- ✓ Realiza seguimiento o monitoreo a la eficiencia y la eficacia de las políticas, procedimientos y controles establecidos.
- ✓ Apoya 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.
- ✓ Monitorea 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.
- ✓ Vela por el adecuado archivo de los soportes documentales y demás información relativa al Sistema Integrado de Gestión de Riesgos de la institución.
- ✓ Participa 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.
- ✓ Analiza 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.
- ✓ Monitorea e informa al Comité de Riesgos y/o quien haga sus veces, 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.

13.5 Auditoría Interna o quien haga sus veces.

- ✓ Evaluar periódicamente la efectividad y cumplimiento de la gestión del riesgo con el fin de determinar las deficiencias y sus posibles soluciones.
- ✓ Informar los resultados de la evaluación de la Gestión de Riesgos al Comité de Riesgos, al Representante Legal y al Administrador de riesgos.
- ✓ Realizar una revisión periódica del registro de eventos de riesgo.

13.6 Líderes de Procesos.

- ✓ Conocen y cumplen las políticas y procedimientos correspondientes a la Gestión y Control del Riesgo.
- ✓ Identifican los riesgos de los procesos y gestionarlos bajo la metodología que se describe en la presente política.
- ✓ Facilitan toda la información que sea necesaria al Administrador de Riesgos y Auditoría Interna de manera que pueda brindar el apoyo necesario para realizar seguimiento a los distintos riesgos.
- ✓ Establecen las medidas preventivas y planes de acción más convenientes para tratar el riesgo y conseguir así el perfil de riesgo que la Institución se ha propuesto.
- ✓ Elaboración, seguimiento y control de implantación de las diferentes recomendaciones de mitigación del riesgo.

13.7 Demás colaboradores.

- ✓ Adherirse a los procesos y procedimientos adoptados en la Institución.
- ✓ Ejecutan las acciones de autocontrol, autorregulación y autogestión en cada una de las actividades que desarrollen, procurando el mejoramiento continuo en sus procesos.

- ✓ Ejecutan los controles establecidos para cada uno de los riesgos y reportar cualquier desviación o falla en éstos a su jefe inmediato.
- ✓ Reportan los eventos o riesgos materializados en los procesos, aún si no es el proceso al que pertenece.

14. Infraestructura tecnológica.

La Institución dispondrá y utilizará la infraestructura tecnológica y los sistemas necesarios para garantizar el funcionamiento efectivo, eficiente y oportuno del Sistema Integrado de Gestión de Riesgos para generar informes confiables.

Cuenta con una herramienta tecnológica acorde con sus actividades, operaciones, riesgos asociados y tamaño que le permita centralizar la información relacionada con la gestión de riesgos, el cual se valida por lo menos una vez al año. Además, se cuenta con la conservación, custodia y seguridad de la información tanto documental como electrónica.

15. Capacitaciones

La comunicación sobre procesos y procedimientos estará alineada con la cultura deseada, la cual se reforzará en todo momento. Para lograr lo anterior, la Institución contará con una estrategia de capacitación sobre el sistema de Gestión de Riesgos.

La estrategia de capacitación se basa en el plan para la comunicación y consulta de cada paso del proceso de gestión de riesgo. El mismo abarca tanto las partes interesadas internas como externas.

II LINEAMIENTOS ESPECIFICOS DE LOS SUBSISTEMAS DE ADMINISTRACIÓN DE RIESGOS

1.1 Gestión del riesgo en Salud

1.1.1 Objetivo

Prevenir la ocurrencia de un evento no deseado, evitable y negativo para la salud de sus usuarios o en el deterioro de una condición previa o la necesidad de requerir más consumo de bienes y servicios que hubieran podido evitarse; Mediante la implementación de controles, procedimientos para detectar fallas oportunamente para reducir el nivel de exposición al riesgo y fortalecer la cultura de seguridad.

1.1.2 Ciclo general de gestión del riesgo en salud

La Gestión del Riesgo y las Actividades de Control en la institución se basan en un modelo de tres líneas de defensa. Las funciones de las demás líneas de defensa pueden ser consultadas en el numeral 8.1 - Estructura, roles y responsabilidades.

La institución realiza la gestión del riesgo clínico-asistencial. Dicha gestión consiste en utilizar herramientas para la prevención y están dirigidas a monitorear, analizar y prevenir la ocurrencia de estos en las instituciones de servicios de salud.

1.1.2.1 Identificación de riesgos

La identificación de los riesgos en salud estará a cargo de los líderes de los procesos asistenciales. De acuerdo con la metodología descrita en el numeral 9.3.1 del presente manual.

a. **Identificación de la situación en salud del territorio donde se encuentran habilitados y de la población objeto**
Para la adecuada identificación de riesgos, se tendrán en cuenta los siguientes aspectos:

La institución cuenta con una Zona de influencia territorial, por lo cual define su población objetivo con base a la caracterización de las Entidades Administradoras de Planes de Beneficios de Salud (EAPB) y del Plan Territorial en salud, con las cuales tiene acuerdos contractuales, lo cual permite considerar necesidades específicas de la población y sirve como herramienta para la identificación de los riesgos que se encuentre en el contexto y que puedan afectar de manera directa o indirecta a la institución **(Ver Anexo C- Análisis de situación territorial)**

b. **Caracterización de los servicios ofertados:** La institución identifica los riesgos de salud en forma integral por proceso y según el servicio asistencial ofrecido a la comunidad. La Dirección Médica o a quien corresponda realiza el análisis de la capacidad instalada en cada uno de los servicios y determina el personal requerido para la atención oportuna y adecuada de los pacientes, que permita una gestión clínica optima en el marco de un enfoque diferencial.

c. **Caracterización de la demanda:** La institución basa la caracterización de la demanda definida desde el proceso de habilitación de los servicios y establece un protocolo diferencial para la atención de poblaciones vulnerables.

d. **Reporte institucional de incidentes, eventos adversos y complicaciones.** La institución cuenta con un sistema de reporte de eventos tanto asistenciales como administrativos, teniendo en cuenta que el reporte de los eventos no es un único medio confiable para conocer la verdadera magnitud del riesgo, la institución se apoyara en otras fuentes para realizar búsqueda activa de los eventos.

e. **Caracterización de los riesgos existentes en cada uno de los servicios:** Cada líder de proceso asistencial identifica los riesgos, causas, consecuencias y controles, para ello se tiene en cuenta lo establecido en el documento Institucional de Seguridad del Paciente. Los riesgos identificados quedaron registrados en la herramienta tecnológica de la institución.

1.1.2.2 Medición de riesgos

En esta etapa se miden los riesgos por la probabilidad de ocurrencia y su impacto en caso de materializarse, como se describe en el numeral 9.3.2. del presente Manual. La medición en términos económicos los realiza la alta dirección mediante el análisis financiero, con el apoyo de los procesos involucrados y para adoptar los planes de mejora a que haya lugar.

La institución establece el costo jurídico mediante el monitoreo de demandas legales por fallas o errores en los procesos asistenciales durante la prestación del servicio, al igual que el sobre costo generado durante la gestión de las glosas y devoluciones en caso de aplicar.

La institución establece una matriz de riesgo para los procesos de los servicios ofertados, prioriza e implementa controles para reducir el riesgo (**Ver herramienta tecnológica**). La tolerancia de los riesgos se establece en el numeral 9.3.3- “Valoración del riesgo” del presente Manual.

1.1.2.3 Tratamiento y Control del riesgo en salud

La institución toma las medidas para controlar los riesgos inherentes a que se ve expuesta con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que se materialicen. Cada líder de proceso define los planes de mitigación o control para los riesgos residuales catalogados en EXTREMO o ALTO.

Desde el programa de seguridad del paciente se realizan controles para la prevención del riesgo en salud mediante auditoría, paciente trazador, adherencia a guías de práctica clínica o protocolos, a metas internacionales de seguridad del paciente con indicadores que monitorean la ocurrencia de incidentes y eventos adversos y se generan acciones para disminuir o mitigar el riesgo.

Los controles estarán incluidos en las diferentes políticas, procedimientos, guías y demás documentos de la institución y son responsabilidad de los líderes de los procesos. Adicional a lo anterior, la institución cuenta con controles generales. Ver numeral **9.4 -Tratamiento del Riesgo.**

1.2 Gestión del riesgo Operacional

1.2.1 Objetivo General

Prevenir la ocurrencia de situaciones que generen 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, opacidad y soborno ya sea por causa interna o por la ocurrencia de acontecimientos externos, entre otros.

1.2.2 Ciclo general de gestión del riesgo operativo

La Gestión del Riesgo y las Actividades de Control de la Institución se basan en un modelo de tres líneas de defensa. Las funciones de las demás líneas de defensa pueden ser consultadas en el presente Manual (Ver numeral 8.1 - Estructura, roles y responsabilidades).

1.2.2.1 Identificación del riesgo.

La identificación de los riesgos operacionales estará a cargo de los líderes de los procesos (Consultar más detalle en el numeral 9.3.1).

Para la adecuada identificación de riesgos, se tendrán en cuenta los siguientes aspectos:

a. **Levantamiento y documentación de la totalidad de los procesos**: La institución cuenta con el área encargada de formalizar los documentos, mapeo y caracterización de los procesos, donde se indican los objetivos, las actividades realizadas las cuales se encuentran alineadas con la estrategia de la institución y se definen los indicadores de gestión.

b. **Identificación de los eventos de riesgo operacional, potenciales y ocurridos, en cada uno de los procesos:** Al momento de la identificación de los riesgos operacionales, los líderes de los procesos con base en su conocimiento y experiencia, así como con el apoyo de su equipo de trabajo determinará si el riesgo identificado ha ocurrido en algún momento en la institución o si corresponde a riesgos que no han ocurrido, pero que potencialmente podrían materializarse. Para un mejor control de este, se utiliza la herramienta tecnológica de gestión de riesgos.

c. **Identificación de procesos jurídicos en los que se encuentre la entidad:** La institución se encarga de identificar y administrar los diferentes procesos jurídicos que posea y generar las alertas cuando dichos procesos puedan afectar a la organización financiera y reputacionalmente.

d. **Identificación de pérdidas en los resultados en salud de sus pacientes, los cuales, por su relevancia son tratados como riesgos en salud.** La entidad cuenta con una herramienta para gestionar los eventos de riesgo presentados que le permitirá identificar posibles pérdidas en la atención de sus pacientes. Lo importante en la identificación de riesgos es el establecimiento de controles o planes de acción que permitan que a futuro el riesgo se materialice.

e. **Determinación de potenciales pérdidas financieras en la entidad causadas por los eventos de riesgo operacional identificados:** En la medida de lo posible se tratará de determinar las potenciales pérdidas financieras generadas por los eventos operativos, para ello, se contará por lo menos con el apoyo de la Alta Dirección.

Registro de eventos operativos:
Los eventos de riesgo son incidentes que ocurren en un lugar particular durante un periodo de tiempo determinado y que tienen consecuencias económicas, legales o reputacionales para la entidad.

Para la organización, el registro de eventos de riesgo debe ser lo más completa posible para ofrecer a la Alta Gerencia información útil para la toma de decisiones. Para administrarlos, la entidad cuenta con una herramienta tecnológica que permite a los colaboradores registrar dichos eventos y se puedan adelantar los planes de acción requeridos.

1.2.2.2 Medición y evaluación del riesgo operacional
En esta etapa se miden los riesgos por la probabilidad de ocurrencia y su impacto en caso de materializarse, como se describe en el numeral 9.3.2. del presente Manual.

1.2.2.3 Tratamiento y Control del riesgo Operacional
La institución toma las medidas para controlar los riesgos inherentes a que se ve expuesta, con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que se materialicen. Cada líder de proceso define los planes de mitigación o control para los riesgos residuales catalogados en EXTREMO o ALTO.

Adicional a lo anterior, la institución cuenta con controles generales. Ver numeral **9.4 -Tratamiento del Riesgo**

1.2.2.3.1 Plan de Continuidad de Negocio (BCP)
La organización tiene definido e implementado 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. La prueba de este plan puede realizarse a través de pruebas de escritorio.
El detalle del BCP está documentado en forma separada y hace parte integral de este manual. Ver **Manual del plan de continuidad del negocio.**

1.3 Gestión del riesgo Actuarial

1.3.1 Objetivo General

Prevenir pérdidas económicas debido a no estimar adecuadamente el valor de los contratos según los diferentes tipos de contratos establecidos por la Institución con las diferentes entidades aseguradoras.

1.3.2 Ciclo general de gestión del riesgo actuarial

La Gestión del Riesgo y las Actividades de Control de la Institución se basan en un modelo de tres líneas de defensa. Las funciones de las demás líneas de defensa pueden ser consultadas en el en el presente Manual (Ver numeral 8.1 - Estructura, roles y responsabilidades).

1.3.3 Identificación de riesgos

La identificación de los riesgos actuariales estará a cargo de la Alta Dirección.

a. Caracterización y conocimiento de la población:

El Líder Comercial se encargará de suministrar la información a la Alta Dirección de nuevos convenios, contratos o modalidades con las diferentes aseguradoras o entidades que requieran la prestación de servicios por parte de la Institución para determinar la viabilidad financiera de los mismos.

La Institución revisará el perfil epidemiológico, así como el conocimiento de la población para que se puedan revisar los contratos, convenios, guías clínicas, protocolos de atención, entre otros, y determinar si estos requieren ser modificados para garantizar la viabilidad financiera.

b. Particularidades de las diferentes modalidades de contratación:

La Dirección Financiera o quien haga sus veces, se encargará de estimar los costos de los servicios prestados para que de esta manera se puedan definir las diferentes modalidades de contratación que desee realizar la Institución.

c. Identificación de posibles incrementos en costos de insumos y medicamentos:

La Dirección Financiera o quien haga sus veces, se encargará de revisar los costos de los servicios prestados para que de esta manera determinar variaciones en los costos de insumos y medicamentos que puedan afectar la rentabilidad de la Institución.

d. Identificación de posibles incrementos en costos de insumos y medicamentos:

La Dirección Financiera o quien haga sus veces, se encargará de revisar la rentabilidad mediante el análisis de ingresos y costos de los servicios prestados para que de esta manera determinar ajustes en los contratos.

1.3.4 Evaluación y Medición del Riesgo Actuarial

Periódicamente, la Alta Dirección o quien haga sus veces revisan los márgenes operacionales para determinar fluctuaciones en los costos que puedan sobrepasar los valores pactados con las aseguradoras.

La Institución podrá, a necesidad, realizar la construcción de modelos de cuantificación (Back Testing y Stress Testing) que contemplen de manera adecuada, las pérdidas esperadas e

inesperadas, a las que se encuentra expuesta la entidad cuando se realicen otro tipo de convenios de pago diferentes a eventos y paquetes.

1.3.5 Tratamiento y Control del Riesgo Actuarial

La Institución tomará diferente medidas para controlar los riesgos actuariales que se puedan presentar. Dentro de los controles establecidos por la Institución se encuentran la revisión y seguimiento de los resultados operacionales.

Alertas tempranas:

Disminución de márgenes operacionales: La Alta Dirección de la Institución revisará periódicamente los resultados de las operaciones para determinar variaciones o fluctuaciones significativas en el margen bruto.

Variaciones de los perfiles epidemiológicos: Se revisará periódicamente cambios significativos en los perfiles epidemiológicos de la institución para que se pueda determinar los impactos en los esquemas actuales de contratación.

Planes de acción:

Dependiendo de las circunstancias, la Administración de la Institución puede tomar diferentes acciones para evitar un mayor impacto del riesgo actuarial:

- Acuerdos con aseguradoras para actualización de precios.
- Revisión de Guías Clínicas, protocolos de atención para optimizar recursos tanto operativos como financieros para que disminuyan los impactos generados.
- Acuerdos con proveedores de insumos y medicamentos.
- Redistribución de la composición de ingresos mercado público y privado.

1.4 Gestión del riesgo de Crédito

1.4.1 Objetivo General

Prevenir la ocurrencia del riesgo de crédito mediante la evaluación permanentemente del riesgo inherente de que los activos de la institución pierdan valor, como consecuencia de que un deudor o contraparte incumpla sus obligaciones en los términos acordados. Dentro de la evaluación se incorpora los cambios significativos de las condiciones de cumplimiento de sus deudores.

1.4.2 Ciclo general de gestión del riesgo de crédito

La Gestión del Riesgo y las Actividades de Control de la institución se basan en un modelo de las líneas de defensa definidas en este manual atendiendo su estructura, roles y responsabilidades.
Para la gestión del riesgo de crédito, se tendrán en cuenta los siguientes lineamientos y aspectos específicos como mínimo:

1.5 Una evaluación de riesgo por contraparte incluyendo los instrumentos financieros, tratándose de inversiones de renta fija si se tienen.
1.6 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 institución por el incumplimiento de las contrapartes y que se ajuste a la normatividad vigente.
1.7 Seguimiento a gestiones de recaudo y/o cobranza de las deudas y a mecanismos de negociación y recuperación de deudas.
1.8 Una estrategia de gestión de glosas y devoluciones en función del análisis histórico para determinar procesos específicos de actuación.
1.9 La verificación de los literales anteriores se debe realizar al menos una vez al año, para evaluar su funcionamiento y monitorear efectivamente la exposición a este riesgo.

1.4.3 Identificación de riesgos

La identificación de los riesgos de Crédito estará a cargo de la Alta Dirección o a quien designe, a través de todas las áreas que la conforman, entre las que se destacan: Facturación - Cartera

Los aspectos mínimos que se tendrán en cuenta para la identificación de los riesgos de crédito serán las cuentas por cobrar y los instrumentos financieros si aplica.

Dentro de los instrumentos financieros se tendrán en cuenta:

- Cuentas de Bancos y Fondos de Inversión
- Instrumentos inscritos en el Mercado de Valores de Colombia
- Inversiones en títulos o valores de renta fija emitidos por entidades nacionales o extranjeras.

1.4.3.1 Evaluación y Medición del Riesgo de Crédito

La Institución evaluará las pérdidas estimadas como resultado del incumplimiento de sus contrapartes, para ello, diseñará un modelo un modelo contemplando los siguientes aspectos para la estimación:

- La probabilidad de incumplimiento de los deudores dentro de un periodo de tiempo de mínimo de 12 meses.
- Categorización de cartera: A manera de ejemplo sin limitarse a ellas: ARL, Aseguradoras, SOAT, Medicina Prepagada, Entes Territoriales, EPS, Clientes particulares, etc.
- La estimación de la pérdida esperada dado el incumplimiento, para ello, se considerará el valor expuesto del activo (saldo de la obligación o valor neto del activo) en el momento del Incumplimiento y la tasa de recuperación del valor del activo una vez materializado el incumplimiento, la cual debe contemplar las recuperaciones efectivas que se han realizado sobre estos incumplimientos en los últimos 3 años.

Para estimar la probabilidad de no cumplimiento por parte de los deudores se tendrán en cuenta los siguientes aspectos:

- Análisis de información histórica de las cuentas por cobrar de cada deudor según los acuerdos firmados.
- La calidad del deudor y el plazo de la cartera
- Análisis segmentado por líneas de negocio.
- Estimación de las posibles pérdidas que resulten de incumplimientos de pago frente a prestaciones realizadas u obligaciones generadas

Para otros instrumentos financieros diferentes de cartera, la institución se basará en la calificación de crédito por agencias calificadoras.

1.4.2.1 Tratamiento y Control del Riesgo de Crédito

La Administración de la institución tomará diferente medidas para controlar los riesgos de Crédito para ello se tendrán en cuenta los siguientes parámetros sin limitarse a ellos:

Límites de exposición crediticia y de pérdida tolerada:
Para la institución los límites de exposición crediticia y pérdida tolerada estarán definidos en el recaudo de la cartera con las entidades y tomará las acciones a que haya lugar cuando dicho recaudo no se esté dando en la periodicidad establecida. Este control estará a cargo del proceso financiero y se evaluará con la Gerencia o su delegado de manera mensual en la revisión de informes financieros.

Para los demás instrumentos financieros (inversiones) se hará seguimiento por parte de la Dirección Financiera o quien haga sus veces el comportamiento de los mercados.

Deterioro de los activos:
La institución cuenta con políticas y procedimientos de cartera donde, entre otros aspectos, se definen las medidas para una gestión de cobro eficiente de la cartera y se implementan las estrategias de recaudo. En este documento se dan los lineamientos para la estimación del deterioro de cartera.

Capital Expuesto al Riesgo:
El Capital Expuesto de Riesgos en la institución estará definida en recuperación de la cartera con las entidades y tomará las acciones a que haya lugar cuando dicha recuperación no se esté dando en la periodicidad establecida. Este control estará a cargo de la Alta Gerencia y se evaluará con la Gerencia de manera mensual en la revisión de informes financieros. El capital expuesto es el máximo permitido por las normas vigentes para la liquidación de entidades, es decir, cuando concurran pérdidas que reduzcan el patrimonio neto por debajo de 50% del capital suscrito o por instrucciones impartidas desde el máximo órgano social.

Recuperación de Cartera:
La institución cuenta con políticas y procedimientos de cartera donde, entre otros aspectos, se definen las medidas para una gestión de cobro eficiente de la cartera y se implementan las estrategias de cobro.

1.5 Gestión del riesgo de Liquidez

1.5.1 Objetivo General

Prevenir que la institución se quede sin recursos líquidos para cumplir con sus obligaciones; para gestionar este riesgo debe mantener un adecuado recaudo de cartera, plantear una adecuada modelación y monitoreo a las volatilidades del mercado financiero y una adecuada modelación y gestión de ingresos por venta de servicios de salud, contratados bajo modalidades diferentes al pago por evento, que al combinarlo con los costos correspondientes, eviten la disminución de sus recursos líquidos tanto en el corto (riesgo inminente) como en el mediano y largo plazo (riesgo latente).

1.5.2 Ciclo general de gestión del riesgo de liquidez

La Gestión del Riesgo y las Actividades de Control de la institución se basa en un modelo de líneas de defensa consignadas en el presente manual. Ver numeral 8.1 Estructura, roles y responsabilidades.

1.5.2.1 Identificación de riesgos

La identificación de los riesgos de liquidez estará a cargo de la Dirección Financiera o quien haga sus veces a través de todas las áreas que la conforman.

Para la adecuada identificación de riesgos, se tendrán en cuenta los siguientes aspectos:

a. **Identificación de activos líquidos**: La institución considera como activos líquidos aquellos que son o se pueden convertir fácilmente en efectivo, entre los que se destacan en los estados financieros:

   Disponible: Conformada por las siguientes cuentas contables: Caja – Bancos – Cuentas de Ahorro – Equivalentes de Efectivo.

   Cartera: Al valor de la cartera bruta se le descontará el deterioro de cartera, el cual fue construido con los históricos del comportamiento de pago de las diferentes aseguradoras con las cuales interactúa la institución. El deterioro de cartera incluye aquellas situaciones particulares de las aseguradoras, que bien no se manifiestan en los comportamientos negativos de pagos históricos, las condiciones actuales pueden conllevar a futuro tal situación.

   Para el análisis de la liquidez de la institución se tendrá en cuenta los días de rotación de la cartera consolidada para realizar las proyecciones del flujo de caja e ingresos por prestación de servicios de salud.

b. **Identificación de pasivos:** Para la elaboración de los flujos de caja proyectados se tendrá en cuenta los pasivos de la entidad, bajo cualquier concepto (insumos y medicamentos; dispositivos médicos o equipo biomédico; salarios; gastos operativos y administrativos; entre otros); se deben identificar el valor causado y pagado de los costos y gastos de la operación de la entidad; además, se debe proyectar cualquier movimiento de salidas futuras de efectivo bajo cualquier concepto según las periodicidades de pago de estas de acuerdo a lo acordado con los terceros.

1.5.2.2 Evaluación y Medición del Riesgo de Liquidez

La institución mide y proyecta los flujos de caja de sus activos y pasivos, en diferentes horizontes de tiempo, para ello, elabora por lo menos anualmente, el flujo de caja proyectado del año siguiente, para determinar las necesidades o excesos de liquidez. Este flujo de caja proyectado tendrá seguimiento periódico por parte de la Alta Dirección para determinar las variaciones.

Mediciones Adicionales:

Anualmente, la institución proyectará los flujos de caja de sus activos y pasivos en un escenario de crisis bajo hipótesis razonable conocida como Stress Testing, basada en el comportamiento de pagos de cartera y los pagos a terceros. Este modelo se construye con información histórica que permita estimar un mejor modelo.

Esta proyección permite determinar posibles necesidades de liquidez por efecto de cambios imprevistos en el entorno de los mercados, de la institución o de ambos y es de apoyo para la toma de decisiones de la Administración.

Para la elaboración del modelo de Stress Testing, primero se elabora el modelo de flujo de caja con base en información de los elementos que lo conforman y la periodicidad de ejecución real de los mismos, teniendo en cuenta el contexto interno y externo (a manera de ejemplo sin limitarse a ello, días reales de recuperación de cartera, porcentaje de recuperación de glosas, tiempo promedio de pagos a proveedores, etc.). Para determinar que el modelo predictivo es el óptimo, se efectúa pruebas de Back Testing, utilizando datos históricos.

Una vez confirmado que el modelo es el adecuado, se procede con las pruebas de Stress Testing. El objetivo de esta prueba es verificar la estabilidad y fiabilidad del flujo de caja en escenarios extremos para determinar las alternativas a seguir en caso de materializarse dichos escenarios.

Todo lo anterior con el fin identificar señales de alerta temprana y establecer límites encaminados a evitar la materialización de riesgos asociados como el Riesgo de Crédito, Mercado y Actuarial.

1.5.2.2.1 Herramienta básica para calcular la posición de liquidez

La evaluación del riesgo inherente de liquidez se efectuará a través de herramientas tecnológicas que garantice la “prueba de liquidez” en la institución.
Los ítems de desglose son:

- Ingresos: Corresponde a ingresos de caja por dos conceptos: o Ingresos del negocio por la operación por la venta o prestación de servicios de salud de sus diferentes unidades funcionales
- Otros ingresos: incluyen todos los otros ingresos diferentes a los operacionales.
- Costos y Gastos por atenciones o prestaciones de servicios de salud.
- Impacto de operaciones de inversión (Capex).
- Flujo de caja bruto del periodo y acumulado.

1.5.2.3 Tratamiento y Control del Riesgo de Liquidez

La institución toma diferentes medidas para controlar los riesgos de liquidez que se puedan presentar. Dentro de los controles establecidos se encuentran la revisión y seguimiento de los flujos de caja proyectados y reales en forma periódica.

Los controles guardan relación con el volumen y la complejidad de la operación. Son conocidos y aprobados por la Alta Dirección de la entidad o quien haga sus veces.

Alertas tempranas:

- ✓ **Mínimos de caja:** Para solventar las posibles necesidades de liquidez, la institución establece como límite mínimo de caja al cierre de cada mes un % del presupuesto que debe ajustarse a las políticas de la institución.

- ✓ Aplicación de pruebas de medición de escenarios extremos (Stress Testing) y de Back Testing.

- ✓ **Comportamiento de la cartera:** Se efectúa seguimiento periódico al comportamiento de pago de las diferentes entidades contratantes, para determinar incrementos en los días de rotación de cartera.

Planes de acción:

Dependiendo de las circunstancias, la institución puede tomar diferentes acciones para mantener la liquidez en los límites establecidos:

- Prestamos entre filiales o entidades bancarias dependiendo de las condiciones financieras.
- Negociación en mesas de trabajo y conciliaciones.
- Venta de inmuebles sin que genere afectación del servicio con aprobaciones de la Alta Gerencia.
- Manejo de inventarios (consignación, cesión, extensión de plazos, etc.)
- Redistribución de la composición de ingresos mercado público y privado.
- Otros que considere la Alta Gerencia.

1.6 Gestión del riesgo de Mercado de Capitales

1.6.1 Objetivo General

Adoptar las medidas necesarias para evitar incurrir en pérdidas derivadas de un incremento no esperado, de las obligaciones adquiridas o la pérdida en el valor de los activos, por causa de las variaciones en los parámetros del mercado.

1.6.2 Ciclo general de gestión del riesgo de mercado de capitales

La gestión del riesgo y las actividades de control de la institución se basan en un modelo de las líneas de defensa. (Ver numeral 8.1 - Estructura, roles y responsabilidades).

1.6.2.1 Identificación de riesgos

La identificación de los riesgos de mercado de capital estará a cargo de la Dirección Financiera o quien haga sus veces a través de todos los procesos que la conforman. (Ver numeral 9.3.1 del presente manual).

Para la adecuada identificación de riesgos, se tendrán en cuenta los siguientes aspectos:

a. **Factores de Riesgos**: La institución considera como factores de riesgos asociados a los riesgos de mercado de capitales los siguientes: tasas de interés variables, el precio de bienes

inmuebles, la tasa de cambio y el precio de las acciones (cuando aplique).

b. Activos y pasivos expuestos a los factores de riesgo: Los siguientes son los activos y pasivos que pueden estar expuestos al riesgo de mercado de capitales.

Descripción	Tipo	Factor de Riesgo
Cuentas de ahorro	Activo	Tasa de Interés
Equivalentes de efectivo	Activo	Tasa de Interés
Inversiones	Activo	Precio de las acciones, tasas de interés.
Activos Fijos	Activo	Precio Inmuebles
Propiedades de inversión	Activo	Precios inmuebles
Obligaciones Financieras	Pasivo	Tasa de interés variable; tasa de cambio
Proveedores	Pasivo	Tasa de Cambio

1.6.2.2 Evaluación y Medición del Riesgo de Mercado de Capitales

La institución mide y cuantifica las posibles pérdidas esperadas derivadas de la exposición al riesgo de mercado de capitales. Para ello, la Dirección Financiera o quien haga sus veces determina los activos y pasivos a los cuales la organización podría estar expuesta por la variación de los factores de riesgos antes descritos y realiza las siguientes acciones:

- Mediciones, reconocimiento, presentación y revelación en los estados financieros de los resultados generados por efecto del cambio en los factores de riesgos en los activos y/o pasivos de la institución, basado en el marco de información financiera y contable.

- Si los activos y pasivos afectados por los factores de riesgo antes mencionados son relevantes para la organización, se calculará el capital expuesto, mediante una metodología de reconocido valor técnico. La relevancia de los activos y/o pasivos puede estar basado en el nivel de materialidad determinado por la Revisoría Fiscal para la evaluación de estados financieros o por alguna otra que determine la Administración.

1.6.2.3 Tratamiento y Control del Riesgo de Mercado de Capitales

La institución toma diferentes medidas para controlar los riesgos de mercado de capitales que se puedan presentar, dentro de éstas se encuentran la revisión y seguimiento de los activos y pasivos que son afectados por los factores de riesgos asociados.

Alertas tempranas:

- ✓ Incremento del nivel de activos y/o pasivos afectados por factores de riesgos.
- ✓ Variaciones en las tasas de interés, tasas de cambio, en general, cambios políticos y/o macroeconómicos.
- ✓ Resultados de la aplicación de la metodología escogida para la medición de escenarios extremos (*Stress Testing*).

1.7 Gestión del riesgo de Grupo

1.7.1 Objetivo General

Adoptar las medidas necesarias para evitar incurrir en pérdidas que surgen 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 a fuentes de riesgo adicionales a las propias del negocio de la entidad, dentro de las que se encuentran, por ejemplo:

- Riesgo de contagio financiero
- Detrimentos patrimoniales por filtración de flujos o concentración de pasivos
- 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.

1.7.2 Ciclo general de gestión del riesgo de Grupo

La Gestión del Riesgo y las Actividades de Control de la Institución se basan en un modelo de las líneas de defensa. Las funciones de las demás líneas de defensa pueden ser consultadas en el Manual Integral de Gestión de Riesgos (Ver numeral 8.1 - Estructura, roles y responsabilidades).

1.7.2.1 Identificación de riesgos

La Institución forma parte de un grupo empresarial y tiene identificado los siguientes riesgos:

- Riesgo de contagio, donde resultados negativos en el ámbito financiero, calidad del servicio, entre otros, de las demás entidades del grupo empresarial impliquen algún estrés al interior de la entidad.

- Concentración del riesgo, donde un mismo tipo de riesgo se puede materializar en la entidad y de las demás entidades del grupo empresarial 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.

- Conflictos de intereses, especialmente en aquellos procedimientos o procesos donde se comparten sinergias, a manera de ejemplo en procesos de compras.

1.7.2.2 Evaluación y Medición del Riesgo de Grupo

La Institución tiene establecidos mecanismos para la medición y evaluación del riesgo de grupo teniendo en cuenta los descritos en el presente manual (Ver numeral 9.3.1)

1.7.2.3 Tratamiento y Control del Riesgo de Grupo

La Institución tiene implementadas medidas para controlar los riesgos de grupo que se puedan presentar como, por ejemplo, la identificación exacta de las transacciones que se realizan entre vinculadas, revisión y seguimiento de los informes financieros por la Alta Gerencia o quien haga sus veces en el grupo empresarial.

Alertas tempranas:

- ✓ Resultados negativos en el ámbito financiero.
- ✓ Indicadores de calidad del servicio negativo en forma recurrente.
- ✓ Daño reputacional en algunas de las Compañías del Grupo.
- ✓ Integración de procesos corporativos sin rendición de cuentas.

1.8 Gestión del riesgo de falla de mercado

1.8.1 Objetivo General

Prevenir la ocurrencia de pérdidas derivadas de la estructura del mercado de salud que genere pérdidas en el bienestar y beneficios de la Institución.

1.8.2 Ciclo general de gestión del riesgo de fallas de mercado

La Gestión del Riesgo y las Actividades de Control de la Institución se basan en un modelo de las líneas de defensa las cuales pueden ser consultadas en este Manual (Ver numeral 8.1 - Estructura, roles y responsabilidades).

1.8.2.1 Identificación de riesgos

La identificación de los riesgos de fallas de mercado estará a cargo de la Alta Dirección o quien haga sus veces a través de los procesos que la conforman.

Para la adecuada identificación de riesgos, se tendrán en cuenta los siguientes aspectos:

Competencia: La Alta Gerencia a través de la Junta Directiva y demás procesos efectuarán periódicamente un análisis del contexto externo que permita determinar cambios organizacionales y/o estructurales en la competencia.

Aseguradoras: La Alta Dirección de la Institución evaluará periódicamente la concentración de sus ingresos por asegurador que le permita diversificar su portafolio de ingresos en otras y evitar posibles manipulaciones de tarifas que afecten la rentabilidad y sostenibilidad en el mediano y largo plazo.

Proveedores: La Alta Dirección de la Institución efectuará periódicamente un análisis del contexto externo para determinar la conformación de grupos monopólicos y oligopólicos en proveedores que puedan impactar la determinación de precios de medicamentos e insumos afectando los resultados y estrategia.

1.8.2.2 Evaluación y Medición del Riesgo de Fallas de Mercado

Para determinar si el riesgo de fallas de mercado se está materializando, la Institución a través de la Alta Dirección revisa en forma periódica, los resultados de la operación tanto administrativa como asistencial para determinar posibles variaciones o fluctuaciones materiales.

En esta evaluación deben determinar si estas variaciones están originadas por:

- ➢ Sobrecostos por precios de medicamentos e insumos transados con los proveedores.
- ➢ Disminución de ingresos por:

1. Convenios de las aseguradoras con otras IPS para presionar reducción de tarifas.
2. Dobles autorizaciones requeridas por las aseguradoras en atenciones de usuarios para retraso de pagos.
3. Las restricciones en la gestión de riesgos y sobrecostos asociados al déficit de la oferta de servicios de salud respecto de la demanda de estos.

1.8.2.3 Tratamiento y control del riesgo de fallas de mercado

Teniendo en cuenta la probabilidad e impacto de las diferentes fallas de mercado sobre las pérdidas que se puedan generar en la Institución, se tomarán los siguientes controles:

Competencia: La Alta Gerencia o quien haga sus veces efectúa periódicamente un análisis del contexto externo que permita determinar cambios organizacionales y/o estructurales en la competencia.

Aseguradoras:

- Diversificación de la concentración de ingresos a través de la vinculación de nuevas aseguradoras que cumplan con los requisitos de la Institución.

- Revisión y/o elaboración de guías clínicas y/o protocolos teniendo en cuenta el perfil epidemiológico de la institución que permita optimizar recursos al interior de la organización.

Proveedores:

- Revisión y/o elaboración de guías clínicas y/o protocolos, teniendo en cuenta el perfil epidemiológico de la institución que permita optimizar medicamentos e insumos al interior de la organización.

- Seguimiento al comportamiento de precios de los medicamentos e insumos. Se determinará al interior de la institución la viabilidad de otras alternativas de medicamentos o insumos sin que afecte la atención a los pacientes y usuarios.

La Institución, a través de su Representante Legal o a quien designe, informará a las autoridades competentes actos o acuerdos contrarios a la libre competencia o que constituyan abuso de la posición dominante en el mercado.

Alertas tempranas:

- ✓ Concentración de la mezcla de mercado por asegurador.
- ✓ Información pública obtenida en medios de comunicación.
- ✓ Análisis del contexto interno y externo del sector.
- ✓ Informes de grupos y asociaciones a los que este afiliado.

1.9 Gestión del riesgo Reputacional

1.9.1 Objetivo General

El Riesgo Reputacional corresponde a la posibilidad de toda acción propia o de terceros, que pueda afectar negativamente el buen nombre y prestigio de la Institución, como publicidad negativa, ya

sea verdadera o no, que puede disminuir la confianza pública en la Institución, dar lugar a litigios costosos, a una disminución de usuarios, clientes, negocios o los ingresos, entre otros.

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.

1.9.2 Ciclo general de gestión del riesgo reputacional

La Gestión del Riesgo y las Actividades de Control de la Institución se basan en un modelo de las líneas de defensa (Ver numeral 8.1 - Estructura, roles y responsabilidades).

La rápida y efectiva resolución de problemas es clave para evitar situaciones que puedan afectar negativamente la reputación de la Institución.

1.9.3 Identificación de riesgos

La entidad identifica un inventario de eventos (matriz de riesgos) que tienen posibles efectos sobre su reputación y estos están a cargo de los líderes de los procesos de cada área que conforma la organización. Para la Institución, cualquiera de sus procesos puede generar riesgo reputacional, algunos en mayor escala que otros, pero por ser un riesgo de alto impacto, es obligación de todas las áreas considerar la existencia de este riesgo.

Dentro de los factores que pueden originar un riesgo reputacional se encuentran:

- ✓ Atención de usuarios: A manera de ejemplo sin limitarse a ellos: atención inoportuna, tratamiento médico incorrecto, falta de información, resultados de exámenes incorrectos, desabastecimiento de medicamentos.
- ✓ Facturación: Cobros excesivos, mayor valor facturado o errores en facturación.
- ✓ Pagos: Inoportunidad en los pagos, toma de descuentos no autorizados.

1.9.4 Evaluación y Medición del Riesgo Reputacional

Para determinar si el riesgo reputacional se está materializando, la institución realizará las siguientes actividades:

- ➢ Validación periódica de las peticiones, quejas, reclamos de las partes interesadas.
- ➢ Seguimiento a los indicadores NPS (Net Promoter Score)
- ➢ Monitoreo de redes sociales, prensa, noticia, radio y televisión, en caso de aplicar.
- ➢ Encuestas de satisfacción.
- ➢ Línea de transparencia
- ➢ Informes de abogados internos y externos, y aseguradores.

1.9.5 Tratamiento y Control del Riesgo Reputacional

Teniendo en cuenta la naturaleza de este riesgo, se recomiendan las siguientes medidas:

- ✓ La Alta Dirección o quien haga sus veces, efectúa seguimiento periódico al comportamiento de las encuestas de satisfacción y peticiones, quejas, reclamos y solicitudes de los usuarios para determinar si las mismas obedecen a situaciones puntuales o a mejoras que requieren los

procesos.

- ✓ Relacionamiento con proveedores y aseguradoras para determinar niveles de satisfacción y oportunidades de mejora.
- ✓ Seguimiento en redes sociales.
- ✓ Plan de Manejo de crisis, articulado con el plan de comunicaciones institucional.
- ✓ El Código de Conducta y Buen Gobierno incorpora políticas encaminadas a la medición, evaluación y seguimiento continuo de la reputación de la entidad y la toma de acciones, con el fin de mejorar los procesos que tienen relación directa o indirecta con la reputación.

1.10 Gestión del riesgo de corrupción, opacidad, fraude y soborno (COFS)

1.10.1 Objetivo General

Prevenir y mitigar oportunamente los riesgos de corrupción, opacidad, fraude y soborno, a través de la implementación de las acciones preventivas o correctivas que se consideren necesarias para controlar los factores que los generan.

1.10.2 Ciclo general de gestión del riesgo de COFS

Por la particularidad normativa y operativa de la gestión del riesgo de corrupción, opacidad, fraude y soborno se maneja en documento separado y hace parte integral de este manual.

1.11 Gestión del riesgo de lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva (LA/FT/FPADM)

1.11.1 Objetivo General

Prevenir la posibilidad de pérdida o daño que puede sufrir la institución por su propensión a ser utilizada directa o a través de sus operaciones como instrumento para cometer delitos de Lavado de activos, Financiación del terrorismo y Proliferación de armas de destrucción masiva, o para dar apariencia de legalidad a las actividades delictivas.

1.11.2 Ciclo general de gestión del riesgo de LA/FT/FPADM.

Por la particularidad normativa y operativa de este riesgo se maneja en documento separado y hace parte integral de este manual.

1.12 Gestión del riesgo de protección de datos personales (PDP)

1.12.1 Objetivo General

Regular los procedimientos de recolección manejo y tratamiento de los datos de carácter personal que realiza la institución a fin de garantizar y proteger el derecho fundamental de HABEAS en el marco de lo establecido en la ley 1581 del 2012.

1.12.2 Ciclo general de gestión del riesgo de PDP.

Por la particularidad normativa y operativa de este riesgo se maneja en documento separado y hace parte integral de este manual.

Anexos

Anexo A – Definiciones de criterios de riesgo
Anexo B - Instructivo de Registro de Riesgos.
Anexo C - Análisis de situación territorial
Anexo D - Metodología para el monitoreo de las señales de alertas tempranas