HOSPITAL GENERAL DE MEDELLÍN
Oficina de Auditoría Interna
Construimos Confianza

Informe Final Auditoría Gestión de Riesgos

EQUIPO OFICINA DE AUDITORÍA INTERNA

CARLOS URIEL LÓPEZ RÍOS
Jefe de Auditoría Interna

MARÍA JANETH AGUDELO ARANGO
Profesional de Auditoría Interna

JOSE HERIBERTO VARGAS LEMA
Profesional de Auditoría Interna

Medellín
Julio de 2018

CONTENIDO

PRESENTACIÓN

La Oficina de Auditoría Interna, en cumplimiento de sus funciones y en especial la de "Planear, dirigir y organizar la verificación y evaluación del Sistema Institucional de Control Interno - SICI", presenta el Informe de la Auditoría al programa de Gestión de Riesgos de la Institución.

En la institución se tienen levantados los riesgos de 39 procesos con sus respectivos seguimientos, se tiene un apropiada metodología que permite obtener de manera cuantitativa el riesgo residual, se tiene debidamente documentado con sus respectivos informes de seguimiento el tema de la gestión de riesgos institucional, el cual cuenta con nivel profesional especializado en su manejo

El informe se estructura en seis capítulos. En el primero se enuncian las generalidades, el fundamento normativo, los documentos base y la terminología; en el segundo se establece el programa de gestión de riesgos. Por su parte, en el tercero se describe el núcleo de la auditoría. En el cuarto se presenta el consolidado de observaciones y recomendaciones. En capítulo quinto se presenta el ciclo de auditoría. En el sexto se presentan las conclusiones.

El presente Informe, se enmarca en la Línea III, Eje I. Aseguramiento y Control Interno Innovador del Plan Estratégico 2017 – 2021 **"Construimos Confianza"** de la Oficina de Auditoría Interna.

Nos anima el propósito de continuar liderando, desde la Oficina de Auditoría Interna, un conjunto de estrategias y acciones que permitan contribuir, desde la evaluación del gobierno, el control y los riesgos, a la consolidación, afianzamiento y sostenibilidad de los propósitos del Hospital General de Medellín, en el marco de la Mega definida para el año 2027.

I. GENERALIDADES.

1.1. Objetivo.

Realizar evaluación al programa de Gestión integral de Riesgos año 2018 del Hospital General de Medellín con el fin de verificar su conformidad en el gobierno, gestión de riesgos y controles.

1.2. Alcance.

Esta auditoría inicia con la revisión de la política de riesgos, el instructivo para la administración de riesgos, el programa de gestión integral del riesgo y el proyecto de implementación de la gestión de riesgos de acuerdo con la NTC ISO 31000.

1.3. Metodología.

1.3.1. La Auditoría inicia con una reunión de apertura con personal del área líder objeto de la Auditoría.
1.3.2. Se realiza análisis documental, revisión del proceso, sus procedimientos, formatos, instructivos.
1.3.3. Se entrevista con funcionarios y líder del proceso.
1.3.4. Se entrevista con funcionarios de otros procesos relacionados. Cliente proveedor.
1.3.5. Se aplica el cuestionario de tablero de controles.
1.3.6. Se revisan los indicadores de gestión, la matriz de riesgos y de controles; así como la información del avance del plan de acción.
1.3.7. Se verifican y organizan las evidencias.
1.3.8. Se revisa y analiza la información.
1.3.9. Se realiza entrevista con personal del proceso.
1.3.10. Se revisan carpetas con soportes e informes generados.
1.3.11. Se identifican las observaciones y se formulan las recomendaciones de la auditoría.
1.3.12. Se elabora Informe Preliminar de Auditoría.
1.3.13. Se realiza reunión de cierre para formalizar informe.
1.3.14. Se envía el Informe Preliminar.
1.3.15. Se reciben observaciones del proceso auditado.
1.3.16. Se realiza Informe Final.
1.3.17. Se elabora Plan de Mejoramiento de Auditoría.

1.4. Fundamento Normativo.

1.4.1. Ley 87 de 1993. Por la cual se establecen las normas para el ejercicio del Control interno en las entidades y organismos del estado.

Artículo 2 Objetivos del control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

ARTÍCULO 4. ADMINISTRACIÓN DE RIESGOS. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas, las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.

1.4.2. Ley 1474 de 2011. Estatuto Anticorrupción. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Artículo 73. Plan anticorrupción y de atención al ciudadano que deben elaborar anualmente todas las entidades incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.

1.4.3. Circular Externa 09 de 2016 de la Supersalud. Por la cual se imparten instrucciones relativas al sistema de administración de riesgos de lavado de activos y financiación del terrorismo (SARLAFT).

1.4.4. Decreto 903 de 2014. Por la cual se dictan disposiciones en relación con el Sistema Único de Acreditación en Salud.

1.4.5. Decreto 648 del 19 de Abril de 2017. Por el cual se modifica y Adiciona Título 16 del Decreto 1083 de 2015 - Reglamentario Único del sector de la Función Pública.

Art 17. “Las unidades u oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control” (10).

1.4.6. Decreto 1499 del 11 de Septiembre de 2017. Por medio del cual se modifica Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley de la Ley 1753 de 2015.

Art 2.2.23.1. “El Sistema de Control Interno previsto en la Ley 87 de 1993 y en la Ley 489 de 1998, se articulará al Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades”.

1.4.7. Resolución 4559 de 2018 de la Supersalud. Por medio de la cual se adopta el modelo de inspección, vigilancia y control para la Superintendencia Nacional de Salud para el ejercicio de la supervisión de riesgos inherentes al Sistema General de Seguridad Social en Salud.

Anexo Documento Técnico - Supervisión de los riesgos inherentes al sistema general de seguridad social.

1.4.10 Decreto 2462 de 2013 de la Supersalud.

Artículo 7 numeral 6. Impartir las instrucciones a los sujetos vigilados sobre la manera cómo debe administrar los riesgos propios de su actividad.

1.5. Documentos Base.

1.5.1. Política de la Gestión de Riesgos del HGM. Código ES-GIC-GC001P04

1.5.2. Programa Gestión integral del riesgo. Código ES-GIC-GC001F13

1.5.3. Documento ayuda memoria para la identificación y valoración de riesgos. Código ES-GIC-GC001D14.

1.5.4. Formato matriz de riesgos. Código ES-GIC-GC001F13

1.5.5. Instructivo para la administración de riesgos en el HGM. Código ES-GIC-GC001I02

1.5.6. NTC ISO 31.000

1.6. Terminología básica.

- **Alta Dirección.**

Se denomina a los directivos con más alto cargo en una organización. En nuestra institución está conformado en el siguiente orden jerárquico: Gerente, Subgerente de procesos administrativos y Subgerente de procesos asistenciales y Directores de las diferentes áreas.

- **Análisis del Riesgo.**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis del riesgo proporciona las bases para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo. El análisis de los riesgos incluye su valoración.

- **Causa.**

Medios, circunstancias, situaciones o agentes generadores del riesgo.

- **Consecuencia.**

Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento. Es el resultado de un evento que afecta los objetivos. Las consecuencias se pueden expresar cualitativa o cuantitativamente.

- **Control.**

Medida que modifica al riesgo.

- **Corrupción.**

Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

- **Evaluación del Riesgo.**

Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **Gestión del Riesgo.**

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- **Identificación del Riesgo.**

Proceso para encontrar, reconocer y describir el riesgo. Implica identificación de las fuentes de riesgo, los eventos, sus causas y sus consecuencias potenciales.

- **Impacto.**

Medida de severidad.

- **Marco de Referencia para la Gestión del Riesgo.**

Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo a través de toda la organización.

- **NTC ISO 31000.**

Norma Técnica Colombiana Principios y Directrices para la gestión del Riesgo.

- **Parte Interesada.**

Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad, entre ellas tenemos:

- Junta Directiva.

- Alta Dirección: Gerencia y directores responsables de los procesos.
- Colaboradores.
- Entidades reguladoras, Autoridades locales.
- Clientes, usuarios y sus familias.
- Proveedores de bienes y servicios.
- Comunidad en general.

- **Perfil del Riesgo.**

Descripción de cualquier conjunto de riesgos. El conjunto de riesgos puede contener aquellos que se relacionan con la organización en su totalidad.

- **Plan para la Gestión del Riesgo.**

Esquema dentro del marco de referencia para la gestión del riesgo que específica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo.

- **Probabilidad.**

Medida de la oportunidad de ocurrencia.

- **Proceso para la Gestión del Riesgo.**

Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento y monitoreo.

- **Riesgo.**

Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.

- **Riesgo Inherente.**

Es aquél al que se enfrenta una entidad en ausencia de acciones para modificar su probabilidad o impacto.

- **Riesgo Estratégico.**

Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- **Riesgo de LA/FT.**

Es la posibilidad de pérdida o daño que puede sufrir una entidad, por su propensión a ser utilizada directo o a través de sus operaciones, como instrumento para cometer los delitos de lavado de activos o la canalización de recursos para la financiación del terrorismo.

- **Riesgo Operativo.**

Posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye los riesgos legal y reputacional, asociados a tales factores.

- **Riesgo Puro o de Azar.**

Son aquellos que únicamente ofrecen una probabilidad de pérdida, entendidas como resultados no deseables. Los seguros funcionan principalmente alrededor de los riesgos de pérdidas y no de riesgos de ganancias, es decir, trabajan con riesgos puros más que con riesgos especulativos. Ejemplo incendio, hurto, entre otros.

- **Riesgo Residual.**

Es aquel que permanece después que se desarrollan respuestas o acciones (controles) para enfrentar los riesgos.

- **Tratamiento del Riesgo.**

Proceso para modificar el riesgo.

- **Valoración del Riesgo.**

Proceso global de identificación del riesgo análisis del riesgo y evaluación del riesgo.

1.7. Limitaciones

La auditoría no presentó limitaciones que afectará el desarrollo de la misma. Al contrario los profesionales, y el responsable del proceso que fueron citados, atendieron de manera oportuna y diligente los requerimientos de la auditoría, al igual que toda la información solicitada fue suministrada de manera oportuna y confiable.

II. PROGRAMA GESTIÓN INTEGRAL DEL RIESGO.

2.1. Comunicación y Reporte de Riesgos.

Dice el numeral 5.4.2.4 del Programa de gestión integral del riesgo que es necesario que la alta gerencia comunique el propósito y la importancia del programa de gestión de riesgos a todas las partes interesadas y uno de los mecanismos utilizados es mediante la política de gestión de riesgos debe ser desplegada a todos los niveles de la institución, como un factor clave para la gestión del riesgo.

La auditoría observa que esta actividad no se está realizando con todas las partes interesadas en la Institución, ya que no hay evidencia de la misma.

2.2. Rendición de cuentas.

Dice el numeral 5.4.2.5 del programa que los responsables de los procesos, son los propietarios de sus riesgos y les corresponde rendir cuentas sobre su gestión, para esto se tienen implementados indicadores que evalúan el desempeño de su proceso y la vez realizan seguimiento a los controles implementados para mitigar los riesgos que puedan afectar el logro de los objetivos del proceso, en términos de eficiencia, eficacia y efectividad. Reportes detallados preparados y revisados por directores y líderes, con referencia a los riesgos en sus áreas de responsabilidad, de forma periódica en las evaluaciones del Plan de acción.

La auditoría observa que esta actividad de Rendición de cuentas no se está ejecutando en la actualidad, ni en la presentación de los planes de acción, ni en informes gerenciales para la Junta Directiva.

2.3. Mejora continua.

Dice el numeral 5.4.2.6 del programa que a medida que se cumplen los objetivos, nuevos objetivos se establecen para generar una mejora continua del marco y el proceso de gestión de riesgos. Que el Hospital General de Medellín asume de manera permanente, homologada y coherente las mejores prácticas para la gestión de riesgos, en la búsqueda de su mejoramiento continuo. Es importante el reconocimiento y manejo de riesgos emergentes, la gestión del riesgo, ayuda a identificar y manejar riesgos que pueden afectar a una o algunas veces varios procesos dentro de la institución. Que la gestión del riesgo está alineada con el modelo de mejoramiento institucional y es una de las fuentes de mejora. Para el tratamiento de los riesgos se implementan planes de mejoramiento, especialmente en los casos que se identifican nuevos riesgos, cuando es necesario rediseñar los controles existentes o definir unos nuevos controles.

La auditoría observa que esta actividad de Mejora continua y todo el relacionamiento de gestión de riesgos con el modelo de mejoramiento institucional, aún es incipiente en la institución.

2.4 Identificación del riesgo

Identificar un riesgo es determinar los posibles eventos que con su materialización puedan impactar objetivos, estrategias, planes o proyectos de la institución.

La identificación de los riesgos es considerada la actividad o etapa más importante del proceso de gestión; no sólo porque los riesgos no identificados son asumidos inicialmente por la empresa, sino también porque es el momento que habilita un buen ejercicio de análisis de riesgos, de tratamiento, monitoreo y comunicación.

Para identificar los riesgos de la institución es necesario, inicialmente, tener claridad acerca de los tipos de riesgos inherentes al sector de la salud. La variedad de riesgos puede ser alta, igual que las formas de clasificarlos y abordarlos.

La auditoría observa falta de integración de los riegos institucionales tal cual lo propone el programa de gestión integral de riesgos, no es clara la integración de los riesgos de los procesos, con riesgos ocupacionales, ambientales, clínicos, de corrupción, de fraude, tecnológicos y seguridad de la información.

2.5 Tratamiento de riesgos

En el numeral 5.4.3.4 de tratamiento de los riegos, está enunciado que para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros. El tratamiento de riesgos implica tomar decisiones basadas en los resultados de la identificación de riesgos y su análisis.

La auditoría observa que no hay claridad de las acciones encaminadas a prevenir la materialización de los riesgos críticos de la institución. Adicionalmente no está definido el apetito de Riesgo en la institución.

Observación de Auditoría Interna N° 1.

Revisado el programa de gestión integral del riesgo, la auditoría observa falta de evidencias que demuestren el desarrollo de los siguientes temas:

- Comunicación y reporte de riesgos del programa de gestión de riesgos a todas las partes interesadas.
- Rendición de cuentas no se está ejecutando en la actualidad, ni en la presentación de los planes de acción, ni en informes gerenciales para la Junta Directiva.
- Actividad de mejora continua y todo el relacionamiento de gestión de riesgos con el modelo de mejoramiento institucional aún es incipiente en la institución.
- Falta de integración de los riegos institucionales tal cual lo propone el programa de gestión integral de riesgos, no es clara la integración de los riesgos de los procesos, con riesgos ocupacionales, ambientales, clínicos, de corrupción, de fraude, tecnológicos y seguridad de la información.
- No hay claridad de las acciones encaminadas a prevenir la materialización de riesgos, especialmente aquellos riesgos críticos de la institución, ni acciones para reducir o compartir el riesgo. Adicionalmente no está definido el apetito de Riesgo en la institución.

Criterios de Auditoría:

Programa Gestión integral del riesgo. Código ES-GIC-GC001F13

Riesgo:

Afectación del nivel de madurez de la gestión de riesgos en la institución.

Recomendación:

Medir de manera periódica el nivel de adherencia al programa gestión integral de riesgos.

2.6 Indicadores de Gestión

En el capítulo número 6, del programa gestión integral del riesgo están considerados dos indicadores de gestión, uno el índice de riesgo residual por proceso y el otro el nivel de madurez de la gestión del riesgo.

El nivel de madurez de la gestión del riesgo es una herramienta utilizada para capturar y evaluar las prácticas de riesgos de la institución y proporcionar realimentación en forma de una calificación de Madurez de la Gestión de Riesgos. El índice se calcula en base a preguntas relacionadas con las actuales prácticas de gestión de riesgos, la estructura de gobierno corporativo y el proceso de toma de decisiones de la empresa.

Observación de Auditoría Interna N° 2.

La auditoría observa que el indicador de Nivel de madurez de la gestión de riesgos, medida en el Hospital en el mes de diciembre del año 2017, dio como resultado un índice del 1.5% en una escala de madurez del 1 al 5., lo que significa un nivel inicial a básico. Este nivel de madurez tiene según la metodología las siguientes características:

- Desarrollo limitado de capacidades para identificar, evaluar y priorizar riesgos por toda la organización.
- Inconsistencias en las prácticas/enfoques de gestión de riesgos en la organización (es decir que las prácticas son compartimentadas).
- Consideraciones informales y poco constantes hacia la información de riesgos y su gestión en la toma de decisiones.

Este indicador, con la misma metodología, se aplicó en la institución en el año 2014, con idénticos resultados de 1.5 en la escala de 1 al 5, es decir en el periodo de 3 años no se logró impactar el indicador.

Criterios:

La meta propuesta de Nivel de Madurez de la Gestión del Riesgo para el Hospital General de Medellín, es: Mayor de 3.0, La tabla que orienta la calificación es la siguiente:

5 Avanzado	La organización ha desarrollado completa y adecuadamente su capacidad para identificar, medir, gestionar y monitorizar sus riesgos; sus procesos de gestión de riesgos son dinámicos y se adaptan a los cambios de los mismos y a los ciclos del negocio. • Existe una declaración formal de apetito frente al riesgo, niveles de tolerancia y políticas de decisión • El riesgo y su gestión está expresamente considerado en la toma de decisiones • La medición y análisis de los riesgos es continuo, con técnicas cuantitativas y cualitativas • La gestión de los riesgos se considera una ventaja competitiva
4 Operativo	La organización conoce claramente sus principales riesgos y lleva a cabo actividades concretas para el tratamiento y gestión de los mismos; algunas de sus áreas aplican técnicas sofisticadas de medición. • El catálogo de pérdidas y el concepto de tolerancia están definidos o en desarrollo • Información sobre el riesgo y su gestión se considera de forma indirecta en la toma de decisiones • La medición y análisis de los riesgos es avanzado, utilizando técnicas cuantitativas y cualitativas
3 Definido	La organización ha identificado y está en proceso de conocer sus riesgos; su capacidad para identificar, medir, gestionar y están definidas pero son inconsistentes dentro de toda la organización. • Directrices generales sobre pérdidas y tolerancia a las mismas están todavía en fase inicial • El riesgo y su gestión se consideran informalmente en la toma de decisiones • Algunos riesgos se miden principalmente de forma cuantitativa
2 Básico	Inconsistencias en toda la organización sobre el concepto de riesgo y su gestión; capacidad para identificar, medir, gestionar y monitorizar los riesgos es limitada. • Las actividades de gestión de riesgo ocurren en niveles funcionales, no a nivel corporativo • Las gestión de riesgo se centra en asuntos de cumplimiento normativo • El riesgo y su gestión se considera informalmente en el momento y en base a circunstancias especificas
1 Inicial	Si la organización identifica y clasifica sus riesgos lo hace cada departamento o función de forma independiente, sin criterios, coordinación y comunicación común; sus componentes y metodologías son simples y limitadas a cada función.

Riesgo:

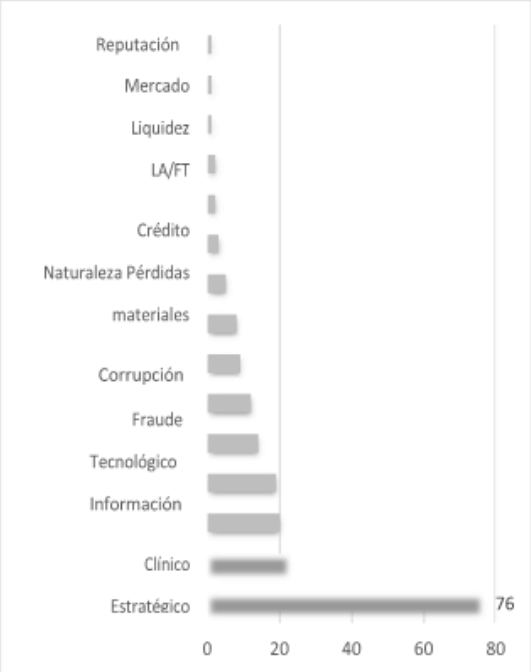
El no cumplimiento de este indicador afecta el logro del objetivo estratégico número seis, que plantea consolidar la institución como un hospital líder en buenas prácticas de gobierno corporativo y gestión pública, ya que dentro de este está formulado el proyecto de gestión de riesgos institucional.

Recomendación:

- Aumentar la concientización de la gestión de riesgos a nivel directivo y ejecutivo.
- Investigar mejores prácticas de gestión de riesgos.
- Desarrollar un plan para aumentar las capacidades de gestión de riesgos y la constancia de las mismas.
- Obtener un consenso a nivel ejecutivo y directivo sobre los riesgos principales de la organización.
- Asegurar la claridad con respecto a la asignación de responsabilidades de gestión de riesgos y su cumplimiento.

2.7 Mapa de Riesgos institucional

Se tiene un mapa de riesgos institucional debidamente actualizado con la versión 3. De las matrices de riesgos de los 39 procesos y programa de ensayos clínicos, en los cuales se observa identificados 201 riesgos en los procesos. Así:



CATEGORÍAS Y TIPOS DE RIESGOS	CANTIDAD
Operativo	169
Clínico	19
Corrupción	8
Cumplimiento o legal	22
Fraude	9
Información	14
LA/FT	2
Operativos	76
Reputación	1
Salud y Seguridad en el Trabajo	6
Tecnológico	12
Estratégico	20
Estratégico	20
Azar asegurable	8
Naturaleza	3
Pérdidas materiales	5
Financiero	4
Crédito	2
Liquidez	1
Mercado	1
Total general	201

Fuente: Documento informe de riesgo año 2017

Observación de Auditoría Interna N° 3.

Revisado el mapa de riesgos institucional la auditoría observa que este no ha sido socializado, revisado y evaluado en el comité coordinador de control interno, para que desde allí se direccione el tema de la gestión integral de riesgos, adicionalmente no se ha socializado con la Junta Directiva ni demás partes interesadas. No están todos los riesgos clínicos y estratégicos debidamente identificados, no está definido como se monitorean los riesgos extremos.

Criterios:

El modelo integrado de planeación y gestión (MIPG), decreto 1499 de 2017, establece que el equipo directivo debe identificar aquellos riesgos que impidan el logro de su propósito fundamental, las metas y los objetivos estratégicos.

Riesgo:

No cumplimiento de directrices de gestión del Riesgo.
Recomendación: Identificar de manera apropiada los riesgos estratégicos y claves de la institución y asegurar su monitoreo permanente para revisar la efectividad de los controles establecidos. Adicionalmente hacer seguimiento a los riesgos calificados como extremos. Los riesgos estratégicos y los calificados como extremos debe estar identificada su afectación a los objetivos estratégicos.

III. NÚCLEO DE AUDITORÍA: CONSOLIDACIÓN DEL SISTEMA DE GESTIÓN INTEGRAL DEL RIESGO

De acuerdo con el decreto 1499 de 2017, el manual operativo de implementación del modelo integrado de planeación y gestión (MIPG), en el numeral 7.2.2 Gestión de los riesgos institucionales estable que las entidades deberán asegurar la gestión del riesgo.

Hace referencia al ejercicio efectuado bajo el liderazgo del equipo directivo y de todos los servidores de la entidad, y permite identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos institucionales.

Estos eventos pueden tener un impacto negativo, positivo o de ambos tipos a la vez. Los de impacto negativo pueden interferir en la creación de valor o bien afectarlo de forma importante, en tanto que pueden lesionar la imagen institucional así como entorpecer la operación, la estrategia u otros aspectos relacionados con la prestación del servicio. Por su parte, los eventos de impacto positivo pueden compensar los negativos o representar oportunidades, ayudando a la creación de valor o a su conservación. Este componente, requiere que la alta dirección canalice las oportunidades que surgen para que se reflejen en la estrategia y los objetivos, y formular planes que permitan su aprovechamiento.

Para su efectivo desarrollo es necesario tener en cuenta que:

- Es un proceso continuo que fluye por toda la entidad
- Es llevado a cabo por todos los servidores de la entidad
- Se aplica en el establecimiento de la estrategia
- Está diseñado para identificar acontecimientos potenciales que, de ocurrir, afectarían a la entidad.
- Está orientado al logro de las metas estratégicas, los resultados esperados y en general de los objetivos de la entidad.
- Brindar atención prioritaria a los riesgos de carácter negativo y de mayor impacto potencial.
- Considerar la probabilidad de fraude que pueda afectar la adecuada gestión institucional.
- Identificar y evaluar los cambios que pueden afectar los riesgos al Sistema de Control Interno.
- Se debe dar cumplimiento al artículo 73 de la Ley 1474 de 2011, relacionado con la prevención de los riesgos de corrupción, - mapa de riesgos de corrupción.

Fortalecer la gestión del riesgo a partir del desarrollo de las otras dimensiones de MIPG

El trabajo abordado desde dimensiones como Direccionamiento Estratégico y Planeación, Gestión con Valores para Resultados y Talento Humano, es fundamental para materializar una adecuada gestión del riesgo, de conformidad con las siguientes interacciones:

- En la dimensión de Direccionamiento Estratégico y la Planeación, el representante legal y la alta dirección deben definir los lineamientos para la administración del riesgo de la entidad; el equipo directivo debe identificar aquellos riesgos que impidan el logro de su propósito fundamental y las metas estratégicas.
- La política para la gestión del riesgo se constituye en una política de operación para la entidad, por lo que la misma es aplicable a todos los procesos, proyectos y programas especiales. Para su definición se requiere contar con una visión sistémica y estratégica de las operaciones, se debe analizar los principales factores internos y externos acorde con el entorno de la entidad, los riesgos a nivel estratégico y su evaluación, aspectos que dan línea a toda la entidad en la identificación de los riesgos a todos los niveles.

Se requiere una completa correlación, integración y gestión de todos los tipos de riesgos institucionales como los de proceso, con los de salud y seguridad en el trabajo, clínicos, de fraude, tecnológicos, clínicos, seguridad de la información, ambientales, entre otros.

IV. CONSOLIDADO OBSERVACIONES Y RECOMENDACIONES.

4.1. Relación de las observaciones.

N°	Observación	Numeral
1	Revisado el programa de gestión integral del riesgo, la auditoría observa falta de evidencias que demuestren el desarrollo de los siguientes temas: • Comunicación y reporte de riesgos del programa de gestión de riesgos a todas las partes interesadas. • Rendición de cuentas no se está ejecutando en la actualidad, ni en la presentación de los planes de acción, ni en informes gerenciales para la Junta Directiva. • Actividad de mejora continua y todo el relacionamiento de gestión de riesgos con el modelo de mejoramiento institucional aún es incipiente en la institución. • Falta de integración de los riegos institucionales tal cual lo propone el programa de gestión integral de riesgos, no es clara la integración de los riesgos de los procesos, con riesgos ocupacionales, ambientales, clínicos, de corrupción, de fraude, tecnológicos y seguridad de la información. • No hay claridad de plan de acciones encaminadas a prevenir la materialización de riesgos, especialmente aquellos riesgos críticos de la institución, ni acciones para reducir o compartir el riesgo. Adicionalmente no está definido el apetito de Riesgo en la institución.	2.1,2.2 2.3,2.4 2.5
2	La auditoría observa que el indicador de Nivel de madurez de la gestión de riesgos, medida en el Hospital en el mes de diciembre del año 2017, dio como resultado un índice del 1.5% en una escala de madurez del 1 al 5., lo que significa un nivel inicial a básico. Este nivel de madurez tiene según la metodología las siguientes características:	2.6.

	• Desarrollo limitado de capacidades para identificar, evaluar y priorizar riesgos por toda la organización. • Inconsistencias en las prácticas/enfoques de gestión de riesgos en la organización (es decir que las prácticas son compartimentadas). • Consideraciones informales y poco constantes hacia la información de riesgos y su gestión en la toma de decisiones. • Inconsistencias en el entendimiento de ERM (Enterprise Risk Management) y su aplicación. Este indicador con la misma metodología se aplicó en la institución en el año 2014, con idénticos resultados de 1.5 es la escala de 1 al 5, es decir en el periodo de 3 años no se logró impactar el indicador.	
3	Revisado el mapa de riesgos institucional la auditoría observa que este no ha sido socializado, revisado y evaluado en el comité coordinador de control interno, para que desde allí se direccione el tema de la gestión integral de riesgos, adicionalmente no se ha socializado con la Junta Directiva ni demás partes interesadas. No están todos los riesgos clínicos y estratégicos debidamente identificados, no está definido como se monitorean los riesgos extremos.	2.7.

4.2. Recomendaciones.

<u>En el gobierno.</u>

4.2.1. Medir de manera periódica el nivel de adherencia al programa gestión integral de riesgos.

4.2.2. Continuar investigando las mejores prácticas de gestión de riesgos para automatizar y sistematizar el programa actual, el cual se encuentra manualizado. Desarrollar un plan para aumentar las capacidades de gestión de riesgos. Obtener un consenso a nivel ejecutivo y directivo sobre los riesgos principales de la organización. Asegurar la claridad con respecto a la asignación de responsabilidades de gestión de riesgos y su cumplimiento.

4.2.3. Estructurar el programa de gestión de riesgos de tal forma que se logre una completa integración con riesgos ocupacionales, ambientales, clínicos, de tecnología, de seguridad de la información, entre otros.

4.2.4. Socializar el mapa de riesgos y todo lo relacionado con la gestión de riesgos con las partes interesadas incluida la Junta Directiva.

4.2.5. Correlacionar el programa de gestión de riesgos con el modelo de mejoramiento institucional.

4.2.6. Generar estrategias para el fortalecimiento de la gestión de riesgos para establecerlo de arriba hacia abajo empoderando el equipo directivo. Es básico fortalecer los roles y responsabilidades en la gestión de riesgos en la primera, segunda y tercera línea de defensa. Desarrollar de manera

más consciente el tema de riesgos con mayor involucramiento de la alta Dirección para hacerlo de manera proactiva.

En el control

4.2.7. Generar capacidades al grupo de gestores de calidad en el tema de gestión de riesgos. Considerar la posibilidad de trabajar con un comité de riesgos.

4.2.8. Registrar la materialización de los riesgos y llevar datos estadísticos de éstos.

4.2.9. Vincular los planes de contingencia con el programa de gestión integral de riesgos.

4.2.10. Definir para la institución el apetito del riesgo.

4.2.11. Realizar seguimiento a riesgos del proceso de asesoría jurídica, es el único que está pendiente.

4.2.12. Generar evidencia del desarrollo de las acciones que frente al tema de gestión de riesgos está definida en el manual del modelo integrado de planeación y gestión (MIPG).

4.2.13. Estudiar la viabilidad de establecer la designación de recursos presupuéstales para consolidar y transformar la cultura del riesgo, adicionalmente revisar la asignación de recursos actuales a este proceso.

4.2.14. Asegurar un plan de entrenamiento continuo sobre gestión de riesgos, en los diferentes niveles de la organización.

4.2.15. Identificar las áreas o procesos con mayor vulnerabilidad.

En los riesgos

4.2.16. Generar proceso de Identificar de manera apropiada los riesgos estratégicos y claves de la institución y asegurar su monitoreo permanente para revisar la efectividad de los controles establecidos. Adicionalmente hacer seguimiento a los riesgos calificados como extremos.

4.2.17. Los riesgos estratégicos y los calificados como extremos debe estar identificada su afectación a los objetivos estratégicos.

4.2.18. Revisar los riesgos de los servicios habilitados.

4.2.19. Integrar y correlacionar el programa de seguridad del paciente con el sistema de gestión integral de riesgos en lo que corresponde con riesgos clínicos.

4.2.20. Fortalecer la identificación de los riesgos de fraude en la institución.

4.2.21. Dada la importancia actual del Riesgo Reputacional se recomienda generar un tratamiento especial de este riesgo materializado en la institución.

4.2.22. Igualmente generar estrategias para hacer un tratamiento especial al riesgo de liquidez y al riesgo de probable pérdida de la Acreditación.

V. CICLO DE LA AUDITORÍA.

5.1. Posición del Auditado.

Una vez recibido el Informe Preliminar, el responsable del proceso relacionado con el objeto de la presente auditoría, dispondrá de tres (3) días hábiles para manifestar su posición frente al mismo y para hacer la Evaluación del Auditor, en el formato correspondiente.

Mediante correo electrónico el día 22 de agosto de 2018, la líder del proceso de gestión de riesgos presentó un escrito de observaciones al informe de auditoría interna, el cual relacionamos a continuación:

"*OBSERVACIONES AL INFORME DE AUDITORIA INTERNA*
REALIZADA AL PROGRAMA DE GESTIÓN INTEGRAL DE RIESGOS INSTITUCIONAL
De acuerdo a informe de Auditoria recibido, respetuosamente solicito revisar y/o aclarar de ser necesario la anotación realizada en la siguiente observación:
Observación de Auditoría Interna N° 1, en los siguientes ítems:
Revisado el programa de gestión integral del riesgo, la auditoría observa falta de evidencias que demuestren el desarrollo de los siguientes temas:

1. PRIMER ITEM:
Comunicación y reporte de riesgos del programa de gestión de riesgos a todas las partes interesadas:
• Se han realizado despliegues del tema del Eje de Gestión de Riesgos en las reuniones administrativas de las áreas, en algunas de ellas acompañada por la coordinación de riesgos.
• En el nuevo aplicativo de Inducción y Reinducción que se realizó para los servidores, contratistas, terceros y estudiantes. Se tenían dispuestas explícitamente las principales políticas del HGM, ente ellas la de Gestión de Riesgo, incluso los riesgos por procesos.
• En Jornadas de Calidad que hemos venido participando desde el año pasado (2017), desplegando el programa de Gestión de Riesgos.
• En el Entrenamiento del puesto de trabajo de servidores en cargos administrativos que han ingresado el último año, se ha desplegado el Programa de Gestión de Riesgos.
Sin embargo, se reconoce que no se tiene cobertura en el total de las partes interesadas.

2. QUINTO ITEM:

No hay claridad de las acciones encaminadas a prevenir la materialización de riesgos, especialmente aquellos riesgos críticos de la institución, ni acciones para reducir o compartir el riesgo. (Tratamiento de riesgos)
Con la anotación realizada se afirma que no hay implementadas medidas de tratamiento para los riesgos en la institución.
Podemos demostrar que en la institución se dispone de medidas para reducir y compartir el riesgo, como se describen a continuación:

• En la institución como medida de tratamiento se transfiere o comparte el riesgo a través del contrato de seguros que cubre a la institución y que se tiene un contrato que es con la Previsora Seguros S.A y además tenemos un contrato con el Corredor de Seguros ITAU. Además en los contratos de bienes y servicios se exigen pólizas y de esta manera se comparte el riesgo
• El Hospital como medida de tratamiento transfiere o comparte el riesgo de algunos procesos que decidió tercerizar y que la ley por no ser proceso misionales lo permite, como son Mantenimiento, Lavandería, Alimentación e incluso tiene por Outsourcing agremiaciones de médicos especialistas. Como se puede observar se tienen varios contratos de Outsourcing, que es otra manera de transferir el riesgo.

• Para Reducir: se utilizan los CONTROLES implementados que buscan reducir el impacto o la probabilidad o ambos de que se materialicen los riesgos y que están implementados en cada uno de los procesos.

Sin embargo lo anteriormente expuesto no garantiza que existan suficientes controles o que los controles implementados sean efectivos y que mitigan todos los riesgos. Pero es demostrable que hay implementados controles para mitigar los riesgos en la institución y si se han transferido o compartido riesgos por el mecanismo de Outsourcing y pólizas de seguro, en contraste con la observación del informe que dice que no hay evidencias".
De antemano gracias por la atención a la presente.
Beatriz Stella Restrepo Escobar
Gestor de Riesgos

5.2. Plan de Mejoramiento y Seguimiento.

Una vez en firme, el responsable del proceso auditado, elaborará con su equipo de trabajo la formulación del Plan de Mejoramiento respectivo, en un término de diez (10) hábiles. Los responsables de las actividades del Plan harán el reporte de avance. La Oficina de Auditoría Interna hará seguimiento bimensual del Plan de Mejoramiento y presentará el Informe correspondiente.

5.3. Comunicación y Socialización del Informe Final de Auditoría.

En firme el Informe Final de la Auditoría será socializado en las siguientes instancias, con el fin de que definan las acciones a seguir:

- Comité Coordinador de Control Interno;
- Comité Ampliado de Gerencia; y
- Junta Directiva del Hospital General de Medellín.

De acuerdo a lo dispuesto por el artículo 9° de la Ley 1474 de 2011: "Los informes de los funcionarios de control interno tendrán valor probatorio en los procesos disciplinarios, administrativos, judiciales y fiscales cuando las autoridades pertinentes así lo soliciten".

VI. CONCLUSIONES.

6.1. En el Hospital General de Medellín se tienen levantados los riesgos de 39 procesos con sus respectivos seguimientos, se tiene una apropiada metodología que permite obtener de manera

cuantitativa el riesgo residual, se tiene debidamente documentado con sus respectivos informes de seguimiento el tema de la gestión de riesgos institucional, el cual cuenta con nivel profesional especializado en su manejo.

6.2. Los riesgos extremos deberán ser objeto de un riguroso seguimiento como por ejemplo: envejecimiento de la cartera, incrementos en accidentes laborales, riesgo reputacional, riesgo de pérdida de la acreditación y de hospital universitario, riesgo de pérdida de un bebe, riesgos de demandas, entre otros.

Documento elaborado y revisado por:
Equipo de Trabajo de la **Oficina de Auditoría Interna.**

José Heriberto Vargas Lema	Profesional de Auditoría Interna.
María Janeth Agudelo Arango	Profesional de Auditoría Interna.
Carlos Uriel Lopez Ríos	Jefe de Auditoría Interna.

Medellín, Julio de 2018.