Gerencia	1000.550
RESOLUCION No. **0377**	FECHA: 27-agosto-2024

"POR LA CUAL SE ACTUALIZA LA POLÍTICA INSTITUCIONAL PARA LA ADMINISTRACIÓN DEL RIESGO DE LA E.S.E. ISABU"

EL GERENTE DE LA EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA
E.S.E ISABU

En uso de sus facultades legales y reglamentarias y en especial las conferidas en el Acuerdo Municipal Nº 031 de 1997, Decreto No. 0053 del 18 de marzo de 2024 y diligencia de posesión No. 0266 del 22 de marzo del 2024.

CONSIDERANDO

Que la Constitución Política de Colombia en su artículo 49 dispone que la Atención en Salud y el Saneamiento Ambiental son servicios públicos a cargo del Estado, y se garantiza a todas las personas el acceso a los servicios de promoción, protección y recuperación de la salud.

Que el artículo 209 de la Constitución Política establece que: "La Administración Pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la Ley".

Que el Artículo 269 de la carta Política estipula que: "En las entidades Públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de Control Interno, de conformidad con lo que disponga la Ley".

Que la Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado, en el literal f del Artículo 2 establece como uno de los objetivos del Sistema de Control interno: "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".

Que el artículo 4 del Decreto 1537 de 2001 define la Administración del Riesgo como parte integral del Sistema de Control interno en las Entidades Públicas, para lo cual se deben establecer y aplicar Políticas de Administración del Riesgo.

Que el Gobierno Nacional estableció el Modelo Estándar de Control Interno-MECI para el Estado Colombiano, como una herramienta gerencial de control a la gestión pública, fundamentado en la cultura del control, y la responsabilidad y compromiso de la Alta Dirección para su implementación, a través del establecimiento de acciones, políticas, métodos, procedimientos, mecanismos de prevención, verificación y evaluación.

Que el Anexo Técnico del MECI, define el Componente Administración del Riesgo como el conjunto de elementos que le permiten a la entidad identificar, evaluar y gestionar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales.

Gerencia	1000.550
RESOLUCION No. **0377**	FECHA: 27-agosto-2024

Que el decreto 1011 de 3 de abril de 2006, establece el Sistema Obligatorio de Garantía de la Calidad en la Atención en salud, del Sistema General de Seguridad en Salud, sus características y el sistema único de acreditación como uno de sus componentes, definiéndolo como una herramienta de mejoramiento continuo, para alcanzar el cumplimiento de niveles superiores de calidad por parte las instituciones prestadoras de servicios de salud.

Que de acuerdo al Programa de Transparencia y ética pública el cual fue creado mediante el artículo 31 de la Ley 2195 de 2022, cuyo contenido modificó artículo 73 de la Ley 1474 de 2011 que creaba el Plan Anticorrupción y de Atención al Ciudadano señala como requisito previo la identificación de los riesgos de corrupción en los diferentes niveles de la entidad utilizando las metodologías definidas por la Secretaría de la Transparencia de la Presidencia de la República.

Que la Política de Administración del Riesgo, fija los lineamientos y las guías de acción a todos los servidores de la entidad, identificando los objetivos que se esperan lograr, las estrategias para alcanzar los objetivos, los riesgos que se van a controlar, las acciones a desarrollar y el talento humano requerido, facilitando el control, seguimiento y evaluación a su implementación y efectividad.

Que el Mapa de Riesgos es la herramienta conceptual, metodológica y operacional que permite valorar y administrar los riesgos de la entidad.

Que de conformidad con el artículo 133 de la Ley 1753 de 2015, establece que se deben integrar los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad y este Sistema Único de Gestión se debe articular con el Sistema de Control Interno; en este sentido el Modelo Integrado de Planeación y Gestión – MPIG surge como el mecanismo que facilitará la integración y articulación, determinando el campo de aplicación de cada uno de ellos con criterios diferenciales en el territorio nacional.

Que el Decreto 1499 de 2017 modificó el 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 1753 de 2015.

Que el modelo integrado de planeación y gestión (MIPG) define para su operación articulada la creación en todas las entidades 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, en este marco general, para una adecuada gestión del riesgo.

Que el Decreto 1499 de 2017, en su artículo 2.2.22.3.2 define el Modelo integrado de Planeación y Gestión (MIPG) como "... un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el sistema de salud.

Que de conformidad con la Resolución 5095 de 2018, se adopta el Manual de Acreditación en Salud Ambulatorio y hospitalario de Colombia versión 3,1"

Que por medio de la Resolución 0209 de 25 mayo 2018 adoptó e implementó la política para la Administración del Riesgo de la ESE ISABU.

Gerencia	1000.550
RESOLUCION No. **0377**	FECHA: 27-agosto-2024

Que se hace necesario actualizar la política de Gestión del Riesgo, con la metodología de matriz con criterios básicos para estructurar políticas institucionales definida por la ESE, en el marco del direccionamiento estratégico y la intencionalidad de los estándares de acreditación establecidos en la resolución 5095 2018.

Que el Departamento Administrativo de la Función Pública impartió lineamientos a través de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" mediante el cual se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo que articula los riesgos de gestión, corrupción y de seguridad de la Información.

Que por medio de la Resolución 0236 de 07 de junio 2019 se actualizó y adoptó la política para la Administración del Riesgo de la ESE ISABU.

Que por medio de la Resolución 0199 de 30 de marzo 2021 se actualizó y adoptó la política para la Administración del Riesgo de la ESE ISABU.

Que por medio de la Resolución 0581 de 21 de diciembre 2022 se actualizó y adoptó la política para la Administración del Riesgo de la ESE ISABU.

Que se hace necesario actualizar la política de Administración de Riesgos, respecto a las instrucciones generales relativas al Subsistema de Administración del Riesgo de Corrupción, Opacidad y Fraude (SICOF) y modificaciones de las circulares Externas 018 de 2015, 009 de 2016, 007 de 2017 y 003 de 2018, de acuerdo con la Circular Externa 20211700000005-5 de 17 de septiembre de 2021, expuestas por el marco normativo de la Superintendencia de Salud.

Que se hace necesario actualizar la política de Administración de Riesgos, de acuerdo a la Circular Externa 20211700000004-5 de 15 de septiembre de 2021, expuestas por el marco normativo de la Superintendencia de Salud, teniendo como asunto 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.

Que se hace necesario adoptar en la entidad la Política de Administración del Riesgo, que opere como lineamiento preciso acerca del tratamiento, manejo y seguimiento a los riesgos que puedan afectar el cumplimiento de los objetivos en la entidad.

Que mediante reunión del día 20 de agosto del 2024, bajo acta N°10, los miembros de la Junta Directiva de la E.S.E. ISABU, aprobaron la política Administración de Riesgos.

Que se hace necesario actualizar la política de Administración de Riesgos, asignando responsabilidades al proceso de Gestión de Talento Humano como segunda línea de defensa.

Por lo anteriormente expuesto,

RESUELVE

ARTICULO PRIMERO: Adoptar LA POLÍTICA DE ADMNISTRACIÓN DEL RIESGO DE LA EMPRESA SOCIAL DEL ESTADO – INSTITUTO DE SALUD DE BUCARAMANGA E.S.E

Gerencia	1000.550
RESOLUCION No. **0377**	FECHA: 27-agosto-2024

ISABU, cuyo texto se anexa formando parte integral de la presente resolución.

ARTICULO SEGUNDO: La Política de Administración del Riesgo será actualizada de acuerdo con las acciones de mejora continua provenientes del Modelo Integrado de Planeación y Gestión (MIPG), lineamientos del Departamento Administrativo de la Función Pública y al Marco Normativo de la Superintendencia de Salud.

Parágrafo. Las modificaciones que se requieran en todos los documentos que integran la Política de Administración de Riesgos se desarrollará de conformidad al PROCEDIMIENTO DE CREACIÓN, ACTUALIZACIÓN Y CONTROL DE LA INFORMACIÓN DOCUMENTADA DEL SIGC.

ARTICULO TERCERO: La presente resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Bucaramanga, a los veintisiete (27) días del mes de agosto de 2024.

HERNÁN DARIO ZARATE ORTEGÓN
Gerente ESE ISABU

Proyectó: Edinson Rodolfo Ríos Suarez – Apoyo Profesional – Oficina Asesora de Planeación.
Revisó: Martha Liliana Cordero Gómez- jefe Oficina Asesora de Planeación.
Revisó: Sandra Patricia García Tarazona - Profesional Especializado Gerencia.
Aprobó: Giovanny Humberto Durán Romero – jefe de la Oficina Asesora Jurídica.
Anexo: Documento Política Administración del Riesgo (26 folios).

POLÍTICA ADMINISTRACIÓN DEL RIESGO

El Gerente de la Empresa Social del Estado Instituto de Salud de Bucaramanga y sus colaboradores se comprometen a implementar el Sistema Integrado de Gestión de Riesgos, con la capacidad de identificar, evaluar, controlar, prevenir y mitigar los riesgos que puedan afectar el logro de los objetivos institucionales y, especialmente, el cumplimiento de los objetivos del Sistema General de Seguridad Social en Salud (SGSSS) y sus obligaciones contractuales, de acuerdo a los Subsistemas de Administración de Riesgos: en Salud, Operacional, Actuarial, Crédito, Liquidez, Mercado de Capitales, Fallas de Mercado, Reputacionales, SARLAFT, SICOF, Seguridad de la Información y Seguridad y Salud en el Trabajo; a través del Ciclo General de Gestión de Riesgos, identificación de riesgos, evaluación, medición del riesgo, selección de estrategias para el tratamiento y control de los riesgos, procesos y procedimientos, documentación, estructura organizacional, infraestructura tecnológica, divulgando la información y capacitando a los líderes de procesos sobre la administración del riesgo, contribuyendo de esta forma al logro de la Misión y los objetivos de la entidad.

1. OBJETIVO DE LA POLÍTICA

Dar los lineamientos generales para la Administración del Riesgos en la ESE ISABU y fortalecer el enfoque preventivo que conlleve al cumplimiento de los objetivos estratégicos del Plan de Desarrollo Institucional.

1.1. OBJETIVOS ESPECÍFICOS DE LA POLÍTICA

- Adoptar la metodología que permita a la ESE ISABU gestionar de manera efectiva los riesgos que afectan el logro de los objetivos institucionales.
- Suministrar herramientas que permitan implementar las diferentes etapas del ciclo general de riesgos y los elementos específicos de los diferentes Subsistemas de Administración de Riesgos.
- Fomentar una cultura de autocontrol y de gestión de riesgos por parte de los líderes de proceso y equipos de apoyo, de manera que sea una política organizacional que se interiorice en toda la estructura corporativa, incluyendo políticas de control interno.
- Promover la cultura institucional hacia una supervisión y administración basada en riesgos que desarrolle habilidades evaluativas sobre la calidad de la gestión de los riesgos por parte de los funcionarios y colaboradores de la entidad.
- Generar informes internos y externos, que permitan la toma de decisiones de manera oportuna en todas las instancias de la organización.
- Reducir la posibilidad de la materialización de los riesgos priorizados en cada proceso, definiendo actividades encaminadas a fomentar la transparencia en la gestión.
- Establecer los procedimientos aplicables para la adecuada implementación y funcionamiento de los elementos y las etapas de cada uno de los Subsistemas que conforman el Sistema Integrado de Gestión de Riesgos.
- Establecer el mapa de riesgos institucional que corresponderá a los riesgos extremos, altos y moderados de los Subsistemas de riesgos en: Salud, Operacional, Actuarial, Crédito, Liquidez, Mercado de Capitales, Fallas de Mercado, Reputacional, Lavado de Activos, Financiación del Terrorismo (SARLAFT) y Corrupción, Opacidad y Fraude (SICOF).
- Detectar y reportar las operaciones que se pretendan realizar o se hayan realizado, para intentar dar apariencia

de legalidad a operaciones vinculadas al lavado de activos o financiación del terrorismo.

- Señalar los lineamientos que debe adoptar la entidad frente a los factores de riesgo y los riesgos asociados de LA/FT/FPADM.
- Establecer las consecuencias que genera el incumplimiento del SARLAFT.
- Establecer el compromiso y la exigencia de que los funcionarios antepongan el cumplimiento de las normas en materia de administración de riesgo de LA/FT/FPADM al logro de las metas comerciales.
- Mejorar la eficiencia y eficacia en las operaciones de las entidades sometidas a inspección y vigilancia evitando situaciones de Corrupción, Opacidad y Fraude.
- Prevenir y mitigar la ocurrencia de actos de Corrupción, Opacidad y Fraudes, originados tanto al interior como al exterior de las organizaciones.
- Realizar una gestión adecuada de los Riesgos.

2. ALCANCE

La presente política es aplicable para todos los procesos y sedes de la Empresa Social del Estado Instituto de Salud de Bucaramanga E.S.E ISABU; la gestión del riesgo integra los conceptos relacionados con los riesgos asociados a la Planeación Estratégica, los Procesos establecidos en el Mapa de Procesos Institucional, Corrupción, Sistema de Seguridad y Salud en el Trabajo, Sistema de Gestión Ambiental, Sistema de Seguridad de la Información, Sistema de Administración del Riesgo de Lavado de Activos y de Financiación del Terrorismo, Sistema de Control Interno y Defensa Jurídica, así mismo, los lineamientos relacionados con el Modelo Integrado de Planeación y Gestión - MIPG.

3. RESPONSABLE

Junta Directiva, Representante Legal, Control Interno, Revisor Fiscal, Oficial de Cumplimiento SARLAFT, Oficinal de Cumplimiento SICOF, Comité de Riesgos, Líderes responsables de los Subsistemas de Gestión de Riesgos, Líderes de Procesos y equipos de apoyo.

4. DEFINICIONES

Política: Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (es decir, un número pequeño), deben ser apoyadas y aprobadas por las directivas de la entidad, y deben ofrecer direccionamientos a toda la organización o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la 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.[1]

[1] Guía para la Administración del riesgo y el diseño de controles en entidades públicas, Versión 5.

Gestión de Riesgo: Es un enfoque estructurado y estratégico liderado por la Alta Gerencia acorde con las políticas de gobierno organizacional de cada entidad, en donde se busca implementar un conjunto de acciones y actividades coordinadas para disminuir la probabilidad de ocurrencia o mitigar el impacto de un evento de riesgo potencial (incertidumbre) que pueda afectar los resultados y, por ende, el logro de los objetivos de cada entidad, así como el cumplimiento de los objetivos en el Sistema General de Seguridad Social en Salud (SGSSS) o sus obligaciones. Dentro de este conjunto de acciones se incluye, entre otros, el ciclo general de gestión de riesgo.

Riesgo en Salud: La probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo, que puede ser también el empeoramiento de una condición previa o la necesidad de requerir más consumo de bienes y servicios que hubiera podido evitarse.

Riesgo Operacional: La probabilidad que una entidad presente desviaciones en los objetivos misionales.

Riesgo Actuarial: La posibilidad de incurrir en pérdidas económicas.

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

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

Riesgo de Mercado de Capitales: La posibilidad de incurrir en pérdidas derivadas de un incremento no esperado, de sus obligaciones con acreedores tanto internos como externos, o la pérdida en el valor de sus activos,

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

Riesgo Reputacional: la posibilidad de toda acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de una entidad.

Riesgo de Lavado de Activos de la Financiación del Terrorismo (SARLAFT): es el sistema de prevención y control que deben implementar los Agentes del Sistema General de Seguridad Social en Salud (SGSSS) para la adecuada gestión del riesgo de Lavado de Activos / Financiación del Terrorismo - LA/FT.

Riesgo de Corrupción, Opacidad y Fraude (SICOF): Conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por el máximo órgano social u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

- Mejorar la eficiencia y eficacia en las operaciones de las entidades sometidas a inspección y vigilancia evitando situaciones de Corrupción, Opacidad y Fraude para el efecto.
- Prevenir y mitigar la ocurrencia de actos de Corrupción, Opacidad y Fraudes, originados tanto al interior como al exterior de las organizaciones.
- Realizar una gestión adecuada de los Riesgos.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.1

Control: Medida que permite reducir o mitigar un riesgo.1

Valoración del riesgo: Encauzar acciones hacia el uso eficiente de los recursos, la continuidad en la prestación de los servicios, la protección de los bienes utilizados para servir a la comunidad.

Matriz de riesgos: La matriz de riesgos, es un esquema grafico el cual permite visualizar la ubicación final de cada uno de los riesgos. Es decir, muestra la zona donde se encuentra cada uno de los riesgos antes de control y después de control. Facilitando la definición de las medidas de respuesta o tratamiento.

5. LINEAMIENTOS DE IMPLEMENTACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN DE RIESGOS

La E.S.E. ISABU a través del Sistema Integrado de Gestión de Riesgos implementará los siguientes Subsistemas de acuerdo a lo establecido en la normatividad vigente y a la clasificación de la entidad como Institución Prestadora de Servicios de Salud.

Subsistemas:

1. Riesgo en Salud
2. Riesgo Opacidad
3. Riesgo Actuarial
4. Riesgo de Crédito
5. Riesgo de Liquidez
6. Riesgo de Mercado de Capitales
7. Riesgos de Fallas de Mercado
8. Riesgo Reputacionales
9. Riesgo de Lavado de Activos y Financiación del Terrorismo - SARLAFT
10. Riesgo de Corrupción, Opacidad y Fraude - SICOF
11. Riesgo de Seguridad de la Información
12. Riesgo de Seguridad y Salud en el Trabajo

Cabe resaltar que los riesgos de Corrupción definidos en el componente 1 Mapa de Riesgo de Corrupción del Plan Anticorrupción y Atención al Ciudadano – PAAC, estarán inversos en el Subsistema Riesgo de Corrupción, Opacidad y Fraude – SICOF.

La entidad para la implementación del Sistema Integrado de Gestión de Riesgos y sus Subsistema deberá adoptar los lineamientos generales que permitirán a la entidad 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 y las normas vigentes que reglamentan cada Subsistema de riesgos.

Tabla 1 Lineamientos generales de Implementación del Sistema Integrado de Gestión de Riesgos

No	Lineamiento	Descripción del Lineamiento

1	**Ciclo General de Gestión de Riesgos**	Análisis de los subsistemas integrados de gestión de riesgos que aplican a la E.S.E ISABU de acuerdo a la norma, con el objetivo de identificar el área responsable y líder responsable de cada subsistema. Cada Subsistema de Administración de Riesgos, se aplica las etapas del Ciclo General de Gestión de Riesgos que son: **a. Identificación de riesgos:** Consiste en reconocer, explorar exhaustivamente y documentar todos los riesgos internos y externos que podrían afectar tanto los objetivos de la entidad como la salud de los usuarios a su cargo, en los casos que aplica, identificando sus causas, efectos potenciales y la posible interrelación entre los diferentes tipos de riesgos, para lo cual se recomienda la utilización de normas técnicas nacionales o internacionales. Para esta identificación, la entidad podrá seleccionar las metodologías y técnicas que consideren más adecuadas, dentro de las que se encuentran estudios científicos, encuestas, entrevistas estructuradas con expertos, talleres, lluvia de ideas, técnicas de escenarios, entre otros. **b. Evaluación y medición de riesgos:** Es la valoración de los efectos asociados a los riesgos que han sido identificados, considerando la frecuencia y la severidad de su ocurrencia. También se deberá considerar el análisis de los riesgos inherentes y residuales, y su participación en el riesgo neto global. Se entenderá por valoración del riesgo, la medida cualitativa o cuantitativa de su probabilidad de ocurrencia y su posible impacto. **c. Selección de estrategias para el tratamiento y control de los riesgos:** Una vez identificados y evaluados los riesgos, deben compararse con los límites (tolerancia) de riesgos aprobados por la instancia definida en el Gobierno Organizacional de la entidad y su política de riesgos, siempre dentro del marco normativo establecido. Todo riesgo que exceda los límites o desviaciones aceptadas, debe ser objeto de actividades de mitigación y control a fin de regresar al nivel de riesgo tolerado, conforme la estrategia adoptada. En cuanto a los riesgos en salud, estos límites hacen referencia a los máximos permitidos por la normatividad vigente, estándares internacionales y sin perjuicio de lo anterior, de acuerdo con lo que establezca la entidad en sus políticas, siempre que estén en pro del beneficio de la población de su área de influencia. Se deben determinar las acciones tendientes a gestionar los riesgos a los que se ve expuesta la entidad, de acuerdo con los niveles de riesgo determinados y las tolerancias al riesgo definidas. Todas las acciones de gestión del riesgo deberán identificar formalmente responsables, plazos, formas de ejecución y reportes de avances, los cuales deben corresponder a la complejidad de la operación de la entidad. Asimismo, deberán estar aprobadas por la instancia que corresponda. **d. Seguimiento y monitoreo:** Una vez establecidos los posibles mecanismos o un conjunto de estos, para la mitigación y control de los riesgos que se han identificado como relevantes para la entidad y después de realizar un análisis de causa y efecto para determinar los puntos más críticos a intervenir con mayor prelación, la entidad deberá poner en práctica tales mecanismos y reflejarlos en un plan de implementación de las acciones planteadas en la fase anterior, guardando correspondencia con las características particulares de cada entidad, teniendo en cuenta el grado de complejidad, el tamaño y el volumen de sus operaciones. Con el fin de realizar el respectivo seguimiento y monitoreo permanente y continuo de la evolución de los perfiles de riesgo y la exposición frente a posibles pérdidas a causa de la materialización de cada uno de los riesgos identificados, la entidad debe desarrollar un sistema de alertas tempranas que facilite la rápida detección, corrección y ajustes de las deficiencias en cada uno de sus Subsistemas de Administración de Riesgo para evitar su materialización. Lo anterior, con una periodicidad acorde con los eventos y factores de riesgo identificados como potenciales, así como con la frecuencia y naturaleza de estos. El diseño de dicho sistema de alertas debe incluir la definición de los límites máximos de exposición o niveles aceptables de riesgo previamente establecidos por la entidad teniendo en cuenta los análisis realizados, la normatividad vigente y los criterios definidos en esta política de gestión de riesgos. Las mediciones de riesgos esperadas, los riesgos derivados y sus controles deben ser contrastados regularmente con la realidad observada, de forma tal que permita establecer si los Subsistemas de Administración de Riesgos han logrado su mitigación y la corrección oportuna y efectiva de eventuales deficiencias. De esta manera la entidad debe contar con indicadores de gestión para hacer seguimiento a la administración de los riesgos residuales y netos, y que estos a su vez se encuentren y se mantengan en los niveles de aceptación previamente establecidos por la entidad. De llegarse a presentar desviaciones o que se superen los límites previamente establecidos, se deben establecer planes de contingencia para intervenir y tratar los diferentes riesgos, teniendo en cuenta la variabilidad de los riesgos identificados, con el propósito de ajustar las desviaciones lo más pronto posible. Todas las acciones y actividades incluidas en estos planes deben contener la definición de los estándares de seguimiento y monitoreo, además de contar con un responsable, plazos, periodicidad, reportes de avance y de evaluaciones periódicas sobre las estrategias seleccionadas que incluyan el monitoreo de los indicadores propuestos para el seguimiento de las acciones de gestión del riesgo planteadas, los cuales deben ser definidos mediante un cronograma y ser objeto de un proceso de seguimiento, verificación y calidad de la información. Los planes de contingencias resultantes del seguimiento a riesgos deben ser coherentes con otras medidas contingentes o planes de mejoramiento resultantes de otras actividades de control, internas o externas, a fin de lograr soluciones estructurales e integrales a las problemáticas

		identificadas. En esta etapa cobra importancia la implementación de mecanismos de retroalimentación, donde se promueva la comunicación dinámica y continua, la entrega de reportes gerenciales y de monitoreo donde se evalúen los resultados obtenidos, su evolución y la ejecución de los controles y estrategias implementadas para mejorar el desempeño en la mitigación de los factores de riesgo en cada uno de los Subsistemas de Administración de Riesgo, dirigidos a todos los involucrados tanto externos como internos, en especial a los órganos de seguimiento definidos por el Gobierno Organizacional de cada entidad.
2	**Política de Gestión de Riesgos**	La política debe ser revisada como mínimo una vez al año, con el fin de actualizarla a las condiciones particulares de la entidad y a las del mercado en general. Tanto la aprobación como las modificaciones que se efectúen a dichas políticas, deben tener constancia en acta del máximo órgano de administración, de la Junta Directiva o quien haga sus veces. Asimismo, esta política debe ser conocida por todos los funcionarios de la organización y se debe establecer mecanismos de comunicación y socialización que permita que los responsables a cargo de las funciones de la gestión de los diversos riesgos conozcan los hechos que pueden impactar sus funciones.
3	**Documentación para la Gestión de Riesgos**	Generar la documentación interna y externa necesaria para la adecuada gestión de los riesgos. Entre ellos se encuentran los manuales, instructivos, volantes, intranet, páginas web, actas, registros, entre otros. Cada Subsistema de Administración de Riesgos deben quedar plasmados en documentos y registros, garantizando la integridad, oportunidad, trazabilidad, confiabilidad y disponibilidad de la información allí contenida. Los procesos y procedimientos deben adoptar y plasmar mediante documentos controlados, en los cuales deben quedar claramente definidas las funciones, responsabilidades y atribuciones específicas para cada uno de los funcionarios de los diferentes órganos de dirección, administración y control involucrados en la administración de los diversos riesgos. **Documentar:** **a.** Las metodologías y procedimientos para la identificación, medición, control y monitoreo de los riesgos identificados. A su vez, el establecimiento de los niveles de aceptación y límites de exposición. **b.** Los roles y responsabilidades de quienes participan en la gestión de los diversos riesgos identificados, especialmente los prioritarios. **c.** Las medidas necesarias para asegurar el cumplimiento de las políticas y objetivos de cada uno de los Subsistemas de Administración de Riesgos. **d.** Roles, responsabilidades y acciones de los órganos de control interno frente a cada uno de los Subsistemas de Administración de Riesgos. **e.** Las estrategias de capacitación y divulgación de cada uno de los Subsistemas de Administración de Riesgos.
4	**Área de Gestión de Riesgos**	La ESE ISABU conformará el área de Gestión de Riesgos con las oficinas de: Calidad, Planeación y Jurídica y será liderada por la Oficina de Planeación, esta área brindará apoyo, orientación y evaluación, que tendrá a su cargo la administración y gestión de los diferentes riesgos a los cuales la entidad se encuentra expuesta (incluyendo los riesgos priorizados) a través de la identificación, medición, control y monitoreo de cada uno de ellos de tal manera que se realice la evaluación continua del ciclo para detectar las desviaciones y generar insumos para la formulación de los planes de mejoramiento y demás información que requiera el Comité de Riesgos, en los casos que aplique, mediante el trabajo conjunto con todas las áreas.
5	**Comité de Gestión de Riesgos**	El Comité de Riesgos en caso de que la entidad decida establecerlo, la Junta Directiva nombrará el comité y define sus funciones y aprueba su reglamento, de acuerdo con las normas legales que le apliquen. El Comité de Gestión de Riesgos está encargado de liderar la implementación y desarrollar el monitoreo de la política y estrategia de la gestión de riesgos de la entidad.
6	**Órgano de control**	El diseño, desarrollo y ejecución de políticas para la gestión de riesgos deben contemplar procesos de auditoría y control tanto internos como externos, mediante los cuales se audite el cumplimiento de las políticas y procedimientos establecidos. Los órganos de control deben abarcar todas las áreas de la organización, aplicando para cada una de ellas los objetivos, principios, elementos y actividades de control, información, comunicación y otros fundamentos del sistema. No obstante, por su particular importancia se considera pertinente entrar a analizar algunos aspectos relacionados con las áreas de salud, financiera y tecnología. Los órganos de control serán, por lo menos, Revisoría Fiscal y la Oficina de Control Interno. Estos deberán identificar las operaciones realizadas con entidades o personas vinculadas a la entidad, y promover revisiones independientes para validar la efectividad del Sistema Integrado de Gestión de Riesgos de la entidad y de los Subsistemas por los cuales está conformado, además de las responsabilidades y obligaciones que se encuentren establecidas en otras disposiciones legales, estatutarias o en reglamentos. Estos órganos de control efectuaran la revisión y evaluación del Sistema Integrado de Gestión de Riesgos, compuesto

		por cada uno de los Subsistemas de Administración de Riesgos, así como por otros riesgos identificados por cada entidad, las cuales deben informar oportunamente a los órganos competentes, de las inconsistencias y falencias que detecte respecto a la implementación de los diferentes Subsistemas de Administración de Riesgos o la violación a los controles y límites establecidos.
7	**Infraestructura Tecnológica**	Disponer y utilizar la infraestructura tecnológica y los sistemas necesarios para garantizar el funcionamiento efectivo, eficiente y oportuno del Sistema Integrado de Gestión de Riesgos, los cuales deben generar informes confiables sobre dicha labor y contar con un soporte tecnológico acorde con sus actividades, operaciones, riesgos asociados y tamaño. Además, deben contar con procesos que permitan realizar un control adecuado del cumplimiento de las políticas y límites establecidos, además de contar con un plan de conservación, custodia y seguridad de la información tanto documental como electrónica.
8	**Divulgación de la información y capacitaciones**	Diseñar, programar y coordinar planes de divulgación y capacitación como mínimo una vez al año a todas las áreas y funcionarios de la entidad, con mayor énfasis a las áreas involucradas en la gestión de estos riesgos, sobre las políticas, procedimientos, herramientas y controles adoptados por parte de la entidad para dar cumplimiento al Sistema Integrado de Gestión de Riesgos. La divulgación y capacitación sobre cada uno de los Subsistemas de Administración de Riesgos deben hacer parte de los procesos de inducción de los nuevos empleados. Se debe dejar constancia de las capacitaciones realizadas por medio de la presentación de una prueba de los temas expuestos a los participantes, para incentivar la adherencia y el entendimiento, y, en donde se indique como mínimo la fecha, los temas tratados y el nombre de los asistentes. Por otro lado, la entidad debe diseñar un sistema efectivo, veraz, eficiente y oportuno de manejo de la información capaz de generar reportes, tanto internos como externos, que garantice el funcionamiento de cada uno de los Subsistemas de Administración de Riesgos, teniendo en cuenta los procesos y procedimientos establecidos para cada uno. Este sistema de información debe ser funcional y permitir la dirección y control de la operación en forma adecuada. Además, estos sistemas deben garantizar que la información cumpla con los criterios de seguridad (confidencialidad, integridad y disponibilidad), calidad (completitud, validez y confiabilidad) y cumplimiento, para lo cual se deben establecer controles generales y específicos para la entrada, el procesamiento y la salida de la información, atendiendo su importancia relativa y nivel de riesgo. **Divulgación de la Información Interna** Como resultado del monitoreo y control de cada uno de los riesgos identificados y especialmente los prioritarios, las entidades deben elaborar reportes semestrales como mínimo, que permitan establecer el perfil de riesgo de éstas. Asimismo, debe elaborar informes de gestión al cierre de cada ejercicio contable sobre el cumplimiento de las políticas, los límites establecidos y su grado de cumplimiento, el nivel de exposición a los diferentes riesgos a los que se ven expuestas las entidades que incluya los prioritarios y la cuantificación de los efectos de la posible materialización de estos sobre la salud de la población de su área de influencia, las utilidades, el patrimonio y el perfil de riesgo de cada entidad. Los informes deben dirigirse por lo menos al Representante Legal, a la Junta Directiva y los líderes de los procesos involucrados, los cuales deben quedar plasmados en acta donde se socialicen estos informes. Estos informes deben ser presentados de manera comprensible y deben mostrar las exposiciones por tipo de riesgo y de la manera más desagregada, detallada y clara posible. **Divulgación de la Información Externa** En el informe de gestión, al cierre de cada ejercicio contable, debe incluir en las notas a los estados financieros un apartado sobre la gestión adelantada en materia de administración como mínimo de los subsistemas de gestión de riesgos. En este sentido, las notas deberán contener un resumen de su situación en materia de la administración de dichos riesgos con información tanto cualitativa como cuantitativa. Por un lado, la información cualitativa es indispensable para elaborar y proveer una mejor compresión de los estados financieros de las entidades, por tanto, es necesario que la entidad informe sobre sus objetivos de negocio, estrategias y filosofía en la gestión de riesgos y los controles implementados en cada uno para mitigarlos. Además, la información revelada debe considerar los cambios potenciales en los niveles de riesgo, cambios materiales en las estrategias y límites de exposición para cada uno de los Subsistemas de Administración de Riesgos. Por otro lado, la entidad debe revelar al público en general, la información cuantitativa sobre la gestión integral de los riesgos, como resultado de sus políticas y metodologías internas aplicadas para su control, de acuerdo con lo que la entidad considere pertinente revelar, sin perjuicio de aquella que sea de carácter privilegiado, confidencial o reservado, respecto de la cual se debe adoptar todas las medidas que consideren necesarias para su protección, incluyendo lo relacionado con su almacenamiento, acceso, conservación, custodia y divulgación.
9	**Ética y Conducta**	Incorporar en el Código de Conducta y Buen Gobierno de la entidad los lineamientos de ética y conducta que orienten el actuar de los funcionarios de la entidad para el oportuno y efectivo funcionamiento de cada uno de los Subsistemas de Administración de Riesgos e inclusión de disposiciones sobre la confidencialidad de la información, manejo de información

		privilegiada y conflictos de interés.

5.1 RESPONSABLE DE LOS SUBSISTEMAS INTEGRADOS DE GESTIÓN DE RIESGOS (SIGR)

El Instituto de Salud de Bucaramanga, tiene implementado un Mapa de Procesos, el cual le permite alcanzar los resultados y alinear sus actividades en una sola dirección, para brindar servicios de calidad y lograr la satisfacción de los clientes, usuarios y su familia.

Teniendo en cuenta que la entidad no tiene en su mapa de procesos Área de Gestión de Riesgos, se establece que el Área de Gestión de Riesgos para la E.S.E. ISABU estará conformado por la Oficina Asesora de Calidad, Oficina Asesora Jurídica y la Oficina de Planeación y el área será liderada por la Oficina Asesora de Planeación.

Para el diseño y adopción de cada uno de los Subsistemas de Administración de Riesgos, se establecen como responsables a cargo de los órganos de dirección, administración y el revisor fiscal de la entidad dentro de su Código de Conducta y Buen Gobierno establecidos en la tabla 2.

Tabla 2 Responsables de los Subsistemas Integrados de Gestión de Riesgos

SUBSISTEMA INTEGRADO DE GESTIÓN DE RIESGOS (SIGR)	ÁREA RESPONSABLE	LÍDERES RESPONSABLES
Subsistema Riesgo de Salud	1. Gestión de Calidad	1.Jefe Oficina Asesora de Calidad 1.Seguridad del paciente
Subsistema Riesgo Operacional	1.Gestión de Calidad 2.Gestión Jurídica 3.Gestión Planeación y Direccionamiento Estratégico	1.Jefe Oficina de Asesora de Calidad 2.Jefe Oficina Asesora Jurídica 3.Jefe Oficina Asesora de Planeación
Subsistema Riesgo Actuarial	1.Subgerencia Administrativa 2.Subgerencia Científica	1.Subgerente Administrativo 2.Subgerente Científico 3.Directora técnica Unidades Hospitalarias
Subsistema Riesgo de Crédito	1.Subgerencia Administrativa	1.Subgerente Administrativo
Subsistema Riesgo de Liquidez	1.Subgerencia Administrativa	1.Tesorero General
Subsistema Riesgo de Mercado de Capitales	1.Subgerencia Administrativa	1.Tesorero General
Subsistema Riesgo Fallas de Mercado	1.Subgerencia Administrativa 2.Subgerencia Científica	1.Subgerente Administrativo 2.Subgerente Científico
Subsistema Riesgo y Reputacionales	1.Gestión Planeación y Direccionamiento Estratégico	1.Jefe Oficina Asesora de Planeación
Subsistema Riesgos de Lavado de Activos, Financiación del terrorismo (SARLAFT)	1.Subgerencia administrativa	1.Subgerente Administrativo 2. Tesorero General
Subsistema Riesgo de Corrupción Opacidad y Fraude (SICOF)	1.Gestión Planeación y Direccionamiento Estratégico	1. Jefe Oficina Asesora de Planeación
Subsistema Riesgos de Seguridad de la Información	1. Gestión de las TICS	1.Subgerente Administrativo 2.Profesional especializado TICS
Subsistema Riesgos Seguridad y Salud en el Trabajo	1. Gestión de Talento Humano	1.Profesional de Talento Humano 2.Profesional en Seguridad y Salud en el Trabajo

5.2 RESPONSABILIDAD Y COMPROMISOS FRENTE AL SISTEMA INTEGRADO GESTIÓN DEL RIESGO Y CONTROL

La gestión de riesgos, por tratarse de una actividad que conjuga un conjunto de elementos de control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales, depende de la decidida intervención y participación de la Junta Directiva, alta dirección, los servidores públicos y contratistas. Por ello es preciso identificar los diferentes roles y responsabilidades de los actores en la implementación, operación, seguimiento y fortalecimiento, propuesto en el Modelo Integrado de Planeación, Gestión -MIPG, Circular externa 20211700000004-5 de 2021, Circular

externa 20211700000005-5 de 2021.

Las responsabilidades y compromisos frente al Sistema Integrado de Gestión de Riesgos se establece de acuerdo al Modelo Integrado de Planeación y Gestión en la Dimensión 7 Control Interno, la cual promueve el mejoramiento continuo de las entidades, razón por la cual éstas deben establecer acciones, métodos y procedimientos de control y de gestión del riesgo, así como mecanismos para la prevención y evaluación de éste y establece el Esquema de líneas de Defensa, siendo este esquema de asignación de responsabilidades para la gestión de riesgos y del control en una entidad, a través de cuatro roles: línea estratégica, integrada por la alta dirección de la entidad y el comité institucional de control interno; primera línea de defensa, integrada por los gerentes públicos y líderes de procesos, programas y proyectos; segunda línea de defensa, integrada por las oficinas de planeación, líderes de otros sistemas de gestión o comités de riesgos; tercera línea de defensa, integrada por las oficinas de control interno. Este esquema permite distribuir estas responsabilidades en varias áreas y evitando concentrarlas exclusivamente en las oficinas de control.

La interacción entre las líneas que conforman el Esquema de Líneas de Defensa, como eje articulador entre la Dimensión 7 y las demás dimensiones del Modelo Integrado de Planeación y Gestión MIPG, se define que la implementación del Sistema Integrado de Gestión de Riesgos de la ESE ISABU para las responsabilidades y compromisos frente al SIGR se organiza de acuerdo al Esquema de Líneas de Defensa como se establece en la tabla 3.

Tabla 3 Implementación del SIGR de acuerdo con el Esquema de Líneas de Defensa

LÍNEA ESTRATÉGICA *Define, controla y supervisa.*	**Responsables:** Junta Directiva, Representante Legal, Comité Institucional de Coordinación de Control Interno.

Responsabilidades de la Junta Directiva frente al Riesgo:

Aprobar la política de la entidad en materia de administración de todos los riesgos que pueden afectar los objetivos de la entidad y que son presentadas por el Comité de Riesgos, a partir del trabajo con el área de gestión de riesgos, en caso de que existan, órgano equivalente o de las diferentes áreas de la entidad.

a. Aprobar los reglamentos, manuales de procesos, procedimientos y funciones de las áreas pertenecientes a la entidad, así como sus respectivas actualizaciones.
b. Aprobar el Código de Conducta y de Buen Gobierno. el sistema de control interno, la estructura organizacional y tecnológica del Sistema Integrado de Gestión de Riesgos.
c. Aprobar el diseño y definir la periodicidad de los informes internos para los reportes de la gestión de los riesgos, especialmente los prioritarios que se van a presentar a las diferentes áreas de la entidad.
d. Aprobar el marco general de indicadores de alerta temprana y los límites de exposición como mínimo a los riesgos prioritarios.
e. Garantizar los recursos técnicos y humanos que se requieran para implementar y mantener en funcionamiento el Sistema Integrado de Gestión de Riesgos, teniendo en cuenta las características de cada riesgo y el tamaño y complejidad de la entidad.
f. Realizar el nombramiento del Comité de Riesgos en caso de que la entidad decida establecerlo, definir sus funciones y aprobar su reglamento, de acuerdo con las normas legales que le apliquen.
g. Pronunciarse y hacer seguimiento sobre los informes periódicos que elabore el Comité de Riesgos y la Revisoría Fiscal, respecto a los niveles de riesgo asumidos por la entidad, las medidas correctivas aplicadas para que se cumplan los límites de riesgo previamente establecidos y las observaciones o recomendaciones adoptadas para el adecuado desarrollo de cada uno de los Subsistemas de Administración de Riesgo.
h. Designar la(s) instancia(s) responsable(s) del diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de la exposición como mínimo a los riesgos prioritarios en los casos que aplique.
i. Aprobar las metodologías de segmentación, identificación, medición, control y monitoreo de lo diferentes Subsistemas de Administración de Riesgos, diseñadas por la instancia responsable.
j. Monitorear el cumplimiento de los lineamientos de los diferentes Subsistemas de Administración de Riesgos promoviendo su continuo fortalecimiento y que la toma de decisiones este en función de la selección e implementación de las estrategias para el tratamiento y control de los diversos riesgos y de su comportamiento.

Responsabilidades de la Junta Directiva frente al subsistema SARLAFT:

a. Diseñar y actualizar las políticas para la prevención y control del riesgo de LA/FT/FPADM que harán parte del SARLAFT, para una posterior aprobación por la Asamblea o el máximo órgano social o quien haga sus veces.

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

Responsabilidades de la Junta Directiva frente al subsistema SICOF:

a. Definir y aprobar las estrategias y políticas generales relacionadas con el SICOF, con fundamento en las recomendaciones del Oficial de Cumplimiento o persona encargada por la entidad para la ejecución del SICOF.
b. Adoptar las medidas necesarias para garantizar la independencia del Oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF y hacer seguimiento a su cumplimiento.
c. Aprobar el Manual de prevención de la Corrupción, la Opacidad y el Fraude y sus actualizaciones.
d. Hacer seguimiento y pronunciarse sobre el perfil de Corrupción, Opacidad y Fraude de la entidad.
e. Pronunciarse sobre la evaluación periódica del SICOF, que realicen los órganos de control.
f. Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SICOF.
g. Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente e Oficial de Cumplimiento o persona encargada por la entidad para la ejecución del SICOF.
h. Conocer los informes relevantes respecto del SICOF, e impartir las órdenes necesarias para que se adopten las recomendaciones y correctivos a que haya lugar.
i. Efectuar seguimiento en sus reuniones ordinarias a través de informes periódicos que presente el oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF, sobre la gestión del mismo en la entidad y las medidas adoptadas para el control o mitigación de los riesgos más relevantes, por lo menos cada 6 meses.
j. Evaluar las recomendaciones relevantes sobre el SICOF, que formulen el oficial de cumplimiento o persona encargada por la entidad para la ejecución del mismo y los órganos de control interno, adoptar las medidas pertinentes, y hacer seguimiento a su cumplimiento.
k. Analizar los informes que presente el oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF respecto de las labores realizadas para evitar que la entidad sea utilizada como instrumento para la realización de actividades delictivas, actos de Corrupción, Opacidad o Fraude y evaluar la efectividad de los controles implementados y de las recomendaciones formuladas para su mejoramiento.

Todas las decisiones y actuaciones que se produzcan en desarrollo de las atribuciones antes mencionadas deben constar por escrito en el acta de la reunión respectiva y estar debidamente motivadas.

Responsabilidades Representante Legal frente al Riesgo:

a. Apoyar y garantizar el efectivo cumplimiento de las políticas definidas por la Junta Directiva.
b. Adelantar un seguimiento permanente del cumplimiento de las funciones del Comité de Riesgos y mantener informada a la Junta Directiva.
c. Conocer y discutir los procedimientos a seguir en caso de sobrepasar o exceder los límites de exposición frente a los riesgos, así como los planes de contingencia a adoptar respecto de cada escenario extremo.
d. Hacer seguimiento y pronunciarse respecto a los informes periódicos que presente el Comité de Riesgos sobre el grado de exposición de riesgos asumidos por la entidad y los controles realizados, además de los informes presentados por la Revisoría Fiscal. Lo anterior debe plasmarse en un informe a la Junta Directiva o, quien haga sus veces, y hacer énfasis cuando se presenten situaciones anormales como mínimo en algún riesgo prioritario o existan graves incumplimientos a las políticas, procesos y procedimientos para cada uno de los Subsistemas de Administración de Riesgos.
e. Realizar monitoreo y revisión de las funciones del área de control interno.
f. Velar porque se dé cumplimiento a los lineamientos establecidos en el Código de Conducta y Buen Gobierno de la entidad en materia de conflictos de interés y uso de información privilegiada que tengan relación con el Sistema Integrado de Gestión de Riesgos.

g. Vigilar cuidadosamente las relaciones de todas las personas que hacen parte de la entidad tanto interna como externamente, para identificar y controlar de manera eficiente los posibles conflictos de interés que puedan presentarse.
h. Informar de manera oportuna mediante Oficio a la Superintendencia Nacional de Salud, acerca de cualquier situación excepcional que se presente o prevea que pueda presentarse como mínimo en el ámbito de la administración de los riesgos prioritarios, de las causas que la originan y de las medidas que se propone poner en marcha por parte de la entidad para corregir o enfrentar dicha situación, si procede.
i. Evaluar el estado del Sistema de Control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.

Responsabilidades Representante Legal frente al SICOF:

a. Adelantar un seguimiento permanente de las etapas y elementos constitutivos del Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF.
b. Designar el área o cargo que actuará como responsable de la implementación y seguimiento del SICOF.
c. Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la Administración de este Riesgo implica para la entidad.
d. Velar por la correcta aplicación de los controles del Riesgo inherente, identificado y medido.
e. Recibir y evaluar los informes presentados por el oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF, de acuerdo con los términos establecidos en la presente Circular.
f. Velar porque las etapas y elementos del SICOF se cumplan.
g. Velar porque se implementen los procedimientos para la adecuada Administración del Corrupción, Opacidad y Fraude a que se vea expuesta la entidad en desarrollo de su actividad.

Responsabilidades del Comité Institucional de Coordinación de Control Interno:

a. Conocer y resolver los conflictos de interés que afectan la independencia de la auditoria.
b. Someter a aprobación del representante legal de la Empresa Social del Estado Instituto de Salud de Bucaramanga E.S.E ISABU la política de administración del riesgo previamente estructurada por parte de la Oficina Asesora de Planeación, como segunda línea de defensa en la entidad, hacer seguimiento para su posible actualización y evaluar su eficiencia frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta.
c. Verificar la efectividad del sistema de control interno para procurar el incumplimiento de los planes, metas y objetivos previstos, constatando que el control este asociado a todas las actividades de la organización y que se apliquen los mecanismos de participación ciudadana, conforme a las directrices dadas por el Comité de Coordinación del Sistema de Control Interno.
d. Evaluar, decidir y adoptar oportunamente las propuestas de mejoramiento del sistema de control interno que presente en sus informes la Oficina de Control Interno.
e. Analizar los informes de auditoría, seguimientos y evaluaciones que presente el jefe de control interno de la entidad, a fin de determinar las mejoras a ser implementadas en la Empresa Social del Estado Instituto de Salud de Bucaramanga E.S.E ISABU.

PRIMERA LÍNEA DE DEFENSA *Desarrolla e implementa procesos de control y gestión de riesgos*	**Responsables:** Líderes de procesos y Oficiales de cumplimiento SARLAFT – SICOF – Sistema Seguridad de la Información.

Responsabilidades de los Líderes de Procesos frente al Riesgo.

a. Identificar y valorar los riesgos que puedan afectar los planes, programas, proyectos y procesos a su cargo y actualizarlo cuando se requiera.
b. Establecer acciones de control detectivas y preventivas para los riesgos identificados.
c. Realizar seguimiento o monitoreo y análisis a los controles de los riesgos según periodicidad establecida para mitigar los riesgos identificados alineados con las metas y objetivos de la ESE ISABU y proponer mejoras a la gestión del riesgo en su proceso.
d. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
e. Actualizar el mapa de riesgos cuando la administración de los mismos lo requiera.
f. Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
g. Establecer y ejecutar la actuación correctiva y oportuna ante la materialización de los riesgos identificados.
h. Informar a el Área de Gestión de Riesgos (segunda línea de defensa) sobre los riesgos materializados en los planes, programas, proyectos, y/o procesos a su cargo.
i. Reportar a la Oficina de Control Interno los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.

Responsabilidades del Oficial de Cumplimiento frente al Subsistema SARLAFT.

a. Velar por el efectivo, eficiente y oportuno funcionamiento de las etapas que conforman el SARLAFT.
b. Elaborar y desarrollar los procesos y procedimientos a través de los cuales se llevarán a la práctica las políticas aprobadas para la implementación del SARLAFT.
c. Identificar las situaciones que puedan generar riesgo de LA/FT en las operaciones que realiza la entidad.
d. Implementar y desarrollar los controles a las situaciones que puedan generar riesgo de LA/FT en las operaciones, negocios o contratos que realiza la entidad.
e. Realizar seguimiento o monitoreo a la eficiencia y la eficacia de las políticas, procedimientos y controles establecidos.

f. Velar por el adecuado archivo de los soportes documentales y demás información relativa al riesgo de LA/FT de la entidad.
g. Participar en el diseño y desarrollo de los programas de capacitación sobre el riesgo de LA/FT y velar por su cumplimiento.
h. Proponer a la Junta Directiva o quien haga sus veces, los ajustes o modificaciones necesarios a las políticas del SARLAFT.
i. Proponer a la administración la actualización del manual de procedimientos y velar por su divulgación a los funcionarios.
j. Recibir y analizar los reportes internos de posibles operaciones inusuales, intentadas o sospechosas y realizar el reporte de estas dos últimas a la Unidad de Información y Análisis Financiero – UIAF.
k. Realizar todos los reportes a la SNS, incluidas las actas de aprobación de la política, así como el manual de procedimientos.
l. Mantener actualizados los datos de la entidad y el oficial de cumplimiento con la UIAF. utilizando los canales de comunicación correspondientes.
m. Informar a la UIAF cualquier cambio de usuario del Sistema de Reporte en Línea-SIREL
n. Gestionar adecuadamente los usuarios del Sistema de Reporte en Línea - SIREL.
o. Revisar los documentos publicados por la UIAF en la página web como anexos técnicos, manuales y utilidades que servirán de apoyo para la elaboración de los reportes.
p. Diseñar las metodologías de segmentación, identificación, medición y control del SARLAFT.
q. Elaborar y someter a la aprobación de la Junta Directiva o el órgano que haga sus veces, los criterios objetivos para la determinación de las operaciones sospechosas, así como aquellos para determinar cuáles de las operaciones efectuadas por usuarios serán objeto de consolidación, monitoreo y análisis de operaciones inusuales.
r. Presentar cuando menos, de forma semestral a los administradores y anualmente a la Junta Directiva o quien haga sus veces, un informe por escrito donde exponga el resultado de su gestión.

Responsabilidades del Oficial de Cumplimiento Suplente frente al Subsistema SARLAFT

a. Para el caso del Oficial de Cumplimiento suplente, debidamente designado al interior de la organización (quien será el reemplazo en ausencia parcial o total del Oficial de Cumplimiento), debe cumplir como mínimo, los requisitos establecidos en los literales b al f del presente numeral.

Responsabilidades del Oficial de Cumplimiento frente al Subsistema SICOF.

a. Diseñar y someter a aprobación de la Junta Directiva u órgano que haga sus veces, el manual de prevención de la Corrupción, la Opacidad y el Fraude y sus actualizaciones.
b. Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva.
c. Diseñar y proponer para aprobación de la Junta Directiva o quien haga sus veces, la estructura, instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente sus Riesgos de prevención y detección de la Corrupción, la Opacidad y el Fraude, en concordancia con los lineamientos, etapas y elementos mínimos previstos en esta Circular.
d. Desarrollar e implementar el sistema de reportes, internos y externos, de prevención y detección de la Corrupción, la Opacidad y el Fraude de la entidad.
e. Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los Riesgos de Corrupción, Opacidad y Fraude medidos.
f. Establecer y monitorear el perfil de riesgo de la entidad e informarlo al órgano correspondiente, en los términos de la presente Circular.
g. Desarrollar los modelos de medición del riesgo de Corrupción, Opacidad y Fraude.
h. Desarrollar los programas de capacitación de la entidad relacionados con el SICOF.
i. Presentar un informe periódico, como mínimo semestral, a la Junta Directiva y al representante legal, sobre la evolución y aspectos relevantes del SICOF, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.
j. Establecer mecanismos para la recepción de denuncias (líneas telefónicas, buzones especiales en el sitio web, entre otros) que faciliten, a quienes detecten eventuales irregularidades, ponerlas en conocimiento de los órganos competentes de la entidad.
k. Informar al máximo órgano social u órgano equivalente sobre el no cumplimiento de la obligación de los administradores de suministrar la información requerida para la realización de sus funciones.
l. Estudiar los posibles casos de Corrupción, Opacidad y Fraude, dentro del ámbito de su competencia, para lo cual debe contar con la colaboración de expertos en aquellos temas en que se requiera y elaborar el informe correspondiente para someterlo a consideración del máximo órgano social.
m. Informar a la Superintendencia Nacional de Salud los posibles casos de Corrupción, Opacidad y Fraude que se lleguen a presentar a través de los canales dispuestos para tal fin.
n. Proponer a máximo órgano social programas y controles para prevenir, detectar y responder adecuadamente a los Riesgos de Corrupción, Opacidad y Fraude, y evaluar la efectividad de dichos programa y controles.
o. Poner en funcionamiento la estructura, procedimientos y metodologías inherentes al SICOF, en desarrollo de las directrices impartidas por el máximo órgano social, garantizando una adecuada segregación de funciones y asignación de responsabilidades.
p. Elaborar el plan anual de acción del SICOF y darle estricto cumplimiento.
q. Recomendar a la Junta directiva medidas preventivas y/o acciones ante organismos competentes (Judiciales y/o disciplinarlos) para fortalecer el SICOF.

En general, el Oficial de Cumplimiento o persona encargada por la entidad para la ejecución del SICOF, es el responsable de dirigir la implementación de los procedimientos de prevención y control, y verificar al interior de la entidad su operatividad y su adecuado funcionamiento, para lo cual debe demostrar la ejecución de los controles que le corresponden.

El Oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF, debe dejar constancia documental de sus actuaciones en

esta materia, mediante memorandos, cartas, actas de reuniones o los documentos que resulten pertinentes para el efecto.

Adicionalmente, debe mantener a disposición del auditor interno, el revisor fiscal y demás órganos de supervisión o control los soportes necesarios para acreditar la correcta implementación del SICOF, en sus diferentes elementos, procesos y procedimientos.

Responsabilidades del Oficial de Cumplimiento frente al Subsistema Seguridad Informática.

a. apoyo en seguridad digital, servidores, sistemas operativos, dispositivos de red.
b. Plantear y ejecutar proyectos de seguridad informática, identificación de hallazgos, emisión de políticas de seguridad, definir mecanismos de control, e implementar los correctivos a los hallazgos encontrados.
c. Dominio de sistemas operativos, control de usuarios y permisos.
d. Apoyar en la configuración de dispositivos de red, firewall, y equipos de seguridad informática.
e. Realizar capacitaciones al personal del ESE ISABU, socializar con los usuarios internos los riesgos y cuidados que se deben tener en el tema de seguridad informática.
f. Protección de datos personales, encaminado a dar cumplimiento de la ley 1581 de 2018 y decreto 090 de 2018.
g. Gestión de los cambios de sistema de protección de datos y conservación de su registro.
h. Generar y realizar el mantenimiento de política de tratamiento de información y de los avisos de privacidad a que hubiere lugar.
i. Realizar el diligenciamiento de actualizaciones del registro nacional de bases de datos RNBD ante la SIC en caso de requerirse nuevamente.
j. Realizar el registro de nuevas bases de datos ante el RNBD y asegurar su actualización.
k. Realizar los reportes periódicos o esporádicos según el marco legal, de información ante la SIC.
l. Actualización del sistema de protección de datos personales a los cambios de normativa en el país.
m. Realizar actividades de aseguramiento de la cultura organizacional en protección de datos y seguridad informática.
n. Apoyar en la gestión segura de bases de datos conforme al nivel de riesgo.
o. Apoyo en la gestión documental requerida por la ESE ISABU según.
p. Orientación en la gestión de autorizaciones a instrumentos de recolección de datos personales (esto es las herramientas físicas, digitales, de imagen o de voz con que el ISABU recolecta datos personales), mediante la indicación de las autorizaciones que conforme a la ley deben ser incorporadas por el sistema integrado de calidad del ESE ISABU.
q. Realizar la orientación de la aplicación de los procedimientos de seguridad de datos personales del sistema.
r. Realizar el proceso de monitoreo del sistema tecnológico 1581.
s. Brindar información y asesoramiento en protección de datos para el soporte en las siguientes actividades:
    - Resolver dudas verbales o escritas de contenido jurídico asociadas a protección de datos personales.
    - Asesorar en la gestión de incidentes de protección de datos personales incluido el reporte ante la SIC.
    - Asistencia como asesor a la sesión del Gobierno en protección de datos personales.
    - Proyectar como asesor respuesta a requerimientos administrativos de cualquier autoridad no jurisdiccional.
    - Atender como asesor las visitas de la SIC o de la procuraduría general de la nación por temas asociados a protección de datos personales.

SEGUNDA LÍNEA DE DEFENSA *Asiste y Guía la línea estratégica y la primera línea de Defensa en la gestión adecuada de los riesgos.*	**Responsables:** Área de Gestión de Riesgos (Planeación, Calidad, Jurídica), líderes responsables de los subsistemas de administración de riesgos, Comité de Riesgos, Seguridad, Salud en el Trabajo, Seguridad de la Información y Gestión de Talento Humano.

Responsabilidades Líderes de cada Subsistema frente al Riesgo:

a. Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de gestión del riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
b. Acompañar, orientar y entrenar sobre la metodología para la identificación, análisis, calificación y valoración del riesgo a los líderes de los procesos.
c. Monitorear los controles establecidos a los riesgos identificados.
d. Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles de corrupción para que se generen acciones.
e. Evaluar que los riesgos identificados sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.
f. Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
g. Hacer seguimiento a que las actividades de control establecidas para la mitigación del riesgo de los procesos se encuentren documentados y actualizados en los procedimientos.
h. Consolidar el Mapa de Riesgo Institucional y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional.
i. Presentar al Comité institucional de Control Interno el seguimiento a la eficacia de los controles a los riesgos identificados.
j. Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.
k. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo. Supervisar que la primera línea de defensa identifique, evalué y gestione los riesgos en los temas de su competencia.

Responsabilidades Área de Gestión de Riesgos frente al Riesgo:

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

Responsabilidades Comité de Riesgos frente al Riesgo:

a. Establecer estrategias para prevenir y mitigar los riesgos en salud.
b. Identificar, medir, caracterizar, supervisar y anticipar, mediante metodologías adecuadas, los diversos riesgos (de salud, económicos, operativos, de grupo, lavado de activos, reputacionales, entre otros) asumidos por la entidad, propios de su función en el SGSSS.
c. Hacer seguimiento y evaluar periódicamente el funcionamiento de los Comités internos de la institución relacionados con asuntos de salud, incluidos los de vigilancia epidemiológica, historias clínicas, infecciones, y farmacia.
d. Velar por el cumplimiento y mejoramiento progresivo de los procesos y estándares relacionados con la seguridad del paciente.
e. Supervisar los procesos de atención al paciente, velar por una atención humanizada, y medir y evaluar indicadores de atención (seguimiento y análisis de quejas y reclamos, orientación al usuario, tiempos de espera, etc.).
f. Evaluar y formular a la Junta Directiva o quien haga sus veces, las metodologías de segmentación, identificación, medición, control y monitoreo de los riesgos a los que se expone la entidad, para mitigar su impacto, presentadas y diseñadas por el área de gestión de riesgos. Asimismo, las actualizaciones a las que haya lugar.
g. Velar por el efectivo, eficiente y oportuno funcionamiento del ciclo general de gestión de riesgos, incluyendo todas las etapas que se mencionaron en el punto anterior, para cada uno de los riesgos identificados.
h. Evaluar y formular a la Junta Directiva o quien haga sus veces, los ajustes o modificaciones necesarios a las políticas de los diferentes Subsistemas de Administración de Riesgos, presentadas y diseñadas por el área de gestión de riesgos.
i. Evaluar y proponer a la Junta Directiva o quien haga sus veces, el manual de procesos y procedimientos y sus actualizaciones, a través de los cuales se llevarán a la práctica las políticas aprobadas para la implementación de los diferentes Subsistemas de Administración de Riesgos.
j. Identificar las consecuencias potenciales que pueda generar la materialización de los diferentes riesgos sobre las operaciones que realiza la entidad.
k. Evaluar los límites de exposición para cada uno de los riesgos identificados, y presentar a la Junta Directiva y al Representante Legal, las observaciones o recomendaciones que considere pertinentes, presentadas y diseñadas por el área de gestión de riesgos.
l. Objetar la realización de aquellas operaciones que no cumplan con las políticas o límites de riesgo establecidas por la entidad o grupo empresarial oficialmente reconocido al cual esta pertenezca. Cabe resaltar que de acuerdo con las políticas que establezca la entidad, cada instancia podrá tener diferentes atribuciones para aprobar operaciones que incumplan las políticas establecidas inicialmente por la entidad y que violen los límites de exposición para cada uno de los riesgos identificados.
m. Conocer y discutir los resultados de las pruebas de tensión (stress test) en el caso que apliquen y el plan de acción a ejecutar con base en ellos para informarlo a la Junta Directiva, Consejo de Administración u órgano que haga sus veces.
n. Informar a la Junta Directiva y al Representante Legal sobre los siguientes aspectos:
    - El comportamiento y los niveles de exposición de la entidad a cada uno de los riesgos (como mínimo los riegos prioritarios), así como las operaciones objetadas. Los informes sobre la exposición de riesgo deben incluir un análisis de sensibilidad por escenarios y pruebas bajo condiciones extremas basadas en supuestos razonables (stress testing).

- Las desviaciones con respecto a los límites de exposición de riesgo previamente establecidos, si se llegasen a presentar posibles incumplimientos frente a los límites), operaciones poco convencionales o por fuera de las condiciones de mercado y las operaciones con vinculados.
- Validar e informar a la Junta Directiva y al Representante Legal, el avance en los planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.

Responsabilidades de Gestión de Talento Humano frente al Riesgo:

a. monitorear temas claves del ciclo del servidor (capacitación, bienestar, incentivos, convivencia laboral, código integridad), generando alertas sobre incumplimientos, situaciones críticas que afectan el clima laboral y pasibles afectaciones al código de integridad.

TERCER LINEA DE DEFENSA *Asegura y evalúa independientemente la efectividad del sistema de gestión de riesgos.*	**Responsables** Oficina de Control Interno, Revisor Fiscal.

Responsabilidades Oficina de Control Interno frente al Riesgo:

a. Asesorar de forma coordinada con las Oficinas Asesoras, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de Controles.
b. Analizar el diseño e idoneidad de los controles establecidos en los procesos.
c. Realizar revisión y evaluación al cumplimiento de las políticas y procedimientos establecidos en el Sistema Integrado de Gestión de Riesgos y de los Subsistemas por los cuales están conformados e implementados.
d. Realizar seguimiento a los riesgos identificados en los subsistemas de los riesgos de la entidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control interno.
e. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.
f. Evaluar semestralmente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARLAFT y SICOF con el fin de determinar las deficiencias y sus posibles soluciones. Así mismo, debe informar los resultados de la evaluación al Oficial de Cumplimiento y a la Junta Directiva.
g. Realizar una revisión periódica de los procesos relacionados con las parametrizaciones de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico.

Responsabilidades Revisor Fiscal frente al Riesgo de SARLAFT:

De conformidad con lo previsto en los numerales 1, 2 y 3 del artículo 207 del Código de Comercio, el revisor fiscal deberá cerciorarse que las operaciones, negocios y contratos que celebre o cumpla la empresa, se ajustan a las instrucciones y políticas aprobadas por el máximo órgano social, el empresario en el caso de las empresas unipersonales o el accionista único en la sociedad por acciones simplificada unipersonal.

Asimismo, deberá dar cuenta por escrito cuando menos, de forma anual a la Junta Directiva o quien haga sus veces, al representante legal, al empresario en el caso de las empresas unipersonales o al accionista único en la sociedad por acciones simplificada unipersonal, del cumplimiento o incumplimiento a las disposiciones contenidas en el SARLAFT.
De igual forma, deberá poner en conocimiento del Oficial de Cumplimiento, inconsistencias y falencias que detecte respecto a la implementación del SARLAFT o de los controles establecidos.

Finalmente, deberá rendir los informes que, sobre el cumplimiento a las disposiciones contenidas en la Circular 009/2016, le solicite la Superintendencia Nacional de Salud.

Responsabilidades Revisor Fiscal frente al Riesgo de SICOF:

Sin perjuicio de las funciones asignadas en otras disposiciones al Revisor Fiscal, éste debe elaborar un reporte al cierre de cada ejercicio contable, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF.

A su vez, debe poner en conocimiento del Representante Legal los incumplimientos del SICOF, sin perjuicio de la obligación de informar sobre ellos a la Junta Directiva u órgano que haga sus veces.

Responsables
Oficina Asesora de Planeación- Comunicaciones

Responsabilidades frente al Riesgo:

a. Apoyar en la definición de la estrategia de promoción del proceso participativo (actores internos y externos) y difusión de la Política de Gestión del Riesgo, mapas de Riesgo y Plan Anticorrupción y de Atención al Ciudadano –PAAC.

Responsables

Gestión Control Disciplinario Interno
Responsabilidades frente al Riesgo: **a.** Reportar anualmente, al área de Gestión del Riesgo y a la Oficina Asesora de Control Interno información sobre sanciones por conductas disciplinarias asociadas a riesgos de SICOF.
Responsables Oficina de Atención al Usuario - SIAU
Responsabilidades frente al Riesgo: **a.** Reportar semestralmente al Área de Gestión del Riesgo y a la Oficina Asesora de Control Interno información sobre PQRSD relacionadas con Riesgos de Corrupción. **b.** Reportar semestralmente al encargado de seguridad de la información, seguridad digital y oficial de protección de datos personales según ley 1581 del 2012 (**Gestión de las Tics)** sobre las PQRSD relacionadas con incidentes o vulneraciones a sistemas de información o archivos físicos donde se gestionen de datos personales.

Responsables
Servidores Públicos y Colaboradores
Responsabilidades frente al Riesgo: **a.** Conocer y mantener niveles de responsabilidad sobre la administración de los riesgos de los procesos que apoyan.

5.3 FACTORES Y CLASIFICACIÓN DEL RIESGO

Los factores de riesgos son las fuentes generadoras de riesgos que puede tener una entidad.
Lo clasificación de riesgos permite agrupar los riesgos identificados y clasificarlos cada uno de los riesgos en categorías.

La E.S.E ISABU en las políticas de cada Subsistema de Riesgos definirá los factores de riesgos que puedan afectar la entidad y clasificarlos por categorías, teniendo en cuenta la complejidad propia de la entidad, por la misión, por las funciones que desarrolla y con el sector en el que se desenvuelve, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de cada subsistema de riesgos.

5.4 VALORACIÓN DEL RIESGO

Establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente), elementos que se desarrollan:

5.4.1. Análisis de Riesgos: se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

- **Determinar la Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo.

Cada líder del subsistema con su equipo de apoyo realizará el análisis para determinar la probabilidad de ocurrencia que está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

En cada política de los subsistemas se definirá la probabilidad en una escala de frecuencia de realización de la actividad en un periodo de 1 año como se relaciona en la tabla 4.

Tabla 4 Criterios para definir el nivel de probabilidad

Escala	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	20%

Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 100 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 101 veces al año y máximo 1000 veces por año.	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 1000 veces por año.	100%

- **Determinar el impacto:** las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

En la política de cada subsistema se definirá la tabla de criterios específicos de impacto de acuerdo a los definidos en la normatividad y lineamientos vigentes de cada de ellos; en esta política se define la escala de valoración del impacto general que se aplicará en todas las políticas de cada uno de los subsistemas de riesgos de la ESE ISABU. En la tabla 5 se establecen los criterios de valoración cualitativo y cuantitativo para la medición del impacto.

Tabla 5 Criterios para definir el nivel de impacto.

Escala Cualitativa	Escala Cuantitativa	Criterio de impacto a Evaluar
Leve	20%	Definir los criterios de impacto principales de acuerdo a cada Subsistema
Menor	40%	
Moderado	60%	
Mayor	80%	
Catastrófico	100%	

Cuando se presenten varios criterios de impactos y que apliquen para el mismo riesgo, de acuerdo a los definidos para el subsistema, se debe tomar el nivel de riesgo más alto para establecer la zona de riesgo inicial (Riesgo Inherente).

- **Evaluación del Riesgo:** a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (Riesgo Inherente).
- Riesgo Inherente: Se realiza análisis preliminar el cual determina los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor, la cual se aplicará para todos los subsistemas la Matriz de calor.

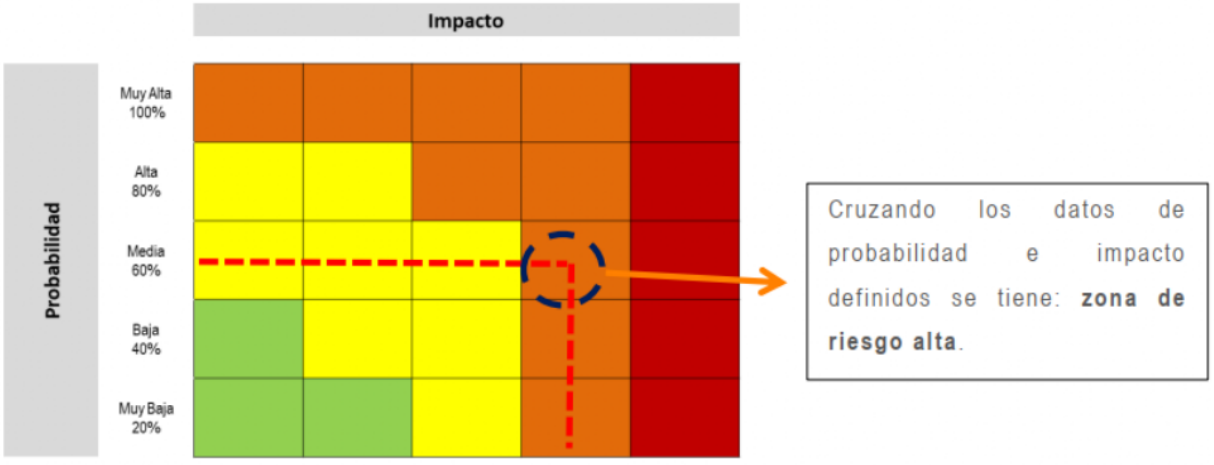
Figura 1 Matriz de calor (Niveles de severidad del riesgo).

		Impacto					
Probabilidad	Muy Alta 100%	Alto	Alto	Alto	Alto	Extremo	Extremo
	Alta 80%	Moderado	Moderado	Alto	Alto	Extremo	Alto
	Media 60%	Moderado	Moderado	Alto	Alto	Extremo	Moderado
	Baja 40%	Bajo	Moderado	Moderado	Alto	Extremo	Bajo
	Muy Baja 20%	Bajo	Bajo	Moderado	Alto	Extremo	
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%	

Fuente: *Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020. (Tomado de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas, Versión 5).*

Al Cruzar las dos variables de probabilidad e impacto definidos se tiene la zona del riesgo

Figura 2 Zona de Riesgo.



5.4.2. Valoración de controles: en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

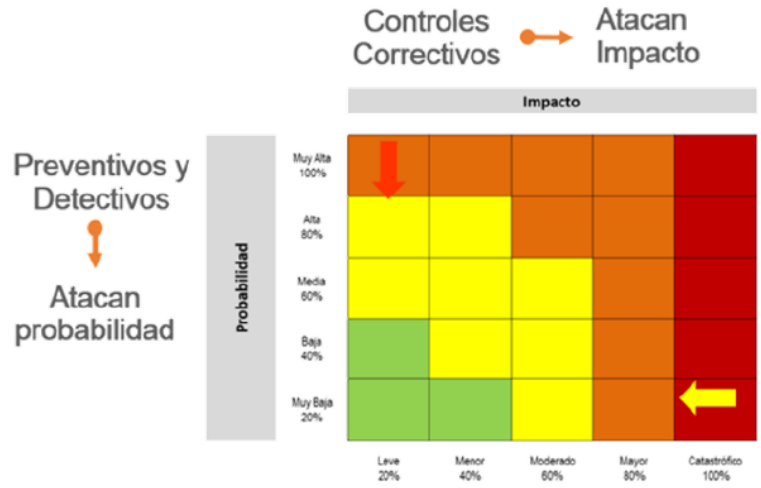
5.4.2.1. Estructura para la descripción del control: para una adecuada redacción del control se establece la estructura que facilitará entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan
- reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

A partir de los controles establecidos para cada riesgo se dará el movimiento, en la matriz de calor que corresponde a la figura 3, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

- **Evaluación de Riesgos:** Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).

Figura 3 Movimiento en la matriz de calor acorde con el tipo de control.



Fuente: *Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.*

5.5. TRATAMIENTO DEL RIESGO

La E.S.E. ISABU determinará el tratamiento para cada uno de los riesgos frente al nivel de severidad del riesgo donde quedó clasificado, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

- **Reducir:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.
- **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional, se establece un Plan de Acción.
- **Transferir:** Después de realizar el análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
- **Aceptar:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conocimiento los efectos de su posible materialización.
- **Evitar:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

5.6. DISEÑO, ASESORÍA, MONITOREO, SEGUIMIENTO Y CONTROL

La ESE ISABU alineada con MIPG de acuerdo a la Dimensión 7 de control interno que integra a MECI, junto con las medidas elaboradas por las circulares externas 20211700000005-5 de 2021, Circular externa 20211700000004-5 de 2021, desarrolla a través de las líneas de defensa un esquema de asignación de responsabilidades y roles para el Sistemas Integrado de Gestión del Riesgo:

Tabla 6 Diseño, Asesoría, Monitoreo, seguimiento y Control del Sistema Integrado de Gestión de Riesgos

DISEÑO, ASESORÍA, MONITOREO, SEGUIMIENTO Y EVALUACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN DE RIESGOS

RIESGO: SALUD - OPERACIONAL – ACTUARIAL - CRÉDITO – LIQUIDEZ - MERCADO DE CAPITALES -FALLAS DE MERCADO – REPUTACIONALES – SEGURIDAD DE LA INFORMACIÓN – SEGURIDAD Y SALUD EN EL TRABAJO - SARLAFT	
RESPONSABLE DEL DISEÑO DE LA METODOLOGÍA DE SEGMENTACIÓN, IDENTIFICACIÓN, CONTROL Y ASESORÍA	
Segunda línea de defensa: • Área de Gestión de Riesgos. • Comité de Gestión de Riesgos.	Anual y cuando se requiera actualizaciones.
Tercera línea de defensa: Oficina de Control Interno (En la construcción de controles).	
RESPONSABLE Y PERIODICIDAD DEL SEGUIMIENTO	
Primera línea de defensa: • Líderes de proceso y equipo de trabajo. • Oficial de cumplimiento de SARLAFT • Oficial de cumplimiento de Seguridad de la Información	Permanente y de acuerdo a la periodicidad de los controles.
Línea Estratégica de defensa: • Junta Directiva • Representante Legal • Comité de Coordinación de Control Interno **Nota:** Seguimiento de forma integral.	**Semestral** **Primer seguimiento:** corte 30 de junio **Segundo seguimiento:** corte 31 de diciembre
Segunda línea de defensa: Comité de Gestión de Riesgos.	**Trimestral** **I Trimestre:** corte 31 de marzo **II Trimestre:** corte 30 de junio **III Trimestre:** corte 30 de septiembre **IV Trimestre:** corte 31 de diciembre
RESPONSABLE Y PERIODICIDAD DE SEGUIMIENTO Y MONITOREO	
Segunda línea de defensa: • Área de Gestión de Riesgos. • Líderes responsables de los subsistemas de administración de riesgo. • Seguridad y Salud en el Trabajo. • Seguridad de la Información.	**Riesgos Extremos y Altos:** Mensual **Riesgos Moderado y Bajos:** Trimestral **Riesgos no priorizados:** Semestral
RESPONSABLE SEGUIMIENTO Y EVALUACIÓN	
Tercera línea de defensa: • Jefe Oficina Asesora de Control Interno • Revisor Fiscal (Solo hace seguimiento y evaluación a SARLAFT)	**Trimestral** **I Trimestre:** corte 31 de marzo **II Trimestre:** corte 30 de junio **III Trimestre:** corte 30 de septiembre **IV Trimestre:** corte 31 de diciembre

MONITOREO, SEGUIMIENTO Y EVALUACIÓN DEL SISTEMA INTEGRADO DE GESTIOS DEL RIESGO RIESGO: SICOF - PAAC	
RESPONSABLE DEL DISEÑO DE LA METODOLOGÍA DE SEGMENTACIÓN, IDENTIFICACIÓN, CONTROL Y ASESORAR	
Segunda línea de defensa: • Área de Gestión de Riesgos. • Comité de Gestión de Riesgos.	Anual y cuando se requiera actualizaciones.
Tercera línea de defensa: Oficina de Control Interno (En la construcción de controles).	
RESPONSABLE Y PERIODICIDAD DEL SEGUIMIENTO	
Primera línea de defensa: • Líderes de proceso y equipo de trabajo. • Oficiales de cumplimiento de SICOF	Permanente y de acuerdo a la periodicidad de los controles.
Línea Estratégica de defensa: • Junta Directiva • Representante Legal • Comité de Coordinación de Control Interno **Nota:** Seguimiento de forma integral.	**Semestral** **Primer seguimiento:** corte 30 de junio **Segundo seguimiento:** corte 31 de diciembre
Segunda línea de defensa: Comité de Gestión de Riesgos.	**Trimestral** **I Cuatrimestre:** corte 30 de abril **II Cuatrimestre:** corte 31 de agosto **III Cuatrimestre:** corte 31 de diciembre

RESPONSABLE Y PERIODICIDAD DEL SEGUIMIENTO Y MONITOREO	
Segunda línea de defensa: • Área de Gestión de Riesgos. • Líderes responsables de los subsistemas de administración de riesgo SICOF – PAAC – Componente Mapa Riesgos de Corrupción.	**Cuatrimestral** **I Cuatrimestre:** corte 30 de abril **II Cuatrimestre:** corte 31 de agosto **III Cuatrimestre:** corte 31 de diciembre
RESPONSABLE Y PERIODICIDAD DEL SEGUIMIENTO	
Línea Estratégica de defensa: • Junta Directiva • Representante Legal • Comité de Coordinación de Control Interno	**Semestral** **Primer seguimiento:** corte 30 de junio **Segundo seguimiento:** corte 31 de diciembre
RESPONSABLE Y PERIODICIDAD DEL SEGUIMIENTO Y EVALUACIÓN	
Tercera línea de defensa: • Jefe Oficina Asesora de Control Interno	**Cuatrimestral** **I Cuatrimestre:** corte 30 de abril **II Cuatrimestre:** corte 31 de agosto **III Cuatrimestre:** corte 31 de diciembre
• Revisor Fiscal (Solo hace seguimiento y evaluación al SICOF).	**Anual** Reporte al cierre de cada ejercicio contable.

5.7. PUBLICACIÓN

En cumplimiento del artículo 73 de la Ley 1474 de 2011, el Plan Anticorrupción y Atención al Ciudadano – PAAC, se debe publicar en su página web a más tardar el 31 de enero de cada año, por lo anterior y teniendo en cuenta que el primer componente del PAAC es el Mapa de Riesgos de Corrupción se debe publicar en dicha fecha, la ESE ISABU publicará el PAAC y sus Mapas o Matrices de riesgos en su página web a más tardar el 31 de enero de cada año; además, realizará publicaciones de las actualizaciones o modificatorias que se generen de los mismos.

La oficina de control interno publicará en la página web los informes de seguimiento y evaluación que realice al Sistema Integrado de Gestión de Riesgos y el PAAC de acuerdo a la periodicidad establecida en el ítem 5.7 de esta política, la cual está alineada con lo estipulado por la normatividad vigente.

5.8. INFORMES Y RESPORTES DE INFORMACIÓN

Tabla 7 Informes y Reportes de información

RESPONSABLE DE INFORMES Y/O REPORTES	TIPO DE INFORME O/Y REPORTE	DESCRIPCIÓN	PERIODICIDAD	REPORTAR A:
Junta Directiva	Reporte de Notificación	Reporte de Notificación del Oficial de cumplimiento y su respectivo suplente de SARLAFT.	Inicial y cuando se genere cambios.	Superintendencia Nacional de Salud.
	Acta de pronunciamiento	Pronunciamiento a través de actas de los informes de seguimiento presentados por el Comité de Riesgos, Oficial de Cumplimiento de SARLAFT, SICOF, la Revisoría Fiscal y Control Interno.	Semestral	Representante Legal
Representante Legal	Informe	Pronunciamiento a través de Informe de los informes periódicos presentados por el Comité de Riesgos, Revisoría Fiscal, Control Interno, Oficial de Cumplimiento de SARLAFT y SICOF.	Semestral	Junta Directiva
	Oficio de reporte	Informar a través de Oficio de la situación excepcional que se presente o prevea que pueda presentarse como mínimo en el ámbito de la administración de los riesgos prioritarios, de las causas que la originan y de las medidas que se propone poner en marcha por parte de la entidad para corregir o enfrentar dicha situación, si procede.	Cuando se presente	Superintendencia Nacional de Salud.
Comité de Riesgos	Informe de Seguimiento	• El comportamiento y los niveles de exposición de la entidad a cada uno de los riesgos (como mínimo	Semestral	Junta Directiva Representante Legal

		los riegos prioritarios), así como las operaciones objetadas. Los informes sobre la exposición de riesgo deben incluir un análisis de sensibilidad por escenarios y pruebas bajo condiciones extremas basadas en supuestos razonables (stress testing). • Las desviaciones con respecto a los límites de exposición de riesgo previamente establecidos, si se llegasen a presentar posibles incumplimientos frente a los límites), operaciones poco convencionales o por fuera de las condiciones de mercado y las operaciones con vinculados. • Validar e informar el avance en los planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.		
Área de Gestión de Riesgos	Informe de avance	Informes Informar en los casos que aplique, el avance en los planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.	Trimestral	Comité de Riesgos
Oficial de Cumplimiento SARLAFT	Reporte de información	Realizar todos los reportes, incluidas las actas de aprobación de la política, así como el manual de procedimientos.	Cuando se actualice o sea requerido.	Superintendencia Nacional de Salud.
	Reporte de operaciones	Reportar las posibles operaciones inusuales, intentadas o sospechosas.	Cuando se presente	Unidad de Información y Análisis Financiero – UIAF
	Reporte de actualización de datos de la entidad y oficial de cumplimiento	Mantener actualizados los datos de la entidad y el oficial de cumplimiento con la UIAF, utilizando los canales de comunicación correspondientes.	Cuando se presente	Superintendencia Nacional de Salud.
	Reporte de cambios del SIREL	Informar a la UIAF cualquier cambio de usuario del Sistema de Reporte en Línea-SIREL	Cuando se presente	Unidad de Información y Análisis Financiero – UIAF
	Informe de Gestión	Presentar cuando menos, de forma semestral a los administradores y anualmente a la Junta Directiva o quien haga sus veces, un informe por escrito donde exponga el resultado de su gestión.	Semestral Anual	Representante Legal Comité de Riesgos Junta Directiva
Oficial de Cumplimiento SICOF	Informe de seguimiento	Informe periódico, como mínimo semestral, a la Junta Directiva y al representante legal, sobre la evolución y aspectos relevantes del SICOF, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.	Semestral	Junta Directiva Representante Legal
	Informe de cumplimiento	Informar al máximo órgano social u órgano equivalente sobre el no cumplimiento de la obligación de los administradores de suministrar la información requerida para la realización de sus funciones.	Semestral	Junta Directiva
	Reporte de los posibles casos de Corrupción, Opacidad y Fraude.	Informar los posibles casos de Corrupción, Opacidad y Fraude que se lleguen a presentar a través de los canales dispuestos para tal fin.	Cuando se presente	Superintendencia Nacional de Salud
Oficial de Cumplimiento Seguridad de la información	Informe de seguimiento	Informe de seguimiento del avance del Sistema de Seguridad de la Información y de los planes de acción y de mejoramiento (en caso que aplique).	Trimestral	Área de Gestión de Riesgos Comité de Gestión de Riesgos

Seguridad y Salud en el Trabajo	Informe de seguimiento	Informe de seguimiento del avance del Sistema de Seguridad y Salud en el Trabajo y de los planes de acción y de mejoramiento (en caso que aplique).	Trimestral	Área de Gestión de Riesgos Comité de Gestión de Riesgos
Líderes de los Subsistemas del Sistema Integrado de Gestión Riesgos	Informe de seguimiento y monitoreo	Informe de seguimiento al cumplimiento de los controles de los riesgos priorizados de cada subsistema de administración de riesgos y avances de los planes de acción y de mejoramiento (en caso que aplique).	Trimestral	Área de Gestión de Riesgos Comité de Gestión de Riesgos.
Líder del Subsistema Liquidez	Reporte Archivo FT018	**Datos para el cálculo de la posición de Liquidez.** **TIPO DE ENTIDAD A LA QUE APLICA**: Instituciones Prestadoras de Servicios de Salud de los grupos B, C1, C2 y D1 públicos, privados y mixtos. **FECHA DE CORTE:** Último día de cada mes. **FECHA DEL REPORTE:** 20 días calendario después de la fecha de corte. Para el cierre de año, el reporte se hará hasta febrero 20 del siguiente año.	Mensual	Superintendencia Nacional de Salud.
Líder de Código de Conducta y Buen Gobierno	Reporte Archivo GT001	**Reporte de Implementación del Código de Conducta y de Buen Gobierno** **TIPO DE ENTIDAD A LA QUE APLICA:** Instituciones Prestadoras de Servicios de Salud - Grupos C1, C2 y D1 de la presente Circular y normas que la modifiquen o sustituyan). **FECHA DE CORTE:** 30 de septiembre **FECHA DEL REPORTE:** 20 días calendario después de la fecha de corte.	Anual	Superintendencia Nacional de Salud.
Jefe de Control Interno	Informe de Evaluación SARLAFT Y SICOF	Informe de Evaluación de la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARLAFT y SICOF con el fin de determinar las deficiencias y sus posibles soluciones.	Semestral	Oficial de Cumplimiento SARLAFT Y SICOF Junta Directiva.
	Informe de Evaluación PAAC	Informe de evaluación del cumplimiento del Plan Anticorrupción y Atención al Ciudadano - PAAC y Mapa de Corrupción.	Cuatrimestral	Representante Legal Área de Gestión de Riesgos
	Informe de Evaluación Sistema Integrado de Gestión de Riesgos	Informe de revisión y evaluación al cumplimiento de las políticas y procedimientos establecidos en el Sistema Integrado de Gestión de Riesgos y de los Subsistemas por los cuales están conformados e implementados.	Anual	Representante Legal Junta Directiva
	Informe de evaluación de los Riesgos del Sistema Integrado de Gestión de Riesgos	Informe de seguimiento y evaluación de los riesgos identificados en los subsistemas de riesgos de: Salud - Operacional – Actuarial - Crédito – Liquidez - Mercado De Capitales -Fallas De Mercado – Reputacionales – Seguridad De La Información – Seguridad y Salud en el Trabajo - SARLAFT.	Trimestral Semestral	Representante Legal. Oficiales de cumplimiento. Líderes de Gestión de Riesgos. Área de Gestión del Riesgo. Junta Directiva
Revisor Fiscal	Informe de evaluación de SARLAFT	Informe de evaluación del cumplimiento o incumplimiento a las disposiciones contenidas en el SARLAFT.	Anual	Oficial de Cumplimiento. Representante Legal. Junta Directiva.
	Informe de evaluación de SARLAFT	Informe de las inconsistencias y falencias con respecto a la implementación del SARLAFT o de los controles establecidos.	Anual	
	Informe de rendición de cumplimiento SARLAFT	Informes de cumplimiento a las disposiciones contenidas en la Circular 009/2016.	Mensual	Superintendencia Nacional de Salud.
	Informe de	Reporte al cierre de cada ejercicio contable, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF. A su vez, debe poner en conocimiento del Representante Legal los incumplimientos del SICOF.	Anual	Representante Legal Junta Directiva
Gestión Control Disciplinario Interno	Reporte	Información sobre sanciones por conductas disciplinarias asociadas a riesgos de SICOF.	Anual	Área de Gestión del Riesgo. Oficina Asesora de Control Interno.
		Reportar al Área de Gestión del Riesgo y a la Oficina	Semestral	Área de Gestión de Riesgos

Oficina de Atención al Usuario	Reporte de PQRSD	Asesora de Control Interno información sobre PQRSD relacionadas con Riesgos de Corrupción.		
		Reportar al encargado de seguridad de la información, seguridad digital y oficial de protección de datos personales según ley 1581 del 2012 (**Gestión de las Tics)** sobre las PQRSD relacionadas con incidentes o vulneraciones a sistemas de información o archivos físicos donde se gestionen de datos personales.	Semestral	Oficial de Cumplimiento de Seguridad de la Información

6. INDICADORES DE LA POLÍTICA DE ADMINSITRACIÓN DE RIESGOS:

- Porcentaje de cumplimiento del Plan Anticorrupción y Atención al Ciudadano.
- Proporción de cumplimiento de la Gestión del Riesgo en Salud.
- Proporción de cumplimiento de la Gestión del Riesgo Operacional.
- Proporción de cumplimiento de la Gestión del Riesgo Actuarial.
- Proporción de cumplimiento de la Gestión del Riesgo de Crédito.
- Proporción de cumplimiento de la Gestión del Riesgo de Liquidez.
- Proporción de cumplimiento de la Gestión del Riesgo de Mercado.
- Proporción de cumplimiento de la Gestión del Riesgo de Fallas de Mercado.
- Proporción de cumplimiento de la Gestión del Riesgo Reputacional.
- Proporción de cumplimiento de la gestión del Riesgo de SARLAFT.
- Proporción de cumplimiento de la gestión del Riesgo SICOF.
- Proporción de cumplimiento de la gestión del Riesgo Seguridad y Salud en el Trabajo.
- Proporción de cumplimiento de la gestión del Riesgo Seguridad de la Información.

7. BIBLIOGRAFÍA

1. Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 5. (Dirección de Gestión y Desempeño Institucional).
2. Instructivo Metodológico para la Elaboración de Políticas Institucionales, Proceso de Gestión, Versión 0.0.
3. Protocolo Líneas de Defensa, Modelo Integrado de Planeación y Gestión MIPG Dimensión 7: Control Interno, Código PT-1300, Versión 1.0-
4. Manual de Acreditación en Salud Ambulatorio y Hospitalario de Colombia, Versión 3.1, Minsalud.
5. Circular externa 20211700000005-5 de 2021.
6. Circular externa 20211700000004-5 de 2021.
7. Ley 1581 de 2012.

8. CONTROL DE CAMBIOS

CONTROL DE MODIFICACIONES			
Versión	**Fecha**	**Descripción de la Modificación**	**Realizada por**
1.0	07-06-2018	Creación de la Política de administración de riesgos	Profesional de Calidad
2.0	30-03-2021	Actualización de la política, objetivo, estrategia de implementación de la política de acuerdo a los lineamientos que brinda la guía de la administración del riesgo y el diseño de controles en las entidades públicas, de la Función Pública, versión 5, diciembre 2020.	Profesional Apoyo Planeación Profesional Especializado de Planeación

3.0	21-11-2022	1. Modificación de la plantilla de la política de acuerdo a la elaboración de documentos por la Oficina Asesora de Calidad. 2. Actualización del contexto de la política, 1. objetivo general, 1.1. objetivos específicos ,2. Alcance, 3. responsable, 4 definiciones, 5. Lineamientos de implementación del sistema de gestión de riesgos, tabla 3. Implementación del SIGR de acuerdo al esquema de líneas de defensa, 5.3 factores y clasificación de riesgos., 5.4 Valoración del riesgo, 5.5 Tratamiento del riesgo, 5.6. Diseño, asesoría, monitoreo, seguimiento y control, 6. Indicadores de la política de administración de riesgos 3. Inclusión de: Tabla 8 Lineamientos generales de Implementación del Sistema Integrado de Gestión de Riesgos, Tabla 9 Responsables de los Subsistemas Integrados de Gestión de Riesgos, 5.2 Responsabilidades y compromisos frente al sistema integrado gestión del riesgo y control, 5.7. Publicación, 5.8. Informe y reportes de información, 8. Control de cambios. 4. Eliminación de los principio y valores, factores de riesgo	Profesional Apoyo Planeación Profesional Especializado de Planeación
4.0	27-08-2024	1.Modificación en los responsables de los subsistemas integrados de Gestión de Riesgos de Seguridad de la Información. 2.Inclusión en la segunda línea de defensa al proceso de Gestión de Talento Humano como responsable de monitorear temas claves del ciclo del servidor (capacitación, bienestar, incentivos, convivencia laboral, código integridad), generando alertas sobre incumplimientos, situaciones críticas que afectan el clima laboral y pasibles afectaciones al código de integridad.	Profesional Apoyo Planeación
5.0	09-10-2024	Actualización de imagen institucional	Oficina de calidad