

Nº 13

INFORME DE AUDITORÍA INTERNA 2020

Gestión de Riesgos

Modalidad Auditoría Regular



Informe tipo:

De Auditoría

Noviembre / 2020



Alcaldía de Medellín



INFORME DE AUDITORÍA INTERNA 2020

Gestión de Riesgos

Modalidad Auditoría Regular

Equipo Oficina de Auditoría Interna

Jefe de la Oficina:
Carlos Uriel López Ríos

Auditores:
José Heriberto Vargas Lema
María Janeth Agudelo Arango
Karina Ruíz De la Hoz

Técnico:
Julio E. Suescún Montoya

Correo Oficina:
oficinadeauditoria@hgm.gov.co

Oficina de Auditoría Interna
Hospital General de Medellín
Carrera 48 #32 – 102
PBX: 3847300
Medellín – Antioquia
Colombia
www.hgm.gov.co



Alcaldía de Medellín

CONTENIDO

I. GENERALIDADES.....	5
1.1. Objetivo.....	5
1.2. Alcance.....	5
1.3. Metodología.....	5
1.4. Marco de la Práctica de Auditoría Interna.....	5
1.5. Fundamento Normativo.....	¡Error! Marcador no definido.
1.6. Documentos Base.....	6
1.7. Limitaciones.....	7
1.8. Terminología Básica.....	7
II. RESUMEN EJECUTIVO DE AUDITORÍA.....	9
2.1. Ficha técnica de auditoría.....	9
2.2. Fortalezas.....	9
2.3. Síntesis Observaciones y Recomendaciones.....	10
III. OBSERVACIONES Y RECOMENDACIONES.....	11
3.1. Para mejorar el proceso de Gobierno.....	14
3.2. Para mejorar el proceso de Control.....	16
3.3. Para mejorar el proceso de Riesgos.....	18
IV. VALIDACION CUMPLIMIENTO DEL SISTEMA DE SARLAFT.....	19
V. CONCLUSIONES.....	21
VI. PLAN DE MEJORAMIENTO Y SEGUIMIENTO.....	21
VII. COMUNICACIÓN Y SOCIALIZACIÓN DEL INFORME.....	22

PRESENTACIÓN

La Oficina de Auditoría Interna del Hospital General de Medellín, 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” y en desarrollo del Plan Anual de Auditoría Interna 2020 “**Para agregar Valor**”, nos permitimos presentar el informe de la auditoría realizada a la gestión de riesgos en el Hospital General de Medellín.

El documento se estructura en siete capítulos. En el primero se enuncian las generalidades, que comprende el objetivo, alcance, metodología, fundamento normativo, documentos base y terminología; el segundo contiene el Resumen Ejecutivo. Por su parte, en el tercero se describen y relacionan las observaciones y recomendaciones y en el capítulo cuarto la validación del Sarlaft, en el quinto se presenta las conclusiones. En el sexto se determina la formulación del Plan de Mejoramiento y en el séptimo se enuncia el proceso de comunicación y socialización del Informe.

Para fines de la mejor comprensión, comunicación y resultados de la auditoría, los avances del trabajo fueron puestos en conocimiento y socializados en reunión de cierre con la gestora de riesgos y la jefe de calidad y planeación, quien presentará su posición sobre las valoraciones y observaciones del informe preliminar.

El presente **Informe de Auditoría** se enmarca en la Línea II, Eje I. Aseguramiento y Auditoría Interna Innovadora del Plan Estratégico 2017-2021 “**Construimos Confianza**” de la Oficina de Auditoría Interna, adoptado mediante Acuerdo N° 167 de la Junta Directiva del 21 de septiembre de 2017.

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.

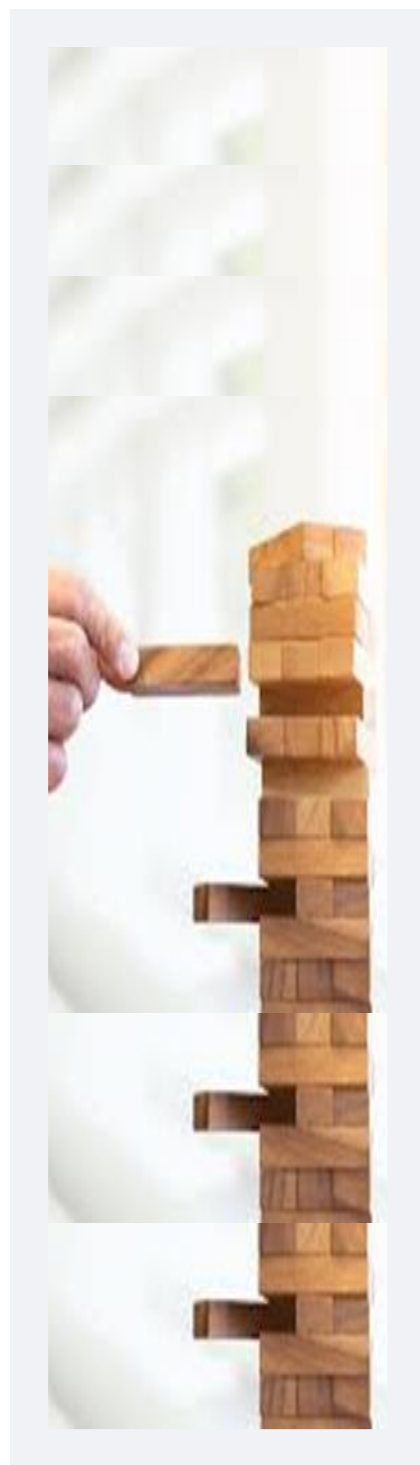
Agradecemos a los servidores de la Entidad que intervinieron en la ejecución de la auditoría por la colaboración prestada en el suministro de la información requerida y su disposición para la mejora continua de los procesos institucionales.

Oficina de Auditoría Interna.

Construimos Confianza

Hospital General de Medellín.

Atención Excelente y Calidad de Vida.



I. GENERALIDADES.

1.1. Objetivo.

Realizar evaluación al programa de Gestión de Riesgos, con el fin de verificar la conformidad con los requisitos legales, identificando oportunidades de mejora que contribuyan al mejoramiento del sistema de gestión del proceso y su desempeño en el gobierno, los controles y los riesgos.

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.

1.3. Metodología.

1.3.1. Interacción con líderes del universo de auditoría.

- Realización de reunión de apertura de la auditoría, para socializar el Programa Específico de Auditoría-PEA y formalizar la Carta de Representación de Auditoría Interna.
- Indagación preliminar con el líder del programa de riesgos.
- Entrevista con funcionarios relacionados con la gestión de riesgos.
- Reunión de cierre para socializar y formalizar Informe de Auditoría.

1.3.2. Revisión y análisis documental.

- Revisión y análisis de la información.
- Revisión de carpetas con soportes e informes generados.
- Identificación de las observaciones y formulación de las recomendaciones de la auditoría.
- Revisión de la información del avance del plan de mejoramiento de la auditoría anterior.

1.3.3. Verificación de gobierno, riesgos y control.

- Revisión de los indicadores de gestión, la matriz de riesgos y de controles.
- Aplicación de cuestionario y listas de chequeos.
- Identificación de los controles claves del proceso.
- Definición de las pruebas a realizar y muestras objeto de evaluación, junto con los requerimientos de información
- Verificación de las evidencias.

1.3.4. Preparación y socialización de los resultados de Auditoría.

- Elaboración de Informe Preliminar de Auditoría.
- Envío del Informe Preliminar y posterior socialización.
- Elaboración del Informe Final de Auditoría.
- Elaboración Plan de Mejoramiento de Auditoría Interna - PMAIN.
- Seguimiento al Plan de Mejoramiento de Auditoría Interna - PMAIN.

1.4. Marco de la Práctica de Auditoría Interna.

La Oficina de Auditoría Interna del HGM evalúa y contribuye a la mejora de los procesos de Gobierno, Gestión de riesgos y Control de la organización, utilizando un enfoque sistemático, disciplinado y basado en riesgos; todo ello en cumplimiento de las mejores prácticas internacionales.

1.4.1. Norma Internacional de Auditoría 2110 – Gobierno.

La auditoría interna debe evaluar y hacer recomendaciones apropiadas para mejorar el proceso de gobierno de la organización para:

- Tomar decisiones estratégicas y operativas.
- Supervisar la gestión de riesgos y el control.
- Promover la ética y los valores apropiados dentro de la organización.
- Asegurar la gestión y responsabilidad eficaces en el desempeño de la organización.
- Comunicar la información de riesgo y control a las áreas adecuadas de la organización.
- Coordinar las actividades y la información de comunicación entre el Consejo de Administración, los auditores internos y externos, otros proveedores de aseguramiento y la Dirección.

Fuente: Marco Internacional para la Práctica Profesional de la Auditoría Interna. IIA. Enero 2017.

1.4.2. Norma Internacional de Auditoría 2120 – Gestión de Riesgos.

La auditoría interna debe evaluar la eficacia y contribuir a la mejora de procesos de gestión de riesgos, con relación a lo siguiente (Norma 2120.A1):

- El logro de los objetivos estratégicos de la organización.
- La fiabilidad y la integridad de la información financiera y operativa.
- La efectividad y la eficiencia de las operaciones y de los programas.
- La protección de los activos, y
- Cumplimiento de las leyes, regulaciones, políticas, procedimientos y contratos.

Fuente: Marco Internacional para la Práctica Profesional de la Auditoría Interna. IIA. Enero 2017.

1.4.3. Norma Internacional de Auditoría 2130 – Control.

La auditoría interna debe asistir a la organización en el mantenimiento de controles efectivos, mediante la evaluación de la efectividad y la eficacia de los mismos y promoviendo la mejora continua.

Fuente: Marco Internacional para la Práctica Profesional de la Auditoría Interna. Enero 2017.

1.4.4. Instrumentos de Auditoría Interna.

Para el desarrollo de su actividad la Oficina de Auditoría Interna del Hospital General de Medellín cuenta con los siguientes Instrumentos de Auditoría Interna:

- EV-EVC-AI001D01 - Código de Ética de Auditoría Interna.
- EV-EVC-AI001D02 - Estatuto de Auditoría Interna.
- EV-EVC-AI001D03 - Carta de Representación de Auditoría Interna.
- EV-EVC-AI001D04 - Programa de Aseguramiento y Mejora de Auditoría Interna.
- EV-EVC-AI001D05 - Directriz de Auditoría Interna.
- EV-EVC-AI001M01 - Manual de Auditoría Interna HGM.
- EV-EVC-AI001D06 - Medición Percepción Gestión Ética HGM.

Fuente: Mapa de Procesos – Hospital General de Medellín.

1.5. Fundamento Normativo.

1.5.1. 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 Sistema de Control Interno: a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten; 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 sus objetivos;

- 1.5.2. Decreto Nacional 648 de abril de 2017 de la Presidencia de la República.
Modifica y adiciona el Decreto Nacional 1083 de 2015. Reglamentario del sector de Función Pública.

Art. 17. El Artículo 2.2.21.5.3 del Decreto 1083 de 2015, quedará así: "Las Unidades u Oficinas de Control Interno desarrollarán su labor a través de los siguientes roles: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, y relación con entes externos de control."

- 1.5.3. Ley 1474 de 2011 de la Presidencia de la República.
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.

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

- 1.5.5. Decreto 1499 del 11 de septiembre de 2017 de la Presidencia de la Republica.
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".

1.6. Documentos Base.

- 1.6.1. Política de la Gestión de Riesgos del HGM.
- 1.6.2. Manual del Sistema de Gestión Integral de Riesgos.
- 1.6.3. Formato Matriz de Riesgos.
- 1.6.4. Instructivo para la Administración de Riesgos en el HGM.
- 1.6.5. Mapa de Riesgos Institucional.
- 1.6.6. Instrumento índice de Madurez de Riesgos.

1.7. Limitaciones

Los profesionales y el responsable del proceso que fueron citados atendieron de manera oportuna y diligente los requerimientos de la auditoría entregando la información solicitada. La auditoría no registró ninguna limitación.

1.8. Terminología básica.

▫ **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.

▫ **Control del riesgo de LA/FT.**

Comprende la implementación de políticas, procesos, prácticas u otras acciones existentes que actúan para minimizar el riesgo de LA/FT en las operaciones, negocios o contratos que realice la entidad.

▫ **Debida Diligencia.**

Equivala a ejecutar algo con suficiente cuidado. Existen dos interpretaciones sobre la utilización de este concepto en la actividad empresarial. La primera, se concibe como actuar con el cuidado que sea necesario para evitar la posibilidad de llegar a ser considerado culpable por negligencia y de incurrir en las respectivas responsabilidades administrativas, civiles o penales. La segunda, de contenido económico y proactiva, se identifica como el conjunto de procesos necesarios para poder adoptar decisiones suficientemente informadas.

▫ **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.

▫ **Herramientas de Sarlaft.**

Son los medios que utiliza la entidad para prevenir que se presente el riesgo de LA/FT y para detectar operaciones intentadas, inusuales o sospechosas. Dentro de dichas herramientas se deben mencionar, entre otras, las señales de alerta, indicadores de operaciones inusuales, programas para administración de riesgos empresariales y hojas electrónicas de control.

▫ **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.

▫ **Oficial de Cumplimiento.**

El Oficial de Cumplimiento, o máxima persona encargada del cumplimiento del Sarlaft, es un funcionario de la entidad vigilada encargado de verificar el cumplimiento de los manuales y políticas de procedimiento de la entidad, así como de la implementación del Sarlaft.

▫ **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 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 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 Inherente.**

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

▫ **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.

II. RESUMEN EJECUTIVO DE AUDITORÍA.

2.1. Ficha técnica de auditoría.

HOSPITAL GENERAL DE MEDELLÍN Oficina de Auditoría Interna Auditoría Gestión de Riesgos			
Ficha Técnica			
Asunto:	Auditoría al Programa de Gestión de Riesgos		
Entidad:	Hospital General de Medellín Luz Castro de Gutiérrez ESE.		
Dependencia:	Oficina de Auditoría Interna		
Auditor Líder:	José Heriberto Vargas Lema		
Líder del proceso	Dra. Yudy Alejandra Cadavid Londoño - Jefe Calidad y Planeación Dra. Katherine Madrid Restrepo - Profesional Gestora de Riesgos		
Fecha:	Octubre de 2020		

Cuadro N° 1. Ficha técnica de auditoría.

2.2. Fortalezas.


Dentro del ejercicio auditor se identificaron las siguientes fortalezas:

- De manera general se resalta la disposición del equipo auditado en la atención de la auditoría y se evidencia buen conocimiento tanto del proceso auditado como de las diferentes normas aplicables.
- La auditoría destaca la disposición de los auditados para interactuar con el equipo de auditoría y formular el plan de mejoramiento respectivo.
- El nombre del proyecto estratégico fue renombrado así: “Implementar un sistema de gestión integral de Riesgo del HGM, adoptando lineamientos del Modelo Integrado de Planeación y Gestión definidos por el DAFP.”, el cual fue debidamente aprobado por la Junta Directiva.
- Se inició un enfoque de implementación del Sistema Gestión Integral del Riesgo, desde la política de planeación integrando la política de gestión de riesgos, los procedimientos, Sarlaf, riesgos de corrupción, manual de riesgos, gestores de riesgos, programa de seguridad del paciente, programa de gestión de tecnología, programa de cultura organizacional y responsabilidad social.
- Se realizaron durante el año 2020, un total de 33 despliegues virtuales del enfoque del SGIR con un total de 279 participantes.
- Se realizó un curso virtual de riesgos con el CES con el cual se certificaron 50 participantes.

- Adicional a los riesgos operativos de cada proceso se dio inicio a la inclusión en las respectivas matrices de riesgos los de seguridad digital, gestión ambiental, seguridad y salud en el trabajo, lavados de activos, riesgos de corrupción, jurídicos, estratégicos y reputacionales.
- Teniendo en cuenta los lineamientos del MIPG Se construye la Política de Planeación, de ésta se desprenden las demás políticas entre ellas la Política Riesgos.
- Se realizaron ajustes a la Política de Riesgos teniendo en cuenta el Modelo Integrado de Planeación y Gestión (MIPG).
- Se construyó el Manual de Riesgos adoptando la metodología del DAFP.
- Se conformó el grupo de gestores de riesgos, uno para cada proceso que fue seleccionado por el director o líder del proceso.
- Se identificaron los riesgos de contratación, los riesgos estratégicos, los riesgos reputacionales, los riesgos generados por el Covid 19.

2.3. Síntesis Observaciones y Recomendaciones.

Como resultado de la verificación y evaluación al proceso de gestión de Riesgos, se identificaron observaciones para fortalecer el control interno, frente a lo cual y después de los análisis de Auditoría Interna se destacan las siguientes observaciones y recomendaciones:

HOSPITAL GENERAL DE MEDELLÍN Oficina de Auditoría Interna Observaciones y Recomendaciones		 	
#Id	Descripción	Cantidad	
1	Observaciones	5	100%
	<i>En el Proceso de Gobierno</i>	2	40%
	<i>En el Proceso de Control</i>	2	40%
	<i>En el Proceso de Riesgos</i>	1	20%
2	Recomendaciones	45	100%
	<i>Para Mejorar el Gobierno</i>	21	47%
	<i>Para Mejorar el Control</i>	15	33%
	<i>Para Mejorar la gestión de Riesgos</i>	9	20%

Cuadro N° 2. Observaciones y Recomendaciones - Síntesis.

OFICINA DE AUDITORÍA INTERNA Auditoría Gestión de Riesgos Observaciones y Recomendaciones		
N°	Observaciones	Recomendaciones
1	<p>La metodología de medición de la madurez de la gestión de riesgos para ISO 31.000, para el año 2019 dio un resultado de 3.2 en una escala de 1.0 a 5.0, resultado que corresponde a un criterio de cumplimiento de Básico – táctico.</p> <p>Al momento de la auditoría se observa que para el año 2020, aún no se ha aplicado la metodología para medir el índice de madurez de riesgos.</p>	<ol style="list-style-type: none"> 1.1. Fortalecer la Gestión del Riesgo como parte integral de todos los procesos del Hospital. 1.2. Continuar el enfoque estructurado y exhaustivo de la Gestión del Riesgo que contribuya a los resultados coherentes y compatibles del Hospital. 1.3. Adaptar la Gestión de Riesgos a los contextos externo e interno del Hospital. 1.4. La Gestión del Riesgo se deberá anticipar, detectar, reconocer y responder a los cambios interno y externo de la organización de manera apropiada y oportuna. 1.5. La Alta Dirección deberá comunicar el valor de la Gestión del Riesgo a la organización y sus partes interesadas. 1.6. La Alta Dirección deberá asegurar que se asignen los recursos necesarios para la gestión del riesgo, en lo posible con asignación de recursos presupuestales propios al programa. 1.7. Fortalecer la integración de la gestión del riesgo en el Hospital como un proceso dinámico e iterativo adaptado a las necesidades y a la cultura organizacional. 1.8. Generar estrategias para integrar la gestión del riesgo como parte de todo el gobierno corporativo, el liderazgo, el compromiso, la estrategia, los objetivos estratégicos y la operación. 1.9. Dar a conocer a todas las partes interesadas la naturaleza y el nivel de riesgo residual después del tratamiento. 1.10. Documentar y ser objeto de seguimiento y revisión el riesgo residual. 1.11. Los planes de tratamiento del riesgo se deberán integrar al proceso de gestión del riesgo. 1.12. El plan de tratamiento de riesgo deberá incluir, entre otros los siguientes aspectos: a) El fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados. b) Las personas que rinden cuentas y aquellas responsables de la aprobación y la implementación del plan. c) Las acciones propuestas, d) Los recursos necesarios, incluyendo las consecuencias, e) Las medidas del desempeño, f) Las restricciones, g) Los informes y seguimientos requeridos, h) Los plazos previstos para la realización y finalización de las acciones. 1.13. Aplicar instrumento del índice de madurez de riesgos para la vigencia 2020.
2	<p>La auditoría observa que la política de gestión de riesgos aún no está evaluada para la vigencia 2020, ni desplegada a todos los niveles de la organización y no se tiene un seguimiento al cumplimiento de ésta, y a todas las partes interesadas, adicionalmente se observa que está pendiente la identificación de riesgos del área de compras y suministros y los contratos y órdenes de prestación de servicios.</p> <p>La auditoría observa que no se encuentra aprobada formalmente la Política de Planeación, ni el Comité de Gestores de Riesgos, ni la política de transparencia y acceso a la información pública, y lucha contra la corrupción.</p> <p>Adicionalmente no se ha definido el perfil de riesgos institucional para la vigencia 2020 y se encuentra pendiente ajustar la Política de Riesgos describiendo claramente la segregación de funciones de las tres líneas de defensa.</p>	<ol style="list-style-type: none"> 2.1. Comunicación y reporte de riesgos del programa de gestión de riesgos a todas las partes interesadas. 2.2. Rendición de cuentas basada en riesgos, seguimiento a riesgos en la evaluación del plan de acción y en el informe gerencial e informes a la Junta Directiva. 2.3. Integrar el programa de Gestión de Riesgos al modelo de mejoramiento institucional. 2.4. Continuar integrando los riesgos institucionales tal cual lo propone el programa de gestión integral de riesgos, los riesgos ocupacionales, ambientales, clínicos, de corrupción, de fraude, tecnológicos y seguridad de la información. 2.5. Generar acciones encaminadas a prevenir la materialización de riesgos, especialmente aquellos riesgos críticos de la institución, acciones para reducir o compartir el riesgo y definir el apetito de Riesgo en la institución. 2.6. Aprobar la política de planeación. 2.7. Aprobar el comité de gestores de riesgos. 2.8. Construir la política de transparencia y acceso a la información pública.

3	<p>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 direcciona 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.</p>	<p>3.1. Revisar y actualizar los controles que aseguren una adecuada gestión de los procesos.</p> <p>3.2. Identificar y hacer seguimiento de riesgos a los proyectos institucionales.</p> <p>3.3. Para los riesgos estratégicos y claves de la Institución asegurar su monitoreo permanente para revisar la efectividad de los controles establecidos. Adicionalmente hacer seguimiento a los riesgos calificados como extremos.</p> <p>3.4. Los riesgos estratégicos y los calificados como extremos debe estar identificada su afectación a los objetivos estratégicos.</p> <p>3.5. Revisar los riesgos de los servicios habilitados.</p> <p>3.6. Integrar y correlacionar el programa de seguridad del paciente con el sistema de gestión integral de riesgos en lo que corresponde con riesgos clínicos.</p> <p>3.7. Fortalecer la identificación de los riesgos de fraude en la institución.</p>
4	<p>Observa la auditoría que aún no se ha definido el formato para documentar la materialización de los riesgos, para asegurar su control y monitoreo, para el conocimiento del gestor de riesgos, asegurando un registro en la materialización de los riesgos.</p> <p>Adicionalmente es necesario para un efectivo desarrollo del Programa de Gestión Integral de Riesgos mantener un proceso continuo que fluya por toda la entidad, que sea desarrollado por todos los servidores, aplicado sobre las estrategias organizacionales. Identificar los riesgos de fraude y sobre este asegurar un monitoreo periódico</p>	<p>4.1. Generar capacidades al grupo de gestores de calidad en el tema de gestión de riesgos.</p> <p>4.2. Formalizar la creación del Comité de Riesgos.</p> <p>4.3. Registrar la materialización de los riesgos y llevar datos estadísticos de éstos.</p> <p>4.4. Vincular los planes de contingencia con el programa de Gestión Integral de Riesgos.</p> <p>4.5. Definir para la institución el apetito del riesgo.</p> <p>4.6. 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).</p> <p>4.7. Asegurar un plan de capacitación y entrenamiento continuo sobre gestión de riesgos, en los diferentes niveles de la organización.</p> <p>4.8. Identificar las áreas o procesos con mayor vulnerabilidad.</p>
5	<p>La Oficina de Planeación como segunda línea de defensa deberá consolidar periódicamente la información de gestión de riesgos para darla a conocer a la alta Dirección, quienes deben analizar los resultados y en especial considerar la evaluación sobre los riesgos materializados. Sobre éstos se deberá definir planes de acción o de intervención para actualizar los mapas de riesgos.</p> <p>Adicionalmente se observa que no se están llevando a cabo seguimientos a las acciones definidas para resolver materialización de riesgos detectados. Igualmente, la alta dirección debe monitorear los riesgos de corrupción con la periodicidad establecida en la política de riesgos.</p> <p>Un riesgo importante al cual no se tiene evidencia o registro de seguimiento es el que se refiere a la segregación de funciones. Toda transacción en el Hospital General de Medellín pasa por las fases de registro, autorización, aprobación y ejecución; sin embargo, es necesario realizar la revisión completa de las segregación de funciones en cuanto a perfiles de SAP identificando las transacciones autorizadas por usuario; esta actividad se deberá coordinar entre el proceso de gestión humana y el área de sistemas.</p> <p>Las actividades tercerizadas no tienen elaboradas matrices de riesgos, que permitan su monitoreo y seguimiento periódico.</p> <p>La auditoría observa que no se evidencia debidamente documentados y socializados el análisis del impacto en los cambios organizacionales. Se deberá fortalecer el programa de gestión de cambios institucional.</p>	<p>5.1. Generar información periódica de riesgos para la Alta Dirección, éstos deberán analizar los resultados y evaluarán los riesgos materializados.</p> <p>5.2. Realizar seguimiento a las acciones definidas a la materialización de riesgos materializados.</p> <p>5.3. Realizar evaluación al riesgo de segregación de funciones en la institución.</p> <p>5.4. Realizar evaluación a los riesgos financieros de la institución.</p> <p>5.5. Realizar evaluación a los riesgos reputacionales de la institución.</p> <p>5.6. Levantar las matrices de riesgos de las actividades tercerizadas y asegurar un seguimiento periódico.</p> <p>5.7. Monitorear los riesgos aceptados.</p> <p>5.8. Realizar evaluación de fallas en los controles.</p> <p>5.9. Fortalecer el programa de gestión de cambios en el hospital.</p>

Cuadro N° 3. Observaciones y recomendaciones.

III. OBSERVACIONES Y RECOMENDACIONES.

Como resultado de la auditoría realizada se identificaron oportunidades de mejoramiento en las actividades de control, que podrían posibilitar la materialización de los riesgos definidos, y los cuales se encuentran asociados con la documentación y cumplimiento de los controles. A continuación, se presentan las observaciones con recomendaciones:

3.1. Para mejorar el proceso de Gobierno.

Observación de Auditoría Interna N° 1.

a. Descripción.

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.

La metodología de medición de la madurez de la gestión de riesgos para ISO 31.000, para el año 2019 dio un resultado de 3.2 en una escala de 1.0 a 5.0, resultado que corresponde a un criterio de cumplimiento de Básico – táctico.

Al momento de la auditoría se observa que para el año 2020, aún no se ha aplicado la metodología para medir el índice de madurez de riesgos. Este nivel de madurez básico tiene las siguientes características:

- Los procedimientos del Sistema de Gestión de Riesgos están documentados, pero se ejecutan en la operación diaria de manera irregular y poco sistemática.
- El seguimiento de los procedimientos depende de la iniciativa de cada individuo y es poco probable que las posibles no conformidades sean detectadas.
- Débil funcionamiento del SGR.
- Uso de la automatización y herramienta de una manera limitada o fragmentada.

b. Criterios.

La tabla que orienta la calificación en la metodología para ISO 31.000 es la siguiente:

Criterios de Calificación del SGR:	Entre	
Efectivo	4.1	5.0
Cumplimiento Básico - Táctico	3.1	4.0
En Proceso	2.1	3.0
Crítico y Reactivo	1.1	2.0

c. 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.

d. Recomendación.

- Fortalecer la Gestión del Riesgo como parte integral de todos los procesos del Hospital.
- Continuar con el enfoque estructurado y exhaustivo a la Gestión del Riesgo que contribuya a los resultados coherentes y compatibles del Hospital.
- Adaptar la Gestión de Riesgos a los contextos externo e interno del Hospital.
- La Gestión del Riesgo se deberá anticipar, detectar, reconocer y responder a los cambios interno y externo de la organización de manera apropiada y oportuna.
- La Alta Dirección deberá comunicar el valor de la Gestión del Riesgo a la organización y sus partes interesadas.
- La Alta Dirección deberá asegurar que se asignen los recursos necesarios para la gestión del riesgo, en lo posible con asignación de recursos presupuestales propios al programa.

- Fortalecer la integración de la gestión del riesgo en el Hospital como un proceso dinámico e iterativo adaptado a las necesidades y a la cultura organizacional.
- Generar estrategias para integrar la gestión del riesgo como parte de todo el gobierno corporativo, el liderazgo, el compromiso, la estrategia, los objetivos estratégicos y la operación.
- Dar a conocer a todas las partes interesadas la naturaleza y el nivel de riesgo residual después del tratamiento.
- Documentar y ser objeto de seguimiento y revisión el riesgo residual.
- Los planes de tratamiento del riesgo se deberán integrar al proceso de gestión del riesgo.
- El plan de tratamiento de riesgo deberá incluir, entre otros los siguientes aspectos: a) El fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados. b) Las personas que rinden cuentas y aquellas responsables de la aprobación y la implementación del plan. c) Las acciones propuestas, d) Los recursos necesarios, incluyendo las consecuencias, e) Las medidas del desempeño, f) Las restricciones, g) Los informes y seguimientos requeridos, h) Los plazos previstos para la realización y finalización de las acciones.
- Aplicar instrumento del índice de madurez de riesgos para la vigencia 2020.

e. Posición del auditado.

Escribir aquí:

f. Plan de mejoramiento.

Observación de Auditoría Interna N° 2.

a. Descripción.

La auditoría observa que la política de gestión de riesgos aún no está evaluada para la vigencia 2020, ni desplegada a todos los niveles de la organización y no se tiene un seguimiento al cumplimiento de ésta, y a todas las partes interesadas, adicionalmente se observa que está pendiente la identificación de riesgos del área de compras y suministros y los contratos y órdenes de prestación de servicios.

La auditoría observa que no se encuentra aprobada formalmente la Política de Planeación, ni el Comité de Gestores de Riesgos, ni la política de transparencia y acceso a la información pública, y lucha contra la corrupción.

Adicionalmente no se ha definido el perfil de riesgos institucional para la vigencia 2020 y se encuentra pendiente ajustar la Política de Riesgos describiendo claramente la segregación de funciones de las tres líneas de defensa.

b. Criterios.

- Manual del Sistema de Gestión Integral de Riesgos. Código ES-PLI-GP006M01

c. Riesgo.

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

d. Recomendación.

- Comunicación y reporte de riesgos del programa de gestión de riesgos a todas las partes interesadas.
- Rendición de cuentas basada en riesgos, seguimiento a riesgos en la evaluación del plan de acción y en el informe gerencial e informes a la Junta Directiva.
- Integrar el programa de Gestión de Riesgos al modelo de mejoramiento institucional.
- Continuar integrando los riesgos institucionales tal cual lo propone el programa de gestión integral de riesgos, los riesgos ocupacionales, ambientales, clínicos, de corrupción, de fraude, tecnológicos y seguridad de la información.
- Generar acciones encaminadas a prevenir la materialización de riesgos, especialmente aquellos riesgos críticos de la institución, acciones para reducir o compartir el riesgo y definir el apetito de Riesgo en la institución.

- Aprobar la política de planeación.
- Aprobar el Comité de Gestores de Riesgos.
- Construir la política de transparencia y acceso a la información pública.

e. Posición del auditado.

Escribir aquí:


f. Plan de mejoramiento.

3.2. Para mejorar el proceso de Control.

Observación de Auditoría Interna N° 3.

a. Descripción.

Se tiene un mapa de riesgos institucional sin variación del año 2018 al año 2019, construido con las matrices de riesgo de los 39 procesos institucionales. El mapa de riesgos año 2020 se encuentra en proceso de construcción dado que los procesos están actualizando sus riesgos. Se observan identificados 197 riesgos en los procesos, así:

HOSPITAL GENERAL DE MEDELLÍN Oficina de Auditoría Interna Mapa de Riesgos					
AÑO	ZONA DE RIESGO EXTREMO	ZONA DE RIESGO ALTO	ZONA DE RIESGO MODERADO	ZONA DE RIESGO BAJO	TOTAL RIESGOS
2016	14	74	64	53	205
2017	10	71	88	32	201
2018	14	70	83	30	197
2019	14	71	83	29	197

Cuadro N° 5 Mapa de Riesgos

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 direcciona 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.

b. Criterios.

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

c. Riesgo.

- Ausencia de controles para una adecuada gestión del Programa de Gestión de Riesgos.

d. Recomendación.

- Revisar y actualizar los controles que aseguren una adecuada gestión de los procesos.
- Identificar y hacer seguimiento de riesgos a los proyectos institucionales.
- Para los riesgos estratégicos y claves de la Institución 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.
 - Revisar los riesgos de los servicios habilitados.
 - Integrar y correlacionar el programa de seguridad del paciente con el sistema de gestión integral de riesgos en lo que corresponde con riesgos clínicos.
 - Fortalecer la identificación de los riesgos de fraude en la institución.
- e. Posición del auditado.**
Escribir aquí:
- f. Plan de mejoramiento.**

Observación de Auditoría Interna N° 4.

a. Descripción.

Observa la auditoría que aún no se ha definido el formato para documentar la materialización de los riesgos, para asegurar su control y monitoreo, para el conocimiento del gestor de riesgos, asegurando un registro en la materialización de los riesgos.

Adicionalmente es necesario para un efectivo desarrollo del Programa de Gestión Integral de Riesgos mantener un proceso continuo que fluya por toda la entidad, que sea desarrollado por todos los servidores, aplicado sobre las estrategias organizacionales. Identificar los riesgos de fraude y sobre este asegurar un monitoreo periódico.

b. Criterios.

- Decreto 1499 de 2017 Modelo Integrado de Planeación y Gestión (MIPG),

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.

c. Riesgo.

- Ausencia de controles para una adecuada gestión del Programa de Gestión de Riesgos.

d. Recomendación.

- Generar capacidades al grupo de gestores de calidad en el tema de gestión de riesgos.
- Formalizar la creación del comité de Riesgos.
- Registrar la materialización de los riesgos y llevar datos estadísticos de éstos.
- Vincular los planes de contingencia con el programa de Gestión Integral de Riesgos.
- Definir para la institución el apetito del riesgo.
- 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).
- Asegurar un plan de capacitación y entrenamiento continuo sobre gestión de riesgos, en los diferentes niveles de la organización.
- Identificar las áreas o procesos con mayor vulnerabilidad.

e. Posición del auditado.

Escribir aquí:

f. Plan de mejoramiento.

3.3. Para mejorar el proceso de Riesgos.

Observación de Auditoría Interna N° 5.

a. Descripción.

De acuerdo con la evaluación semestral del Sistema Institucional de Control Interno, la auditoría observa que es necesario fortalecer las siguientes actividades de Gestión de Riesgos:

La Oficina de Planeación como segunda línea de defensa deberá consolidar periódicamente la información de gestión de riesgos para darla a conocer a la alta Dirección, quienes deben analizar los resultados y en especial considerar la evaluación sobre los riesgos materializados. Sobre éstos se deberá definir planes de acción o de intervención para actualizar los mapas de riesgos.

Adicionalmente se observa que no se están llevando a cabo seguimientos a las acciones definidas para resolver materialización de riesgos detectados. Igualmente, la alta dirección debe monitorear los riesgos de corrupción con la periodicidad establecida en la política de riesgos.

Un riesgo importante al cual no se tiene evidencia o registro de seguimiento es el que se refiere a la segregación de funciones. Toda transacción en el Hospital General de Medellín pasa por las fases de registro, autorización, aprobación y ejecución; sin embargo, es necesario realizar la revisión completa de las segregación de funciones en cuanto a perfiles de SAP identificando las transacciones autorizadas por usuario; esta actividad se deberá coordinar entre el proceso de gestión humana y el área de sistemas.

Las actividades tercerizadas no tienen elaboradas matrices de riesgos, que permitan su monitoreo y seguimiento periódico.

Adicionalmente la alta Dirección no monitorea los riesgos aceptados revisando que sus condiciones no hayan cambiado para definir su pertinencia para sostenerlos o ajustarlos, tampoco hay evidencia de la evaluación de fallas en los controles para definir cursos de acción.

La auditoría observa que no se evidencia debidamente documentados y socializados el análisis del impacto en los cambios organizacionales. Se deberá fortalecer el programa de gestión de cambios institucional.

b. Criterios.

- Matriz de evaluación del Sistema de Control Interno.

c. Riesgo.

Bajo cumplimiento del estado del Sistema de Control Interno.

d. Recomendación.

- Generar información periódica de riesgos para la Alta Dirección, éstos deberán analizar los resultados y evaluarán los riesgos materializados.
- Realizar seguimiento a las acciones definidas a la materialización de riesgos materializados.
- Realizar evaluación al riesgo de segregación de funciones en la institución.
- Realizar evaluación a los riesgos financieros de la institución.
- Realizar evaluación a los riesgos reputacionales de la institución.
- Levantar las matrices de riesgos de las actividades tercerizadas y asegurar un seguimiento periódico.
- Monitorear los riesgos aceptados.
- Realizar evaluación de fallas en los controles.
- Fortalecer el programa de gestión de cambios en el hospital.

e. Posición del auditado.

Escribir aquí:

f. Plan de mejoramiento.

IV. VALIDACIÓN CUMPLIMIENTO DEL SARLAFT.

La auditoría ha validado el cumplimiento de la Circular 000009 del 21 de abril de 2016 de la Superintendencia Nacional de Salud, en la cual imparte instrucciones frente al Sistema de Administración de Riesgos y Lavado de Activos (SARLAFT), encontrando que se viene dando cumplimiento en el diseño e implementación del Sarlaft de acuerdo con los criterios y parámetros mínimos exigidos en la circular y de conformidad con estándares internacionales definiendo procedimientos y metodologías para que el hospital evite ser utilizado para el lavado de activos.

Se vienen tomando las medidas necesarias para controlar el riesgo inherente, en razón de los factores de riesgo y de los riesgos asociados. Para ello se ha establecido las metodologías para definir las medidas de control del riesgo de LA/FT, los niveles de exposición y efectuar los Reportes de Operaciones Sospechosas (ROS) a la UIAF. Está en proceso de establecer el perfil de riesgo residual de LA/ FT. Y realizar seguimiento y monitoreo a estos riesgos.

Se valida el diseño de políticas y procedimientos debidamente aprobados y comunicados, se recomienda que una vez identificadas las situaciones que puedan generarle riesgo de LA/FT según las fuentes de riesgo, el Oficial de Cumplimiento debe elaborar una relación y dejar documentado el análisis de cada una, con el fin de implementar los controles necesarios y facilitar su seguimiento.

Asimismo, cuando el Hospital involucre nuevos mercados u ofrezca nuevos servicios, el Oficial de Cumplimiento deberá evaluar el riesgo de LA/FT que implica, dejando constancia de este análisis, adicionalmente se debe verificar los antecedentes de los empleados y proveedores antes de su vinculación y realizar por lo menos una actualización anual de sus datos. Cuando se detecten comportamientos inusuales en cualquier persona que labore o tenga contacto con la entidad, se debe analizar tal conducta.

Determinar el monto máximo de efectivo que puede manejarse al interior de la entidad por tipo de cliente/usuario

Dentro del Sistema de Administración de Riesgos de Lavado de Activos la Junta Directiva viene cumpliendo sus funciones estableciendo las políticas para la prevención y control del riesgo de LA/FT, aprobando manual de procedimientos y sus actualizaciones garantizando los recursos técnicos y humanos que se requieren para mantener en funcionamiento el Sarlaft, adicionalmente se requiere una adecuación al sistema de información SAP para ingresar variables para la segmentación.

La Junta Directiva tiene designado un Oficial de cumplimiento que cuenta con suplente, por lo que la Auditoría recomienda su creación como una buena práctica ya que, ante la ausencia temporal del titular de Oficial de Cumplimiento, no se cuenta con persona que pueda asumir sus funciones.

El Oficial de Cumplimiento demanda de ciertos requisitos para ejercer, como son: 1) Que el Oficial de Cumplimiento tanto titular como suplente, son nombrados por la Junta Directiva o el Órgano Social que haga sus veces. De tal forma, que, ante la ausencia del Oficial Principal, no puede ser reemplazado sino, por quien dicho Órgano decida y nombre y se lo hayan informado a la Supersalud, para que administre las claves y es el designado para reportar a la SNS y a la UIAF toda la información. El suplente debe cumplir con todos los requisitos del titular, con excepción al de pertenecer como mínimo, al segundo nivel jerárquico de la estructura organizacional.

La Junta Directiva garantiza la inclusión en sus reuniones periódicas del informe del Oficial de cumplimiento.

Dentro de las funciones del Oficial de cumplimiento se ha recomendado Analizar los informes presentados por la auditoría interna y los informes que presente el Revisor Fiscal para que sirvan como insumo para la formulación de planes de acción para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas de Sarlaft.

La Revisoría Fiscal deberá dar cuenta por escrito cuando menos, de forma anual a la Junta Directiva y al representante legal, del cumplimiento o incumplimiento a las disposiciones contenidas en el Sarlaft. De igual forma, deberá poner en conocimiento del Oficial de Cumplimiento, las inconsistencias y falencias que detecte respecto a la implementación del Sarlaft o de los controles establecidos.

Adicionalmente la Revisoría Fiscal, deberá rendir los informes que, sobre el cumplimiento a las disposiciones contenidas en esta Circular, le solicite la Superintendencia Nacional de Salud.

Se debe programar y coordinar planes de capacitación como mínimo una vez al año a todas las áreas y funcionarios de la entidad sobre las políticas, procedimientos, herramientas y controles adoptados para dar cumplimiento al Sarlaft. Como resultado de esta capacitación, el personal debe estar en la capacidad como mínimo de identificar cuándo una operación es intentada, inusual o sospechosa, cuándo debe reportarse, el medio para hacerlo y a quién.

La capacitación debe ser considerada en los procesos de inducción de los nuevos empleados. Se debe dejar constancia de las capacitaciones realizadas, donde se indique como mínimo la fecha, el tema tratado y el nombre de los asistentes.

RECOMENDACIONES:

1. Establecer el perfil de riesgo residual de LA/ FT, y realizar seguimiento y monitoreo a estos riesgos.
2. Elaborar una relación de los riesgos de lavado de activos y dejar documentado el análisis de cada uno, con el fin de implementar los controles necesarios y facilitar su seguimiento.
3. Evaluar el riesgo de LA/FT cuando se tengan nuevos mercados u ofrezca nuevos servicios, dejando constancia de este análisis.
4. Determinar el monto máximo de efectivo que puede manejarse al interior de la entidad por tipo de cliente/usuario.
5. Nombramiento de un oficial de cumplimiento Suplente, ya que como una buena práctica ya que ante la ausencia temporal del Oficial de Cumplimiento, no podrá asumir las funciones una persona que reemplace su cargo que no cumpla requisitos.
6. Analizar los informes presentados por la auditoría interna y los informes que presente el Revisor Fiscal.
7. La Revisoría Fiscal deberá dar cuenta por escrito cuando menos, de forma anual a la Junta Directiva y al representante legal, del cumplimiento del Sarlaft.
8. Programar y coordinar planes de capacitación como mínimo una vez al año a todas las áreas y funcionarios de la entidad sobre las políticas, procedimientos, herramientas y controles adoptados para dar cumplimiento al Sarlaft.
9. Actualizar las bases de datos de contrapartes, clientes, proveedores, colaboradores y entidades responsables de pago para determinar el proceso de segmentación.
10. Mantener actualizadas las tablas de retención documental para un efectivo archivo documental.
11. Generar capacitación institucional para un mayor conocimiento del Sistema General de Sarlaft.

V. CONCLUSIONES.

- 4.1 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.
- 4.2 Es recomendable, establecer un plan de mejoramiento asegurando el cumplimiento del Sistema de Gestión Integral de Riesgos, asegurando un debido seguimiento dentro del modelo de mejoramiento institucional.
- 4.3 El Hospital ha logrado avanzar en un 3.2 en una escala de 1 a 5 aplicada la herramienta de medición del índice de madurez del riesgo para un programa de gestión integral de riesgos en la implementación de los principios y directrices de la norma ISO 31.000 – 2018. Se ha recomendado actualizar este indicador para el año 2020.
- 4.4 El Hospital cumple con todos los reportes que se deben enviar a la UIAF tales como: 1) El Reporte de Operaciones Intentadas y Operaciones Sospechosas (Reporte de Operaciones Sospechosas - ROS), 2) El Reporte de ausencia de Operaciones Sospechosas, si no se presentaron ROS en el mes inmediatamente anterior. 3) Reporte con todas las transacciones individuales en efectivo iguales o superiores a 5 millones de pesos diarias realizadas por una misma persona natural o jurídica (\$5'000,000) y el Reporte con todas las transacciones múltiples en efectivo iguales o superiores a 25 millones de pesos mensuales realizadas por una misma persona natural o jurídica (\$25'000,000). 4) Reporte de ausencia de transacciones en efectivo, si no se presentaron durante el mes inmediatamente anterior.

VI. PLAN DE MEJORAMIENTO Y SEGUIMIENTO.

Una vez en firme el presente Informe, 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 bimestral del Plan de Mejoramiento y presentará el Informe correspondiente.

VII. COMUNICACIÓN Y SOCIALIZACIÓN DEL INFORME FINAL.

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.

Nota: De acuerdo con 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”.

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

Preparó: **José Heriberto Vargas Lema**
Profesional de Auditoría Interna.

Revisó: **Carlos Uriel López Ríos,**
Jefe de Auditoría Interna.



Medellín, noviembre de 2020.