Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E.

Alcaldía de Medellín

HOSPITAL GENERAL DE MEDELLÍN
Luz Castro de Gutiérrez E.S.E.
Oficina de Auditoría Interna

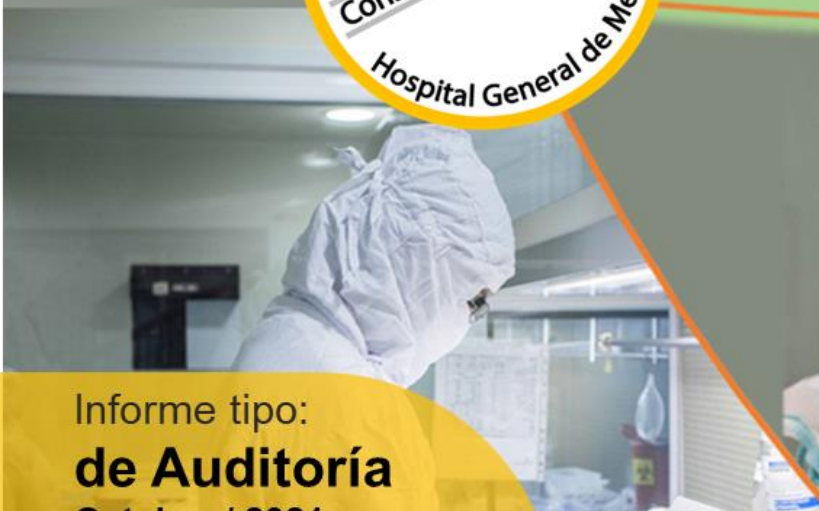
INFORME DE AUDITORÍA 2021

N° 14

Gestión de Riesgos

Modalidad
Auditoría Regular

Oficina de Auditoría Interna
Construimos Confianza
Hospital General de Medellín



Informe tipo:
de Auditoría

HOSPITAL GENERAL DE MEDELLÍN
Luz Castro de Gutiérrez E.S.E.
Oficina de Auditoría Interna

INFORME DE AUDITORÍA 2021
N° 14

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 Janneth Agudelo Arango
Karina Ruíz De la Hoz

Técnico:
Julio E. Suescún Montoya

Correo Oficina:
oficinadeauditoria@hgm.gov.co

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

CONTENIDO

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 2021 "**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 seis 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 se describen las conclusiones, en el quinto se presenta la formulación del Plan de Mejoramiento y en el sexto 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 jefa 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 auditoria 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.

Revisar la gestión de riesgos y la eficiencia de los controles implementados, verificando el cumplimiento de normatividad vigente y el cumplimiento de la política de gestión de riegos.

1.2. Alcance.

Esta auditoría inicia con la revisión de la política de administración riesgos, procedimiento del Sistema de Gestión Integral de Riesgos, el manual del sistema de ~~programa~~ de gestión integral del riesgo y el proyecto estratégico 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 Auditoria 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 Auditoria 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 Auditoria 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".*

1.5.6. Departamento Administrativo de la Función Pública, Dirección de Gestión y Desempeño Institucional. Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. diciembre de 2020.

1.5.7. Circular Externa 202117000000045 de 2021 del 15-09-2021 de la Supersalud, por la cual se imparten instrucciones generales relativas al código de conducta y de buen gobierno organizacional, el sistema integrado de gestión de riesgos y a sus subsistemas de administración de riesgos.

1.5.8. Circular Externa 202117000000055 del 17-09-2021 de la Supersalud, por medio de la cual se imparten instrucciones generales relativas al subsistema de administración del riesgo de corrupción, opacidad y fraude (SICOF) y modificaciones a las circulares externas 018 de 20215, 009 de 2016, 007 de 2017 y 003 de 2018

1.6. Documentos Base.

1.6.1. Caracterización del proceso y sus respectivos procedimientos.
1.6.2. Manual del Sistema de Gestión Integral del Riesgo.
1.6.3 -Procedimiento para la Administración del Riesgo.
1.6.4. Normas aplicables a la Gestión del Riesgo.
1.6.5. Actas de reuniones de Riesgos.
1.6.6. Comité de gestores de riesgo.
1.6.7. Mapa de Riesgo Institucional.
1.6.8. Matrices de Riesgo de los 39 procesos.
1.6.9. Presentaciones del plan de acción en lo referente a Riesgos.
1.6.10. Indicadores de Gestión del programa de Riesgos.
1.6.11. Informes generados de Riesgo a la Alta Dirección.
1.6.12. Aplicación de cuestionario de control al proceso.
1.1.13. Informes de seguimiento a riesgos y controles.
1.1.14. Informes generados de riesgos del Sistema de Seguridad y Salud en el Trabajo- SSST, Sistema de Gestión Ambiental- SGA, Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo – SARLAFT, Seguridad Digital, Oficina Asesora Jurídica y el área de Comunicaciones.

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.**

  Equivale 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:	Auditoria 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 2021

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 auditoria, en la aplicación de la técnica de indagación a la administración, se evidencia buen conocimiento tanto del proceso auditado como de las diferentes normas aplicables.

Se resalta la disposición del equipo de trabajo para atender la auditoría.

- Teniendo en cuenta los lineamientos del MIPG Se construye la Política de Planeación, la cual se encuentra aprobada y normalizada, de ésta se desprenden las demás políticas entre ellas la Política Riesgos.

- Se ajusta, se normaliza y se aprueba la Política de Riesgos según los últimos lineamientos del DAFP. Se detalla claramente los roles y responsabilidades de las 3 líneas de defensa y de la estratégica, la cual es desplegada en las reuniones del comité de gestores de riesgos.

- Se identificaron los riesgos del área de compras y suministros, del almacén y de órdenes de prestación de servicios que están a cargo del área de gestión humana.

- Se realizaron ajustes en la descripción de los riesgos teniendo en cuenta la posibilidad de afectación económica, legal o reputacional.

- Se ajustaron los controles de los riesgos teniendo en cuenta el responsable, la acción, la periodicidad y el complemento.

- El comité de gestores de riesgos, el cual fue aprobado por resolución de gerencia número 055 de 2021, con reuniones periódicas mensuales socializando los riesgos de cada uno de los procesos de la institución.

- Se actualiza el formato de la matriz de riesgos del Plan anticorrupción y atención al ciudadano, adoptando el del Departamento Administrativo de la Función Pública. Se realizó taller y se identificaron los riesgos de corrupción en 26 procesos teniendo en cuenta la Guía de Gestión de Riesgos de Corrupción del DAFP, lo que permitió actualizar el mapa institucional de riesgos de corrupción en el Plan Anticorrupción y Atención al Ciudadano (PAYAC), teniendo en cuenta los lineamientos del DAFP (Componente 1 Riesgos de Corrupción).

- A través del Convenio Docencia Servicio, la Universidad CES desarrolla un curso básico de riesgos de 30 horas, con el que se capacitan 21 gestores de riesgos durante el año 2021.

- Se tiene definido que el sistema de gestión integral de riesgos, se cuenta con una herramienta en carpeta compartida para identificar, valorar, evaluar y administrar los riesgos, la cual es objetivo de evaluación periódica por parte de la líder de riesgos de la institución.

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**	**16**	**100%**
	En el Proceso de Gobierno	3	19%
	En el Proceso de Control	2	13%
	En el Proceso de Riegos	11	69%
2	**Recomendaciones**	**59**	**100%**
	Para Mejorar el Gobierno	12	20%
	Para Mejorar el Control	2	3%
	Para Mejorar la gestión de Riesgos	45	76%

Cuadro N° 2. Observaciones y Recomendaciones - Síntesis.

OFICINA DE AUDITORÍA INTERNA Auditoría Gestión de Riesgos Observaciones y Recomendaciones		
N°	**Observaciones**	**Recomendaciones**
1	La metodología de medición de la madurez de la gestión de riesgos para ISO 31.000, para el año 2020 dio un resultado de 3.8 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 2021, aún no ha aplicado el instrumento para medir el índice de madurez de riesgos.	1.1. Continuar con el enfoque estructurado y exhaustivo a la Gestión del Riesgo que contribuya a los resultados coherentes y compatibles del Hospital. 1.2 La Alta Dirección deberá comunicar el valor de la Gestión del Riesgo a la organización y sus partes interesadas. 1.3 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.

		1.4 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. 1.5 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. 1.6 Dar a conocer a todas las partes interesadas la naturaleza y el nivel de riesgo residual después del tratamiento.
2	La auditoría observa que el manual de riesgos del Hospital, se encuentra desactualizado de acuerdo con la nueva guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020 del Departamento Administrativo de la Función Pública.	2.1. Actualizar el manual de riesgos del hospital de acuerdo con la nueva guía para la administración del riesgo y el diseño de controles en entidades púbicas.
3	El modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada la creación del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, la auditoría observa que en este marco general, para una adecuada gestión del riesgo y que dicha institucionalidad funcione, no se están analizando la gestión de riesgos aplicándoles las correspondientes mejoras ni están subiendo a estos comités el análisis de eventos y riesgos críticos, con análisis periódico de los riesgos institucionales.	3.1. Comunicación y reporte de riesgos del programa de gestión de riesgos a todas las partes interesadas. 3.2. Presentar informe de gestión de riesgos al comité coordinador de control interno y al comité de gestión y desempeño para su análisis de controles y propuestas de acciones de mejora.
4	La auditoría observa que en el mapa de riesgos no se encuentran debidamente analizados, valorados y evaluados los riesgos y controles asociados a la gestión de la prevención del daño antijurídico, y no se encuentran registrado en la matriz de riesgo la materialización de los riesgos jurídicos. La auditoría observa que aún no se presentan al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles, con una supervisión con la segunda y primera línea de defensa generando acciones para mitigar éstos riesgos.	4.1. Revisar la matriz de riesgos jurídicos y actualizar la identificación, valoración y análisis de éstos. 4.2. La Oficina Asesora Jurídica, deberá acompañar a los diferentes procesos de la institución en la identificación de probables riesgos jurídicos. 4.3. La Oficina Asesora Jurídica, deberá definir controles que conlleven a mitigar el daño antijurídico en la institución de acuerdo con los riesgos materializados a través de las diferentes demandas laborales y civiles falladas en contra de la institución.
5	La auditoría observa que en el mapa de riesgos se encuentran debidamente analizados, valorados y evaluados los riesgos y controles asociados a la gestión de los riesgos de lavado de activos y financiación del terrorismo, los cuales aún no se han presentado al comité coordinador de control interno con el respectivo seguimiento a éstos riesgos, y las correspondientes acciones para mitigarlos.	5.1. Establecer el perfil de riesgo residual de LA/ FT, y realizar seguimiento y monitoreo a estos riesgos. 5.2. Evaluar el riesgo de LA/FT cuando se tengan nuevos mercados u ofrezca nuevos servicios, dejando constancia de este análisis. 5.3. Establecer en el proceso de tesorería el monto máximo de efectivo que puede manejarse al interior de la entidad por tipo de cliente/usuario. 5.4. Analizar los informes presentados por la auditoría interna y los informes que presente el Revisor Fiscal. 5.5. 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 e informar al oficial de cumplimiento para la implementación de las respectivas acciones de mejora. 5.6. 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. Coordinadamente con la Dirección de Gestión Humana.

		5.7. Los procesos responsables deben actualizar las bases de datos de contrapartes, clientes, proveedores, colaboradores y entidades responsables. 5.8. Seguir el procedimiento estricto del proceso de Gestión Humana y compromiso por parte de los directivos en que no debe ingresar ningún colaborador sin cumplir con los requisitos de verificación del sarlaft. 5.9. Planear los bienes y servicios de modo que, haya el tiempo suficiente para hacer el procedimiento, y por ningún motivo, hacer comprar o contratar un servicio sin hacer la debida diligencia. 5.10. Hacer análisis de mercado: ¿Libre competencia, Monopolio, Oligopolio? para poder tomar decisiones informadas y mitigar riesgos.
6	La auditoría observa que no se encuentran identificados, valorados y analizados los riesgos de seguridad de la información, ni los riesgos de seguridad digital y de la ciberseguridad.	6.1. El líder de Seguridad Digital, deberá Identificar, valorar y analizar los riesgos de seguridad de la información, los riesgos de seguridad digital y de la ciberseguridad. 6.2. El líder de Seguridad Digital, deberá continuar el levantamiento de los activos de información que son aquellos de software y hardware que tienen valor para la organización en términos de información. 6.3. El líder de Seguridad Digital, deberá presentar al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles.
7	La auditoría observa que, de acuerdo con la metodología de la Función Pública y los ajustes realizados a la misma en diciembre del 2020, se ha ejecutado el respectivo taller de identificación de riesgos de corrupción con los líderes y delegados de 26 procesos del Hospital, quedando pendientes los nueve procesos asistenciales, Gestión de la investigación; Seguridad y Salud en el Trabajo; Información clínica y administrativa y el proceso de costos.	7.1 El oficial de cumplimiento deberá Identificar, valorar y analizar los riesgos de corrupción y la oficina de calidad y planeación a través del profesional u gestor de riesgos realizará seguimiento y la oficina asesora de control interno deberá realizar evaluación de los controles. 7.2 Informar al comité coordinador de control interno para el debido seguimiento con respecto a los resultados de la gestión del riesgo de corrupción, para efectuar el análisis de causas y determinar las acciones preventivas y de mejora.
8	La auditoría observa que los riesgos de contratación, se encuentran debidamente identificados, con análisis, valoración y evaluación, éstos riesgos aún no se presentan al comité coordinador de control interno, para su seguimiento y con la respectiva evaluación de controles. Se debe realizar seguimiento a un riesgo que se materializa referido a la falta de planeación en la contratación institucional, y al aseguramiento de pluralidad de oferentes en los diferentes procesos contractuales, que generen competencia para obtener los mejores precios competitivos en el mercado.	8.1 El director de apoyo logístico y le gestor de riesgos delegado, deberán Identificar, valorar y analizar el riesgo referido a la falta de planeación en la contratación, el aseguramiento de la pluralidad de oferentes en los diferentes procesos e involucrarlos en la matriz de riesgos del proceso. 8.2 El director de apoyo logístico y le gestor de riesgos delegado, deberán Identificar, valorar y analizar el riesgo referido a la falta de contratos en el proceso de compras de medicamentos y material médico quirúrgico. 8.3 El director de apoyo logístico y le gestor de riesgos delegado, deberán Identificar, valorar y analizar el riesgo referido a la desactualización de contratos de comodato.

9	Estos riesgos reputacional, no presentan seguimiento, ni una efectiva valoración y análisis periódico, para determinar el riesgo residual y la valoración de controles. Adicionalmente la auditoría observa que aún no se presentan al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles, con una supervisión con la segunda y primera línea de defensa generando acciones para mitigar éstos riesgos.	9.1 El profesional u comunicaciones, deberá Presentar informe de seguimiento, valoración, análisis y seguimiento de los riesgos reputacional de la institución.
10	La auditoría observa que se ajustó y se normalizó la Política de Riesgos según los últimos lineamientos del DAFP. Donde se detallan claramente los roles y responsabilidades de las tres líneas y de la estratégica, la cual fue desplegada en las reuniones del comité de gestores de riesgos. Esta política no fue presentada al comité coordinador de control interno, el cual debe emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales	10.1 Presentar la política de riesgos al comité coordinador de control interno para que se emitan lineamientos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales. 10.2 Definir el apetito de riegos para la institución. 10.3 Definir la tolerancia del riego, como el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por el Hospital.
11	Las matrices de riesgos de los procesos de Atención en ambulatorios, urgencias, hospitalización, clínicas quirúrgicas y apoyo diagnóstico No se encuentran debidamente actualizadas, ni con el respectivo seguimiento a riesgos.	11.1 Los directores asistenciales deberán, actualizar las matrices de riesgos de los procesos de: Atención en ambulatorios, urgencias, hospitalización, clínicas quirúrgicas y apoyo diagnóstico Revisar y actualizar los controles que aseguren una adecuada gestión de los procesos. 11.2 Presentar el mapa de riegos al comité coordinador de control interno y a la Junta Directiva. 11.3 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. 11.4 Los riesgos estratégicos y los calificados como extremos debe estar identificada su afectación a los objetivos estratégicos. 11.5 Revisar los riesgos de los servicios habilitados. 11.6 Fortalecer la identificación de los riesgos de fraude en la institución.

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 2020 dio un resultado de 3.8 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 2021, 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.

- Continuar con el enfoque estructurado y exhaustivo a la Gestión del Riesgo que contribuya a los resultados coherentes y compatibles del Hospital.
- 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 proyecto estratégico
- 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.
- 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.

Desde el año 2020, se presenta informe del contexto externo del hospital con un enfoque de riesgos.

f. Plan de mejoramiento.

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 proyecto estratégico

Observación de Auditoría Interna N° 2.

a. Descripción.

La auditoría observa que el manual de riesgos del Hospital, se encuentra desactualizado de acuerdo con la nueva guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020 del Departamento Administrativo de la Función Pública, Dirección de Gestión y Desempeño Institucional. Adicionalmente no se ha definido el perfil de riesgos institucional para la vigencia 2021

b. Criterios.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020 del Departamento Administrativo de la Función Pública, Dirección de Gestión y Desempeño Institucional.

c. Riesgo.

- Desactualización del manual de riesgos del Hospital.

d. Recomendación.

- Actualizar el manual de riesgos del hospital de acuerdo con la nueva guía para la administración del riesgo y el diseño de controles en entidades púbicas.

e. Posición del auditado.

La profesional gestora de riesgos fue quien notificó que el manual de riesgos del Hospital, se encuentra desactualizado de acuerdo con la nueva guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020 del Departamento Administrativo de la Función Pública, Dirección de Gestión y Desempeño Institucional. Adicionalmente no se ha definido el perfil de riesgos institucional para la vigencia 2021. Lo anterior es parte de la actividad del proyecto estratégico que tiene como plazo para ejecutarse el 31/12/2021.

f. Plan de mejoramiento.

Se requiere que los 39 procesos tengan identificados todos no solo los riesgos operativos de los procesos, sino también los riesgos de SSST, SGA, SARLAFT, Seguridad Digital, los jurídicos y reputacionales para poder definir el perfil de riesgos institucional para la vigencia 2021

Observación de Auditoría Interna N° 3.

a. Descripción.

Institucionalidad al Sistema Integral de Riesgos

El modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada la creación del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, la auditoría observa que en este marco general, para una adecuada gestión del riesgo y que dicha institucionalidad funcione, no se están analizando la gestión de riesgos aplicándoles las correspondientes mejoras ni están subiendo a estos comités el análisis de eventos y riesgos críticos, con análisis periódico de los riesgos institucionales.

b. Criterios.

- Modelo integrado de Planeación y Control (MIPG).

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.
- Presentar informe de gestión de riesgos al comité coordinador de control interno y al comité de gestión y desempeño para su análisis de controles y propuestas de acciones de mejora.
- Integrar el programa de Gestión de Riesgos al modelo de mejoramiento institucional.

e. Posición del auditado.

Se acepta la observación

f. Plan de mejoramiento.

Fortalecer el despliegue de los riesgos en el Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017

3.2. Para mejorar el proceso de Riesgos.

Observación de Auditoría Interna N° 4.

a. Descripción.

Riesgo jurídico

La auditoría observa que en el mapa de riesgos no se encuentran debidamente analizados, valorados y evaluados los riesgos y controles asociados a la gestión de la prevención del daño antijurídico, y no se encuentran registrado en la matriz de riesgo la materialización de los riesgos jurídicos.

La auditoría observa que aún no se presentan al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles, con una supervisión con la segunda y primera línea de defensa generando acciones para mitigar éstos riesgos.

Entre los riesgos identificados, se encuentran: Incumplimiento de la normatividad vigente, alteración del proceso jurídico por deficiencias en la información, inoportuna o inadecuada defensa judicial de la

Entidad por parte de la Oficina Jurídica, inoportunidad en el pago de los procesos judiciales, inadecuada caracterización documental del proceso estratégico institucional de gestión jurídica.

Se deberá complementar el análisis de riesgo jurídico relacionado con la materialización de las demandas laborales y civiles que le han representado a la institución valores significativos por pago de demandas y de intereses de mora en reliquidaciones de procesos ejecutivos.

Adicionalmente es importante que se avance en la identificación, análisis y valoración del riesgo jurídico referido a los contratos de prestación de servicios, dados Riesgos enunciados para los contratos de prestación de servicios. En diferentes sentencias la corte ha analizado la constitucionalidad del concepto legal de contrato de prestación de servicios, y ha dicho la Corte Constitucional que el contrato de prestación de servicios es el que se celebra por el Estado en aquellos eventos en que la función de la administración no puede ser suministrada por personas vinculadas con la entidad oficial contratante o cuando requiere de conocimientos especializados, para los cual establecen las siguientes características: Realización temporal de actividades inherentes al funcionamiento, la autonomía e independencia del contratista, la vigencia del contrato es temporal.

El día nueve (9) de septiembre de dos mil veintiunos (2021) el Consejo de Estado en SENTENCIA DE UNIFICACIÓN DE JURISPRUDENCIA CONFORME AL ARTÍCULO 271 DE LA LEY 1437 DE 2011, para la nulidad y restablecimiento del derecho, con radicado: 05001-23-33-000-2013-01143-01 (1317-2016), nuevamente recordó sobre el Contrato de prestación de servicios como una relación laboral encubierta o subyacente, temporal, con probable solución de continuidad, pago de prestaciones sociales, aportes al sistema de Seguridad Social en salud.

Sentencio el Consejo de Estado que una (ii) La segunda regla establece un periodo de treinta (30) días hábiles, entre la finalización de un contrato y la ejecución del siguiente, como término de la no solución de continuidad, el cual, en los casos que se exceda, podrá flexibilizarse en atención a las especiales circunstancias que el juez encuentre probadas dentro del expediente.

b. Criterios.

- Manual de gestión de riesgos.

c. Riesgo.

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

d. Recomendación.

- Revisar la matriz de riesgos jurídicos y actualizar la identificación, valoración y análisis de éstos.
- Acompañar a los diferentes procesos de la institución en la identificación de probables riesgos jurídicos.
- Definir controles que conlleven a mitigar el daño antijurídico en la institución de acuerdo con los riesgos materializados a través de las diferentes demandas laborales y civiles falladas en contra de la institución.
- Identificar y valorar los riesgos jurídicos de los contratos de prestación de servicios.

e. Posición del auditado.

Durante el 2020 y 2021 se dio inicio asesoría y acompañamiento a la oficina asesora jurídica en la identificación de éstos riesgos, adicionalmente estos fueron desplegados en el Comité de Gestores de Gestores de Riesgos, es necesario contar con la oficina jurídica para el diseño y la implementación de controles a los riesgos jurídicos, realizar seguimiento a los mismos para reducir o mitigar el daño jurídico en la entidad.

f. Plan de mejoramiento.

La oficina jurídica en acompañamiento de la profesional gestora de riesgos, deberá definir controles que conlleven a mitigar el daño antijurídico en la institución de acuerdo con los riesgos materializados a través de las diferentes demandas laborales y civiles falladas en contra de la institución

Observación de Auditoría Interna N° 5.

a. Descripción.

Riesgos de Lavado de Activos y Financiación del Terrorismo

La auditoría observa que en el mapa de riesgos se encuentran debidamente analizados, valorados y evaluados los riesgos y controles asociados a la gestión de los riesgos de lavado de activos y financiación del terrorismo, los cuales aún no se han presentado al comité coordinador de control interno con el respectivo seguimiento a éstos riesgos, y las correspondientes acciones para mitigarlos.

De acuerdo con el seguimiento que hace el procedimiento a sus riesgos, presentan las siguientes observaciones:

- "Los nuevos miembros de Junta Directiva no llenan los formularios de sarlfat correspondientes al ingreso al Hospital y tampoco lo actualizan anualmente.
- Contratos de prestación de servicios: De los 37 contratos nuevos firmados, 8 se verificaron en listas después de iniciado el contrato.
- Los datos actualizados de todo el personal no se ingresan a una base de datos, no se puede hacer seguimiento a los cambios en los datos personales y financieros con el fin de detectar señales de alerta.
- Alta rotación de personal en los procesos sensibles: Adquisición de bienes y servicios, gestión humana y Financiera, entre otras, el cual no es informado ni es programado para capacitación en el Sistema de sarlaft.
- No se actualizan datos de los proveedores: Certificados, registros, datos básicos, financieros, etc.
- No se inactivan en el Sistema los proveedores con los cuales no se tiene ningún tipo de vinculación en el último año.
- No se identifican los riesgos de corrupción y LAFT en las matrices de los diferentes contratos que tiene el Hospital con sus proveedores.
- Probable fraccionamiento de contratos, debido a que se hacen consecutivas órdenes de servicio por valores que no superen los 50 SMMLV, pero que en el mes suman el valor establecido para hacer un contrato con formalidades plenas.
- No se actualizan datos de las EPS e Instituciones a las que prestamos servicios, se evidencia que hay cambios en la estructura organizacional de estas empresas, cambio de Nit y razón social y no se actualizan datos.
- No se tiene establecido un procedimiento para la contratación de estas Instituciones.
- No hay un adecuado registro de datos (nombres y apellidos completos con número y tipo de identificación) del pagador, que no necesariamente es el paciente. En las taquillas no se les pide

ninguna documentación, lo que hacen es preguntar por el nombre y apellidos y el número de documento, pero éste no es debidamente verificado.

- Se debe tener una política de los pagos en efectivo, no sólo de los usuarios al hospital, sino del Hospital a los proveedores: Cuándo se pueden hacer, el monto y la contraparte".

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 se le deberá informar al Oficial de Cumplimiento para que se realice la respectiva evaluación del 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.

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 su respectivo suplente, para que, en ausencia temporal del titular de Oficial de Cumplimiento, ejecute y asuma sus funciones. Es importante tener en cuenta que la oficial suplente es la profesional universitaria gestora de riesgos de la oficina de calidad y planeación, quien a la fecha de la auditoria no cuenta con las 90 horas de estudio de SARLAFT exigidas acorde a la norma, adicionalmente nunca se ha desempeñado como oficial de cumplimiento y nunca en los encargos de funciones ha recibido la entrega del puesto oficial ni se ha realizado el debido empalme, ni se ha dejado constancia de ello en acta de entrega acorde al proceso institucional.

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.

b. Criterios.

- Circular 000009 del 21 de abril de 2016

c. Riesgo.

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

d. Recomendación.

- Establecer el perfil de riesgo residual de LA/ FT, y realizar seguimiento y monitoreo a estos riesgos.
- Evaluar el riesgo de LA/FT cuando se tengan nuevos mercados u ofrezca nuevos servicios, dejando constancia de este análisis.
- Establecer en el proceso de tesorería el monto máximo de efectivo que puede manejarse al interior de la entidad por tipo de cliente/usuario.
- Analizar los informes presentados por la auditoría interna y los informes que presente el Revisor Fiscal.
- 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 e informar al oficial de cumplimiento para la implementación de las respectivas acciones de mejora.
- 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. Coordinadamente con la Dirección de Gestión Humana.

- Los procesos responsables deben actualizar las bases de datos de contrapartes, clientes, proveedores, colaboradores y entidades responsables.
- Generar capacitación institucional para un mayor conocimiento del Sistema General de Sarlaft.
- Seguir el procedimiento estricto del proceso de Gestión Humana y compromiso por parte de los directivos en que no debe ingresar ningún colaborador sin cumplir con los requisitos de verificación del sarlaft.
- Seguir el procedimiento estricto del proceso de adquisición de bienes y servicios.
- Planear los bienes y servicios de modo que, haya el tiempo suficiente para hacer el procedimiento, y por ningún motivo, hacer comprar o contratar un servicio sin hacer la debida diligencia.
- Hacer análisis de mercado: ¿Libre competencia, Monopolio, Oligopolio? para poder tomar decisiones informadas y mitigar riesgos.
- Los contratistas y los empleados de empresas tercerizadas no son considerados funcionarios públicos, sin embargo, se debe considerar una política sobre los antecedentes penales de los empleados de las empresas tercerizadas, para verificar que ninguno sea fuente de LAFT. Se recomienda que en el contrato con estas empresas se considere la obligación que el contratista revise los antecedentes y riesgos de LA/FT.
- Responsabilizar a los funcionarios para hacer la actualización de datos y documentos anualmente.
- Las recomendaciones de fortalecimiento de controles a riesgos de LA/FT, deberán implementarse a través del modelo de mejoramiento institucional.
- Verificar en listas las contrapartes antes de iniciar la relación contractual, comercial o laboral.
- Crear un proceso que se encargue específicamente del relacionamiento con los clientes, estudio de tarifas, documentación del procedimiento.
- Solicitar actualización de datos de proveedores, empresas responsables de pago y otros clientes activos e instituciones educativas.
- Inactivar en el sistema SAP los proveedores con los cuales no tenemos una relación comercial activa por más de 1 año.
- Incluir las responsabilidades frente al Sarlaft en cada uno de los manuales de funciones.
- Entrenar a la oficial de cumplimiento suplente y realizar el correspondiente empalme acorde a lo definido por la institución y dejar constancia en el acta de entrega.

e. Posición del auditado.

Capacitar y entrenar a la oficial de cumplimiento suplente y realizar el correspondiente empalme acorde a lo definido por la institución y dejar constancia en el acta de entrega.

f. Plan de mejoramiento.

La oficial de cumplimiento en la directa responsable de identificar, analizar los riesgos de corrupción, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento y la oficina de auditoría interna es la responsable de la evaluación de los riesgos de corrupción.

Observación de Auditoría Interna N° 6.

a. Descripción.

Riesgos de Seguridad informática y Seguridad Digital.

La auditoría observa que, en infraestructura de tecnologías de información, se encuentran identificados los siguientes riesgos: interrupción de la operación del sistema de información de SAP, alteración de la información de SAP, fraude a través del Sistema de información SAP, interrupción de las comunicaciones telefónicas, interrupción de los servicios de red, destrucción o daño masiva de equipos o de equipos críticos, uso indebido de la información sensible.

Para los cuales en su seguimiento, el proceso registra los siguientes riegos materializados: "caída del servicio eléctrico, bloqueo en el switch de servidores del datacenter del piso 4, alteración de la red del HGM, no ingreso a la plataforma SAP, situación presentada en el proveedor de hosting con el servicio, bloqueo del servidor de Avaya, interrupciones en servicio de telefonía, caída del servicio eléctrico, no funcionalidad de la UPS, alteración de la red del HGM", constantes fallas eléctricas en zonas del Hospital General, desconexión fibra óptica sede 80, fallas de red en sede 80 debido a conexión de equipos no autorizados"

La auditoría observa que no se encuentran identificados, valorados y analizados los riesgos de seguridad de la información, ni los riesgos de seguridad digital y de la ciberseguridad.

Se recomienda continuar el levantamiento de los activos de información que son aquellos de software y hardware que tienen valor para la organización en términos de información.

La auditoría observa que aún no se presentan al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles, con una supervisión con la segunda y primera línea de defensa generando acciones para mitigar éstos riesgos, que permita proceder de manera inmediata a aplicar planes de contingencia o de tratamiento de incidentes de seguridad de la información.

b. Criterios.

- Manual de gestión de riesgos.

c. Riesgo.

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

d. Recomendación.

- Identificar, valorar y analizar los riesgos de seguridad de la información, los riesgos de seguridad digital y de la ciberseguridad.
- Continuar el levantamiento de los activos de información que son aquellos de software y hardware que tienen valor para la organización en términos de información.
- Presentar al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles.

e. Posición del auditado.

El líder de sistemas es el responsable de identificar, analizar y desplegar los riesgos de seguridad digital en los 39 procesos institucionales, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento.

f. Plan de mejoramiento.

El líder de sistemas es el responsable de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos de seguridad digital teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento.

Observación de Auditoría Interna N° 7.

a. Descripción.

Riesgos de Seguridad y Salud en el Trabajo.

La auditoría observa que en el mapa de riesgos se encuentran debidamente analizados, valorados y evaluados los riesgos y controles asociados a la seguridad y salud en el trabajo, pero aún no se presentan al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles, con una supervisión con la segunda y primera línea de defensa generando acciones para mitigar éstos riesgos.

Entre los riesgos identificados se encuentran.

- Falta de gestionar los riesgos relacionados con condiciones inseguras en las diferentes áreas de trabajo del Hospital General de Medellín.
- Presentación de enfermedades laborales por falta de intervención oportuna ante la exposición a factores de riesgo HGM
- Presentación de enfermedades de orden mental relacionadas con condiciones propias de la actividad laboral por falta de intervención oportuna.
- Aumento del ausentismo por enfermedad general, por patologías susceptibles de manejo con estilos saludables de vida.
- Presentación de conflictos entre colaboradores, usuarios y entre los mismos trabajadores por falta de un manejo integral de la violencia de todo tipo en los lugares de trabajo.
- Pérdidas humanas y materiales ante eventos urgentes al interior de la Institución por falta de una planificación oportuna del manejo de las emergencias internas.
- Materialización de riesgos legales, reputaciones y económicos por falta de alineamiento con el que hacer operacional de contratistas y terceros. (contratación).
- Incumplimiento legal por falta de identificación y valoración de normatividad relacionada con aspectos de seguridad y salud en el trabajo.

Para los cuales el proceso, registra que se han materializado los siguientes riesgos:

"Se presentaron un total de 16 accidentes. El cargo con mayor accidentalidad fue el de auxiliares de enfermería. Se da continuidad a estrategias de accidentalidad las cuales se ha concentrado en realizar inspecciones de seguridad mensualmente, en seguimiento a los hallazgos, retroalimentación al personal sobre comportamientos y condiciones inseguras, cultura del cuidado, capacitación al personal asistencial, Copasst y grupo gestores, seguimiento al ausentismo, además de normas de bioseguridad. El mayor número de accidentes fueron por riesgo Biomecánico, seguidos del mecánico.

En este periodo del año, se han presentado 81 contagios por COVID, por lo que están en estudio estos 81 casos como enfermedad laboral debido al decreto presidencial 676 del 2020. La mayoría de estos eventos no se relacionan con el contagio directo con pacientes y se consiguen en entornos como cafeterías y pasillos.

En el periodo se realizaron 15 inspecciones, sobre todo de áreas técnicas de apoyo y se realizó verificación de estado de los planes definidos para el control de implementación de la mejora así: 72% cerrados, 17% en proceso y 11% abiertas"

Se debe contar con las actas o listados de asistencia de las asesorías realizadas en la identificación y socialización de éstos riesgos de seguridad y salud en el trabajo a todos los procesos institucionales.

Igualmente se debe actualizar y normalizar la caracterización de los procesos con éstos riesgos identificados, según el cronograma del plan de acción.

b. Criterios.

- Manual de gestión de riesgos

c. Riesgo.

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

d. Recomendación.

- Asesorar a todos los procesos en la identificación de sus propios riesgos de seguridad y salud en el trabajo. Se debe contar con las actas o listados de asistencia de las asesorías realizadas en la identificación y socialización de éstos riesgos de seguridad y salud en el trabajo a todos los procesos institucionales.

- Actualizar y normalizar la caracterización de los procesos con éstos riesgos identificados, según el cronograma del plan de acción.

e. Posición del auditado.

El líder de SSST es el responsable de identificar, analizar y desplegar los riesgos de seguridad y salud en el trabajo en los 39 procesos de la entidad, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento.

f. Plan de mejoramiento.

El líder de SSST es el responsable de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos de SSST, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento.

Observación de Auditoría Interna N° 8.

a. Descripción.

Riesgos de Gestión Ambiental.

La auditoría observa que se encuentra en proceso de identificación, análisis, valoración y evaluación los riesgos y controles asociados a la gestión ambiental, pero no se encuentran registrado en la matriz

de riesgo la materialización de éstos riesgos. Aún no se presentan al comité coordinador de control interno el seguimiento a éstos, con la respectiva evaluación de controles.

Dentro de las acciones que están en proceso se encuentran las siguientes:

- Asesoría y acompañamiento para la implementación y sostenimiento de la NTC ISO 14001:2015, con el fin de dar cumplimiento a lo establecido en la norma técnica. Donde se realizará revisión de los documentos del SGA, incluido la Matriz Legal y de Aspectos e Impactos Ambientales.

- Por medio del Profesional de Control a Terceros se realiza seguimiento y supervisión al desarrollo de las actividades de cada empresa y se evalúan los criterios y directrices dadas por el Hospital, entre ellas a la empresa que realiza la Gestión Integral de los Residuos Hospitalarios.

- Se adjudicó el Contrato N°133C de 2021 con ASEO GLOBAL COLOMBIA S.A.S E.S.P. Y mensualmente se hace seguimiento a la ejecución del mismo.

- Se continúa llevando el registro en el cuadro de indicadores para llevar control y análisis de los consumos de agua, energía y gas.

- Se adelantan trámites para la consultoría de factibilidad para la instalación de un Sistema de Energía Solar.

- Se realizó el monitoreo de agua potable en los sistemas de almacenamiento del hospital, el pasado el 06 de agosto del 2021.

- Se realizó un estudio de emisiones atmosféricas de los gases de combustión según la Resolución Metropolitana 912 de 2017 de las Calderas JCT 100 BHP y Distral 200 BHP.

- Se continua con la ejecución de los mantenimientos preventivos y correctivos a las tuberías, canoas y cajas para control en el taponamiento de tuberías.

- Se realiza de manera periódica el mantenimiento a las trampas de grasas.

- La Brigada de Emergencias realiza monitoreo continuo a los indicadores de alarma de la Institución, de igual modo a los extintores y la red contra incendios.

- Se despliegan piezas gráficas relacionadas con el cuidado del Medio Ambiente, se publican Efemérides Ambientales.

- Se diseñó campaña y se solicitó la difusión de la misma en el Manejo de Vertimientos.

- Se realizan capacitaciones en temas ambientales.

- Se ejecuta el Presupuesto de Gestión Ambiental, conforme a lo establecido en el Plan Anual de Adquisiciones.

- El Hospital contrata un Ingeniero Ambiental por prestación de servicios y una Tecnóloga Ambiental por parte del Corredor de Seguros, para dar ejecución a las actividades propias del Sistema de Gestión Ambiental.

- Se contrataron los análisis de laboratorio para la caracterización microbiológica de residuos.

Se debe contar con las actas o listados de asistencia de las asesorías realizadas en la identificación y socialización de éstos riesgos ambientales a todos los procesos institucionales.

Igualmente se debe actualizar y normalizar la caracterización de los procesos con éstos riesgos identificados, según el cronograma del plan de acción.

b. Criterios.

- Manual de gestión de riesgos.

c. Riesgo.

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

d. Recomendación.

- Asesorar a todos los procesos en la identificación de sus propios riesgos ambientales. Se debe contar con las actas o listados de asistencia de las asesorías realizadas en la identificación y socialización de éstos riesgos a todos los procesos institucionales.

- Actualizar y normalizar la caracterización de los procesos con éstos riesgos identificados, según el cronograma del plan de acción.

e. Posición del auditado.

El líder de Gestión Ambiental, es el responsable de identificar, analizar y desplegar los riesgos ambientales en los 39 procesos de la entidad , teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento

f. Plan de mejoramiento.

El líder de Gestión Ambiental es el responsable de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos ambientales, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento.

Observación de Auditoría Interna N° 9.

a. Descripción.

Riesgos de Corrupción.

La auditoría observa que, de acuerdo con la metodología de la Función Pública y los ajustes realizados a la misma en diciembre del 2020, se ha ejecutado el respectivo taller de identificación de riesgos de corrupción por parte de la profesional u gestora de riesgos, con los líderes y delegados de 26 procesos del Hospital, quedando pendientes los nueve procesos asistenciales, Gestión de la investigación; Seguridad y Salud en el Trabajo; Información clínica y administrativa y el proceso de costos.

Los riesgos de corrupción de los procesos, a nivel institucional identificados son: 1) Pagar o recibir sobornos; 2) Malversación desviación de activos; 3) Conflicto de intereses; 4) Clientelismo favoritismo, nepotismo; 5) Tráfico de influencias; 6) Recibir dádivas o beneficios. Se redactaron los riesgos teniendo en cuenta la posibilidad de afectación económica, legal o reputacional y se diseñaron los controles teniendo en cuenta el cargo, la acción y el complemento, adicionalmente se definieron acciones de seguimiento en cada proceso.

La gestora de riesgos de la Oficina de Calidad y Planeación, cada 4 meses hace monitoreo y seguimiento a los riesgos de corrupción del Plan anticorrupción y atención al ciudadano (PAYAC). Se realizará un plan institucional para el control de los riesgos de corrupción con el despliegue del Código de Integridad, las Políticas institucionales y con los puntos de control en las actividades de los procesos que sean susceptibles a los actos de corrupción.

Todas estas actividades se deberán informar al comité coordinador de control interno para el debido seguimiento con respecto a los resultados de la gestión del riesgo, para efectuar el análisis de causas y determinar las acciones preventivas y de mejora.

b. Criterios.

- Manual de gestión de riesgos.

c. Riesgo.

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

d. Recomendación.

- informar al comité coordinador de control interno para el debido seguimiento con respecto a los resultados de la gestión del riesgo de corrupción, para efectuar el análisis de causas y determinar las acciones preventivas y de mejora.

e. Posición del auditado.

El Oficial de Cumplimiento es el responsable de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos de Corrupción, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento y la oficina de auditoría interna es la responsable de realizar la evaluación de los controles y realizar informe al respecto.

f. Plan de mejoramiento.

El Oficial de Cumplimiento es el responsable de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos de Corrupción, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el seguimiento y la oficina de auditoría interna es la responsable de realizar la evaluación de los controles y realizar informe al respecto.

Observación de Auditoría Interna N° 10.

a. Descripción.

Riesgos de Contratación.

La auditoría observa que los riesgos de contratación, se encuentra debidamente identificados, con análisis, valoración y evaluación, éstos riesgos aún no se presentan al comité coordinador de control interno, para su seguimiento y con la respectiva evaluación de controles.

Entre los riesgos de contratación identificados, se encuentran:

- Ejecución del contrato de manera tardía por parte del contratista.

- Deficiente calidad de uno o varios de los productos y/o servicios, pactados en las obligaciones del contratista y especificaciones técnicas.
- No concordancia entre el servicio ejecutado o el bien entregado y las especificaciones técnicas ofertadas y aceptadas por el Hospital.
- Desnaturalización del contrato de prestación de servicios (Contrato Realidad).
- Incumplimiento de la publicación de los contratos en el SECOP o que se haga de forma tardía.
- Incumplimiento de la publicación de los contratos en la plataforma de Gestión Transparente.
- No realizar la interventoría o supervisión del contrato adecuadamente y de acuerdo con las normas vigentes.
- No iniciar los procesos administrativos de imposición de multas, sanciones o incumplimientos de manera oportuna.
- Problemas de calidad posterior al recibo de los bienes, obras o servicios.
- La probabilidad de direccionar compras al reducir el número de proveedores.
- Retrasos en la elaboración de los contratos
- Retrasos en la legalización de los contratos
- Elaboración de contratos sin el cumplimiento de los requisitos.

De acuerdo con el seguimiento, el proceso registra que solo se han materializado los siguientes riesgos:

- Retrasos en la elaboración de los contratos por demora en la entrega de la documentación por parte de las áreas responsables.

- Se materializó el riesgo de desabastecimiento por parte de proveedores por medicamentos escasos y por orden público.

La auditoría observa que se debe realizar seguimiento a un riesgo que se materializa referido a la falta de planeación en la contratación institucional, y al aseguramiento de pluralidad de oferentes en los diferentes procesos contractuales, que generen competencia para obtener los mejores precios competitivos en el mercado.

Adicionalmente considerar el riesgo en los contratos de medicamentos y material médico quirúrgico, los cuales para el año 2021, solo se tiene un contrato, igualmente no se realizaron convocatorias que lleven a formalizar contratos de medicamentos y/o material médico quirúrgico que contribuyan a fortalecer el control de precios, calidad y formalidad en las compras institucionales, lo cual conlleva a realizar estas actividades vía órdenes de compra de unas cuantías importantes, presentándose casos de órdenes de compra que durante un mismo día superan los montos autorizados para éstas.

Adicionalmente los contratos de comodato se encuentran desactualizados, se requiere hacer un análisis con el área de Activos, con el fin de constatar cuales de estos comodatos se encuentran vigentes e incluso determinar si existen equipos que no tengan contrato asociado

b. Criterios.

- Manual de gestión de riesgos.

c. Riesgo.

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

d. Recomendación.

- Identificar, valorar y analizar el riesgo referido a la falta de planeación en la contratación, el aseguramiento de la pluralidad de oferentes en los diferentes procesos e involucrarlos en la matriz de riesgos del proceso.

- Identificar, valorar y analizar el riesgo referido a la falta de contratos en el proceso de compras de medicamentos y material médico quirúrgico.

- Identificar, valorar y analizar el riesgo referido a la desactualización de contratos de comodato.

e. Posición del auditado.
El director de apoyo logístico y el gestor de riesgos delegado profesional y abogado, con los responsable de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos de Contratación, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el acompañamiento y seguimiento.

f. Plan de mejoramiento.
El director de apoyo logístico y el gestor de riesgos delegado profesional y abogado, con los responsables de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos de Contratación, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el acompañamiento y seguimiento.

Observación de Auditoría Interna N° 11.

a. Descripción.

Riesgos Estratégicos y de planeación.

La auditoría observa que entre los riesgos estratégicos y de planeación, identificados se encuentran:

- Inadecuada definición de la estrategia para lograr que la implementación impacte en la cadena de valor.
- Inoperabilidad en el sistema de seguimiento y evaluación de la estrategia.
- Insuficiente estudio de mercado para identificar los usuarios potenciales y evaluar la competencia
- Incertidumbre asociada a la gestión efectiva y control de las finanzas de la organización
- Desarticulación del modelo de atención de la Organización con la política de atención Integral en salud como agente del sistema desde la complementariedad.
- La estructura organizacional no soportada con el recurso humano determinado para la entidad
- Desalineación de las tecnologías de la información y las comunicaciones con las estrategias definidas, existencia de manuales sin ningún tipo de sistematización con riesgo de que se altere la seguridad de la información.
- Inadecuado alcance de los proyectos planteados para ejecutar en el plan de desarrollo para el periodo.
- Inadecuada integración de los sistemas de gestión para garantizar las acciones que nos obliga el modelo para el sector público y los relacionados con los objetivos de desarrollo sostenible.

Para los anteriores riesgos, el proceso presenta en su seguimiento, las siguientes observaciones:

"La estrategia está definida para el cuatrienio, no obstante, los proyectos no tienen claro el alcance del proyecto en cada una de las vigencias.

Los procesos de apoyo no han permitido el avance de los proyectos misionales que permitan generar aporte a la cadena de valor.

El objetivo estratégico N°3, que permite que seamos más competitivos no cuenta con la estructura requerida para lograr potencializar la venta de servicios.

Los Objetivos estratégicos y misionales N°1 y N°2, no cuenta con la totalidad de resultados esperados de acuerdo con los resultados de la evaluación del segundo trimestre de este año.

Se requiere un lineamiento de la alta gerencia para lograr estabilizar el proceso de seguimiento a la planeación de los procesos y proyectos institucionales.

Insuficientes estudios de mercado para identificar clientes potenciales.

Sistema de costos sin implementación de su proyecto.

El modelo de atención basado en el flujo de pacientes actualizado con MAITE, con despliegue e implementación valorada en los indicadores del modelo de atención y la central de monitoreo, no se ha generado la consistencia en el mejoramiento del modelo de forma articulada, a la fecha se han realizado intervenciones en el eje de humanización, guía de atención al ciudadano y con el proceso transversal de enfermería con resultado positivos.

Aún se observa la falta de avances esperados en el proyecto de estructura organizacional.

Aún no se presentan avances en el desarrollo de la política de gobierno digital".

La auditoría observa que aún no se presentan al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles, con una supervisión con la segunda y primera línea generando acciones para mitigar éstos riesgos.

b. Criterios.

- Manual de gestión de riegos.

c. Riesgo.

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

d. Recomendación.

- Presentar al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles.
- Identificar controles para mitigar los riesgos enunciados con las respectivas observaciones, estableciendo un plan de acción y de mejora.

e. Posición del auditado.

Se aceptan las recomendaciones.

f. Plan de mejoramiento.

Se presentarán ante el comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles, con una supervisión con la segunda y primera línea generando acciones para mitigar éstos riesgos.

Observación de Auditoría Interna N° 12.

a. Descripción.

Riesgos Reputacional.

La auditoría observa que entre los riesgos reputacional identificados se encuentran:

- Inexistencia del Comité Manejo de Crisis
- Inadecuado manejo de los conflictos internos que afectan el clima organizacional
- Inexistencia de una política institucional sobre manejo de las fake news en redes sociales
- Inobservancia de la Protección de Datos y el Derecho a la intimidad
- No existencia de un área de mercadeo
- Emisión de publicidad o información negativa referente a la Institución o alguno de sus integrantes. Esto tiene que ver con publicación de casos de corrupción o de eventos adversos.
- Dificultad de acceso a la información institucional destinada a las diferentes plataformas.

Estos riesgos no presentan seguimiento, ni una efectiva valoración y análisis periódico, para determinar el riesgo residual y la valoración de controles. Adicionalmente la auditoría observa que aún no se presentan al comité coordinador de control interno el seguimiento a éstos riesgos, con la respectiva evaluación de controles, con una supervisión con la segunda y primera línea de defensa generando acciones para mitigar éstos riesgos.

b. Criterios.

- Manual de gestión de riesgos.

c. Riesgo.

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

d. Recomendación.

- Presentar informe de seguimiento, valoración, análisis y seguimiento de los riesgos reputacionales de la institución.

e. Posición del auditado.

El profesional u de comunicaciones y el gestor de riesgos delegado son los responsables de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos reputacionales, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el acompañamiento y seguimiento

f. Plan de mejoramiento.

El profesional u de comunicaciones y el gestor de riesgos delegado son los responsables de identificar, analizar, definir los controles y acciones de seguimiento y desplegar los riesgos reputacionales, teniendo en cuenta la metodología definida por la entidad y la oficina de calidad y planeación a través de la profesional u gestora de riesgos realizará el acompañamiento y seguimiento

Observación de Auditoría Interna N° 13.

a. Descripción.

Política de Administración de Riesgos.

La auditoría observa que se ajustó y se normalizó la Política de Riesgos según los últimos lineamientos del DAFP. Donde se detallan claramente los roles y responsabilidades de las tres líneas y de la estratégica, la cual fue desplegada en las reuniones del comité de gestores de riesgos. Esta política no

fue presentada al comité coordinador de control interno, el cual debe emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales, adicionalmente en la parte final del documento aparece aprobada por un comité de coordinación del sistema de gestión integral de calidad, el cual no existe en la institución.

Es necesario tener en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, el cual es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que el hospital debe o desea gestionar, adicionalmente está pendiente por definir la tolerancia del riego, como el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por el Hospital, adicionalmente está pendiente de determinar la capacidad de riesgo que es el máximo valor del nivel de riesgo que el Hospital puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos.

b. Criterios.

- Manual de gestión de riesgos.

c. Riesgo.

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

d. Recomendación.

- Presentar la política de riesgos al comité coordinador de control interno para que se emitan lineamientos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.
- Definir el apetito de riegos para la institución.
- Definir la tolerancia del riego, como el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por el Hospital.

e. Posición del auditado.

Para determinar el apetito del riesgo es necesario que todos los riesgos del SGIR (Operativos+SSST+SGA+LA/FT+jurídicos+reputacionales) estén identificados en los 39 procesos de la entidad y aún hay procesos como los asistenciales, algunos de apoyo como costos, contabilidad, facturación, infraestructura que no cuentan con la adecuada identificación de riesgos, adicionalmente es necesario contar con todos los análisis y actualización de todos los indicadores de los procesos y estratégicos para contar con el insumo fundamental para definir el apetito, capacidad y tolerancia al riesgo.

Es importante tener en cuenta que implementar el SGIR en el hospital de realiza en marco de un proyecto estratégico y este se desarrolla por fases desde el año 2016, ya que implementar un SGIR en una entidad requiere de compromiso de la alta gerencia, madures en el SGIR, y los cambios políticos y la alta rotación de personal en al entidad a nivel directivo, profesional y operativo retrasan la ejecución oportuna de las actividades del proyecto estratégico "Implementación de un Sistema de Gestión Integral de Riesgos acorde a los lineamientos del MIPG"

f. Plan de mejoramiento.

Identificar todos los riesgos que componente el SGIR en los 39 proceso de la entidad
Contar con todos los indicadores de los procesos y estratégicos debidamente diligenciados.

Observación de Auditoría Interna N° 14.

a. Descripción.

El mapa de riesgos año 2021 se encuentra en proceso de construcción dado que los procesos están actualizando sus riesgos. Por lo tanto, no ha 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.

Las matrices de riesgos de los procesos de Atención en ambulatorios, urgencias, hospitalización, clínicas quirúrgicas y apoyo diagnóstico No se encuentran debidamente actualizadas, ni con el respectivo seguimiento a riesgos.

b. Criterios.

- Manual de gestión de riesgos institucional.

c. Riesgo.

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

d. Recomendación.

- Actualizar las matrices de riesgos de los procesos de: Atención en ambulatorios, urgencias, hospitalización, clínicas quirúrgicas y apoyo diagnóstico, costos, contabilidad, presupuesto, facturación, infraestructura. Revisar y actualizar los controles que aseguren una adecuada gestión de los procesos.
- Presentar el mapa de riegos al comité coordinador de control interno y a la Junta Directiva.
- 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.
- Fortalecer la identificación de los riesgos de fraude en la institución.

e. Posición del auditado.

Se aceptan las recomendaciones

f. Plan de mejoramiento.

- Presentar el mapa de riegos al comité coordinador de control interno y a la Junta Directiva.
- Actualizar las matrices de riesgos de los procesos de: Atención en ambulatorios, urgencias, hospitalización, clínicas quirúrgicas y apoyo diagnóstico, costos, contabilidad, presupuesto, facturación, infraestructura

3.3. Para mejorar el proceso de Control.

Observación de Auditoría Interna N° 15.

a. Descripción.

Establecer un cronograma de cumplimiento de la Circular Externa 202117000000045 de 2021 del 15-09-2021 de la Supersalud, por la cual se imparten instrucciones generales relativas al código de

conducta y de buen gobierno organizacional y el sistema integrado de gestión de riesgos y a sus subsistemas de administración de riesgos. Para lo cual establecen que las entidades deben tener la capacidad institucional para identificar, evaluar, controlar, prevenir y mitigar los riesgos que puedan afectar el logro de sus objetivos y, especialmente, el cumplimiento de los objetivos del SGSSS y sus obligaciones contractuales.

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

En este contexto, las entidades deben gestionar todos los riesgos a los que estén expuestas dentro de su operación, y su gestión dependerá de la discrecionalidad y organización que cada entidad les quiera dar para su tratamiento. Sin embargo, deberán contemplar como mínimo, los siguientes riesgos priorizados y sus respectivos subsistemas:

1. Riesgo en Salud
2. Riesgo Operacional
3. Riesgo Actuarial
4. Riesgo de Crédito
5. Riesgo de Liquidez
6. Riesgo de Mercado de Capitales
7. Riesgo de Grupo
8. Riesgo de Lavado de Activos y Financiación del Terrorismo

b. Criterios.

- Circular Externa 202117000000045 de 2021 del 15-09-2021 de la Supersalud.

c. Riesgo.

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

d. Recomendación.

- Establecer el respectivo cronograma de cumplimiento de la Circular Externa 202117000000045 de 2021 del 15-09-2021 de la Supersalud.

e. Posición del auditado.

Se aceptan las recomendaciones

f. Plan de mejoramiento.

Establecer el respectivo cronograma de cumplimiento de la Circular Externa 202117000000045 de 2021 del 15-09-2021 de la Supersalud.

Observación de Auditoría Interna N° 16.

a. Descripción.

Se deberá establecer un cronograma de cumplimiento de la Circular Externa 202117000000055 del 17-09-2021 de la Supersalud, para que se implemente un adecuado Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude (SICOF), en la medida en que se logren los objetivos, el Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF, brindará mayor seguridad a los diferentes grupos de interés que interactúan con la entidad y al Sistema de salud.

Así mismo, los principios del Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF, constituyen los fundamentos y condiciones imprescindibles y básicas que garantizan su efectividad de acuerdo con la naturaleza de las operaciones autorizadas, funciones y características propias, y se aplican para cada uno de los aspectos que se tratan en la circular. En consecuencia, las entidades, en el diseño e implementación o revisión o ajustes del Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF, deben documentarlos con los soportes pertinentes y tenerlos a disposición de la Superintendencia Nacional de Salud.

b. Criterios.

- Circular Externa 202117000000055 del 17-09-2021 de la Supersalud.

c. Riesgo.

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

d. Recomendación.

- Establecer el respectivo cronograma de cumplimiento de la Circular Externa 202117000000055 del 17-09-2021 de la Supersalud.

e. Posición del auditado.
Se acepta la recomendación

f. Plan de mejoramiento.
Establecer el respectivo cronograma de cumplimiento de la Circular Externa 202117000000055 del 17-09-2021 de la Supersalud

IV. CONCLUSIONES.

4.1 Se logra el objetivo general de implementar un Sistema de Gestión Integral de Riesgos adoptando y adaptando los lineamientos del Modelo Integrado de Planeación y Gestión del Departamento Administrativo de la Función Pública, encontrándose en proceso incluir los riesgos en la caracterización de los procesos y definir el perfil de riesgos institucional.

4.2 Es necesario definir los indicadores claves de riesgo (KRI), que permitan capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

4.3 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.

4.4 El Hospital ha logrado avanzar en un 3.8 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 2021.

4.5 Continuar asegurando la gestión del riesgo en la entidad, este componente 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.

4.6 Considerar que previo a la Gestión del Riesgo, la entidad establece sus objetivos alineados con la planeación estratégica, dirigidos al cumplimiento de la normatividad vigente; partiendo del análisis del contexto interno, externo de la entidad y el del proceso, se identifican los riesgos para la consecución de sus objetivos en todos los niveles y los analiza como base para determinar cómo deben gestionarse, para lo cual la entidad debe contar con mecanismos efectivos de evaluación de riesgos, con el fin de establecer en nivel de riesgo inherente y residual.

4.7 Así mismo fortalecer el seguimiento a riesgos de fraude y corrupción (Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado) que pueda afectar el logro de los objetivos, en cumplimiento al artículo 73 de la Ley 1474 de 2011, relacionado con la prevención de los riesgos de corrupción.

4.8 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.

V. 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.

VI. 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: **Karina Ruíz De la Hoz**
Profesional de Auditoría Interna.
María Janeth Agudelo Arango
Profesional de Auditoría Interna

Heriberto Vargas Lema
Profesional de Auditoría Interna.
Julio E. Suescún Montoya
Técnico de Auditoría

Revisó:

Carlos Uriel López Ríos,
Jefe de Auditoría Interna.

Medellín, octubre de 2021.