1. OBJETIVO

La Política de Gestión de Riesgos de La Cardio, define los criterios generales y elementos principales para identificar, analizar, valorar, tratar, monitorear y reportar los riesgos a los que está expuesta la Organización, así como, la identificación, evaluación e implementación de controles garantizando que sean efectivos, buscando la protección del valor, la continuidad de las operaciones y la generación de confianza en los grupos de interés.

2. ALCANCE

La política aplica a todos los riesgos asociados a la operación de La Cardio y se centra en los riesgos institucionales de tipo Estratégico, Financiero, Clínico, SARLAFT (Sistema de administración del riesgo de lavado de activos y financiación del terrorismo – SARLAFT), SICOF (Subsistema de Administración del Riesgo de Corrupción, Opacidad y Fraude), Operacional (SARO), Actuarial y de proyectos, enfocando la gestión en los procesos misionales y de apoyo para cada escenario de riesgo y aquellos de alto impacto para el cumplimiento de los objetivos estratégicos y su misionalidad.

3. DEFINICIONES

- Apetito de Riesgo: El apetito de riesgo se refiere a la cantidad de exposición a impactos adversos potenciales que La Cardio cómo Organización está dispuesta a aceptar para alcanzar sus objetivos.
- Control: Medida que mantiene y/o modifica un riesgo.
- Gestión del Riesgo: Actividades coordinadas para dirigir y controlar la Organización con relación al riesgo.
- Modelo de las Tres Líneas de Defensa: El modelo define tres líneas de actividades que participan en una efectiva gestión y supervisión de riesgos. La alineación de las tres líneas de defensa permite mitigar de una forma integral los riesgos. i) la primera línea está compuesta por el control de la gerencia, donde cada área operativa de la Organización pone en práctica la gestión de sus propios riesgos y controles, para asegurar el cumplimiento de los objetivos de la Organización, a través de, un adecuado sistema de control interno; ii) la segunda línea contempla las funciones de supervisión de riesgos, controles y cumplimiento de políticas y estándares establecidos por la Administración, abordando riesgos transversales, complejos y específicos; iii) y en la tercera línea está el aseguramiento independiente, la auditoría interna que aporta supervisión objetiva sobre las dos primeras líneas de defensa y evalúa el sistema de control interno de la Organización en su conjunto para identificar debilidades y recomendar mejoras.
- Planes de Tratamiento del Riesgo: El propósito del tratamiento del riesgo es seleccionar e implementar las opciones más apropiadas para abordar el riesgo; el plan de tratamiento identifica claramente el orden y la forma en la cual el tratamiento del riesgo se debería implementar.
- Perfil de Riesgos: Descripción de cualquier conjunto de riesgos.
- Riesgo: Efecto de la incertidumbre sobre los objetivos.
- Riesgo Inherente: Corresponde al riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior.
- Riesgo Residual: Corresponde al remanente después del tratamiento del riesgo.

Copia no controlada

- SGIR: Sistema de Gestión Integral de Riesgos.

- Tolerancia al Riesgo: Es el nivel aceptable de variación en relación con la consecución de un objetivo. La tolerancia al riesgo se alinea con el apetito al riesgo respecto a la cantidad máxima de un riesgo que La Cardio esté dispuesta a aceptar.

- Triangulo del Fraude: El triángulo del fraude es un modelo que incluye los factores que llevan a una persona a cometer un fraude ocupacional. El triángulo del fraude tiene tres instancias; presión, oportunidad y racionalización.

4. DECLARACIÓN DE LA POLÍTICA

El Sistema de Gestión Integral de Riesgos (SIGR), es una herramienta creada para anticipar eventos que impidan el cumplimiento de los objetivos estratégicos. La gestión adecuada de los riesgos a los que está expuesta La Cardio conlleva a la Administración a una correcta toma de decisiones, atención segura y con calidad a nuestros pacientes, la protección de los cuidadores, visitantes, proveedores, colaboradores y a la comunidad en general.

La gestión de riesgos es la combinación de administrar el talento, los procesos, los proyectos, las instalaciones y la implementación de mecanismos de prevención y mitigación de los riesgos identificados, así como, la construcción de una cultura proactiva de conciencia y autocontrol frente al manejo del riesgo. Igualmente, el propósito de la gestión integral de riesgos consiste en reducir la incertidumbre en la toma de decisiones para crear y proteger el valor de la Organización, mejorando su rentabilidad, preservando la imagen y reputación de la Organización frente a sus grupos de interés.

Copia no controlada

Los fundamentos de la gestión de riesgos en La Cardio están enmarcados en el contexto organizacional y se basan en los siguientes principios:

- La gestión de riesgos en La Cardio está orientada en; i. La creación y protección de valor de la Organización, preservando la imagen y reputación frente a sus grupos de interés, ii. Soportar las decisiones estratégicas, tácticas y operativas, para preservar la integridad y rentabilidad de los recursos de la Organización, iii. Fortalecer la comunicación y las herramientas, que permitan actuar de manera oportuna y eficiente ante la incertidumbre asociada al logro de los objetivos y orientada en la creación y fortalecimiento de una cultura de riesgo, mediante la capacitación y concientización de todos los colaboradores, que permiten realizar la identificación de riesgos y controles que se pueden presentar en el desarrollo de las actividades propias de sus procesos. Para ello, es importante contar con un flujo constante de información entre todas las áreas, fortaleciendo la cultura de reporte y apoyando la mitigación de los riesgos potenciales.
- Los órganos de administración, de control y demás colaboradores de la Organización, cuentan con funciones definidas en el sistema de administración de riesgos, evidenciando su rol y las responsabilidades específicas en cada una de las etapas del sistema, asegurando su cumplimiento y alineación con los objetivos de este.
- El área de riesgos como área independiente y manteniendo su imparcialidad, tiene acceso a toda la información que considere necesaria para la ejecución de cada una de las etapas del sistema y en especial para el registro de eventos de riesgo. Para el desarrollo de sus funciones, el área de riesgos cuenta con personal con experiencia y capacitado en la administración de riesgo y con recursos suficientes. Esta área está a cargo de la Gerencia de Control Interno y Riesgos y la Coordinación de Riesgos con nivel organizacional alto y capacidad de toma de decisiones.

- El área de riesgos presenta la evolución y los cambios que se presenten en los controles implementados. Los resultados del avance de cada una de las etapas del sistema de riesgos

están disponibles para consulta por parte de los miembros del Comité de Auditoría y Riesgos para su respectiva retroalimentación y mejoramiento continuo.

5. LINEAMIENTOS GENERALES

5.1. Requisitos para la Implementación de la Política:

- Compromiso de la Alta Dirección para promover la participación de todos los colaboradores de La Cardio en la implementación del Sistema de Gestión Integral de Riesgos. (SIGR).

- El Área de Riesgos es responsable de liderar el Sistema de Gestión Integral de Riesgos (SIGR) y mantener siempre su independencia con las diferentes áreas y procesos de La Cardio.

- Compromiso de todos los miembros de la Organización para la implementación del Sistema de Gestión Integral de Riesgos (SIGR), que promueva la construcción de una cultura de gestión de riesgos sólida y sostenible en el tiempo.

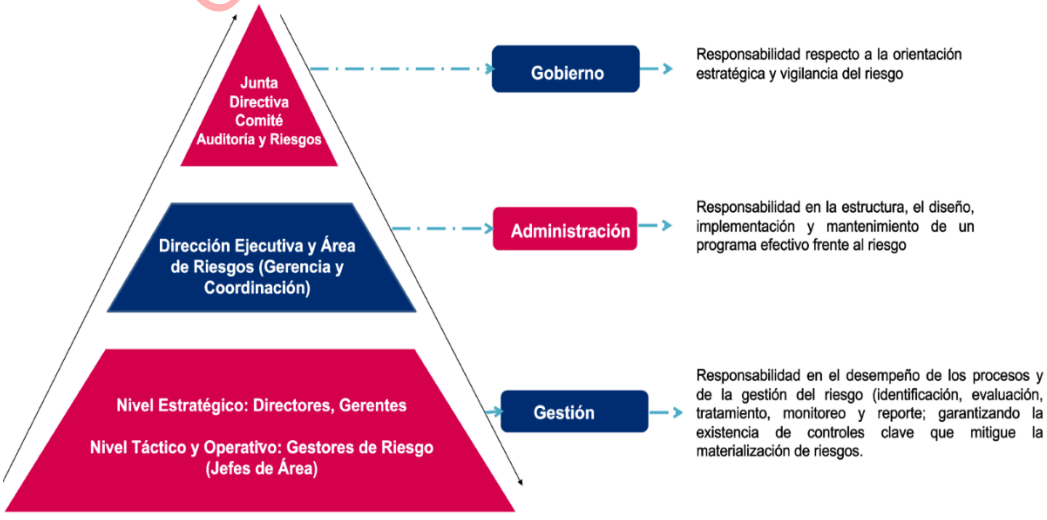
- Cumplimiento del proceso de gestión del riesgo por parte de los diferentes actores, dando continuidad a cada una de las etapas del sistema.

5.2. Estructura de Gobierno del Sistema de Gestión Integral de Riesgos:

En La Cardio se definen los siguientes niveles de gobernanza para lograr la implementación del SIGR, con el propósito de establecer los roles, autoridades y responsabilidades de cada uno.

Autoridades y Responsabilidades:
Las responsabilidades se asignan de acuerdo con la estructura anterior respecto a gobierno, administración y gestión del riesgo, así:

Copia no controlada



5.3. Funciones y Responsabilidades en la Gestión del Riesgo en La Cardio:

5.3.1. Responsables del Gobierno:

Responsable	Funciones y Responsabilidades
Junta Directiva - Comité de Auditoría y Riesgos	1. Aprobar: La asignación de 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. 2. Fortalecer: Fomentar una cultura de gestión de riesgos. 3. Supervisar y monitorear la gestión de riesgos. • Monitorear los "riesgos estratégicos" y aquellos de mayor impacto que le sean elevados por la Gerencia de riesgos. • Supervisar las funciones de la Gerencia de Control Interno y Riesgos, así como, aprobar el reglamento, de acuerdo con las normas legales que le apliquen. • Pronunciarse y hacer seguimiento sobre los informes periódicos que elabore el Comité de Auditoría y Riesgos, respecto a los niveles de riesgo asumidos por la Organización, 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. • Vigilar el adecuado funcionamiento del Eje de Riesgos, como ente delegado por la Administración para ayudar en la correcta administración de riesgos de La Cardio.

Copia no controlada

5.3.2. Responsables de la Administración:

Responsable	Funciones y Responsabilidades
Dirección Ejecutiva	1. Definir el contexto del Sistema de Gestión Integral de Riesgos. 2. Aprobar y promover el cumplimiento efectivo de la presente política y demás lineamientos del Sistema de Gestión Integral de Riesgos. 3. Incentivar la conformación de los grupos de gestión de riesgo. 4. Considerar las competencias y limitaciones de los recursos existentes para la gestión del riesgo.

Responsable	Funciones y Responsabilidades
	5. Asegurar la asignación de los recursos suficientes para la gestión de riesgos (talento humano - programas de entrenamiento, habilidades, experiencia y competencias; presupuesto; procesos, métodos y herramientas para gestionar los riesgos; procesos y procedimientos documentados; Sistema de información módulo de riesgos). 6. Hacer seguimiento a los resultados de los indicadores del sistema de gestión de riesgos, así como de los de procesos.
Área de Riesgos	1. Definir • El contexto del Sistema de Gestión Integral de Riesgos. • La política de riesgos y presentarla para aprobación. • La documentación y metodologías para la segmentación, identificación, análisis, evaluación, control, monitoreo y tratamiento de los diferentes Subsistemas de Administración de Riesgos (Programa, instructivos, formatos, etc.) del Sistema de Gestión Integral de Riesgos. 2. Fortalecer: Fomentar una cultura de gestión de riesgos. 3. Supervisar y Monitorear: • El sistema de información del Sistema Integrado de Gestión de Riesgos. • El marco general de indicadores clave de riesgo de para cada subsistema de riesgo y los límites de exposición como mínimo a los riesgos que se encuentren fuera del nivel de tolerancia. • El cumplimiento de los lineamientos del sistema de gestión integral de riesgos. 4. Reportar: A los diferentes órganos de gobierno y control los resultados de la gestión de riesgos.

Copia no controlada

5.3.3. Responsables de la Gestión:

Responsable	Funciones y Responsabilidades
Directores, Gerentes, Jefes, Gestores de Riesgos (Líderes	1. Implementar:

de subsistemas de Riesgos)	• Un sistema de control efectivo para su proceso y mantenerlo. • Acciones correctivas para hacer frente a deficiencias de proceso y control. 2. Ejecutar: • Garantizar la identificación, evaluación, monitoreo y gestión de los riesgos a los cuales se encuentra expuesto su proceso y/o subsistema. • Desarrollar todas las etapas de implementación del SGIR. • Liderar la participación en todas las etapas del SGIR y fomentar el compromiso de los miembros de su equipo de trabajo. • Definir, implementar y ejecutar planes de tratamiento del riesgo efectivos. • Definir los indicadores de efectividad de los controles implementados. • Garantizar que el desarrollo de nuevos proyectos y procesos implemente la metodología de gestión de riesgos. 3. Supervisar y monitorear • Validar periódicamente si el perfil de riesgo se encuentra alineado con el apetito de riesgo. • Monitorear los indicadores de efectividad de los controles implementados 4. Reportar y comunicar: • Presentar informes periódicos de las actividades de gestión de riesgos desarrolladas. • Garantizar que la información requerida y entregada para la gestión de riesgos se encuentre actualizada. • Realizar reporte al Eje de Riesgos de la gestión de riesgo y los riesgos materializados y priorizados.

Copia no controlada

5.3.4. Otros Actores:

Responsable	Funciones y **Responsabilidades**
Eje de Gestión de Riesgos	1. Alinear los procesos institucionales de mejora continua con la gestión de riesgos 2. Monitorear el cumplimiento y efectividad de las acciones implementadas por la Administración para el tratamiento de los riesgos. 3. Autoevaluar estándares de acreditación nacional e internacional asociados a la gestión de riesgos

Responsable	Funciones y Responsabilidades
Control Interno	1. Evaluar el Sistema de Gestión Integral de Riesgos, su efectividad y cumplimiento. 2. Brindar aseguramiento respecto a la evaluación correcta de los riesgos de cada proceso y los planes de tratamiento. 3. Verificar que las políticas y procedimientos del SGIR se cumplan en todos los procesos de La Cardio.
Revisoría Fiscal	1. Presentar en sus informes las debilidades identificadas frente a la gestión de riesgos, controles y al SGIR.

5.4. Metodología para la Gestión de Riesgos:

La metodología y los componentes del Sistema de Gestión Integral de Riesgos serán descritos en el **Programa de gestión Integral de Riesgos E-02-01-A-001**, así como de los diferentes manuales de los subsistemas de gestión de riesgo, documentos que hacen parte de la operativización de la presente política y es de obligatorio cumplimiento.

Copia no controlada

5.4.1. Alineación del Marco estratégico con la Gestión de Riesgo en La Cardio:

Esta política sigue el principio que la gestión de los riesgos no es estática, se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidianas.

Por lo anterior, la gestión de riesgos en La Cardio define como primera fase de gestión la articulación de la estrategia (Misión, visión y objetivos estratégicos y planeación institucional) y el reconocimiento del modelo de operación de los procesos que la operativizan, definiendo un sistema que permite entender y abordar el rango amplio de los riesgos y las interacciones entre ellos, mejorando los diferentes modelos de operación, así como, también el gobierno del riesgo y la cultura del riesgo. Lo anterior, conlleva a que la administración ajuste las estrategias o su implementación en respuesta a las condiciones cambiantes.

5.4.2. Sistema De Gestión Integral de Riesgos

Como estrategia facilitadora para el entendimiento y conocimiento del enfoque y priorización de la gestión de riesgos, se ha diseñado un sistema de gestión integral de riesgos compuesto de seis elementos:

1. Gobierno: Promueve el aseguramiento que la estrategia es ejecutada – Gobierno Corporativo.
2. Estrategia: Permite definir la visión, misión y promesa de valor que orienta a la Organización.

3. Negocio: Corresponde a la gestión de la estructura adecuada para la ejecución de la estrategia.
4. Operación: Permite visualizar cómo debe estar estructurada la ejecución de la estrategia desde cada proceso operativo en La Cardio.
5. Analítica de Datos y Tecnología: Corresponde a la infraestructura de datos, analítica y tecnología que soporta el negocio y la operación de La Cardio.
6. Cultura: Qué valores compartidos guían a la Organización.

Una vez se ha definido el enfoque de gestión de riesgos basado en los pilares estratégicos, se realiza la articulación de la estrategia con el sistema integrado de riesgos, permitiendo definir y segmentar la gestión de riesgos en escenarios de cumplimiento, promesa de valor, sostenibilidad, eficacia operativa, y talento cardio. Este enfoque se articula con lo solicitado en los diferentes escenarios normativos y de acreditaciones nacionales e internacionales.

5.5. Riesgos de Corrupción y Ética

Para la gestión de riesgos de fraude se identifican las posibles en los que un empleado, directivo, funcionario o tercero comete algún acto en perjuicio de la Organización. Los tres tipos principales de fraude en el entorno laboral son corrupción, apropiación indebida de activos y las declaraciones fraudulentas.

Para la identificación de riesgos de corrupción se deben identificar las posibles situaciones de corrupción que podrían presentarse (causas) y consolidar el(los) riesgo(s) de corrupción que podrían surgir a partir de ellas, verificando que el(los) riesgo(s) consolidados(s) refiera(n) a los siguientes componentes: acción u omisión, desviación de la gestión, beneficio privado y uso del poder.

En La Cardio las políticas y lineamientos relacionados a fraude, corrupción y ética empresarial se dimensionan desde el riesgo de cumplimiento alineado a la supervisión del conducta y buen gobierno y a las políticas relacionadas a SICOF.

Copia no controlada

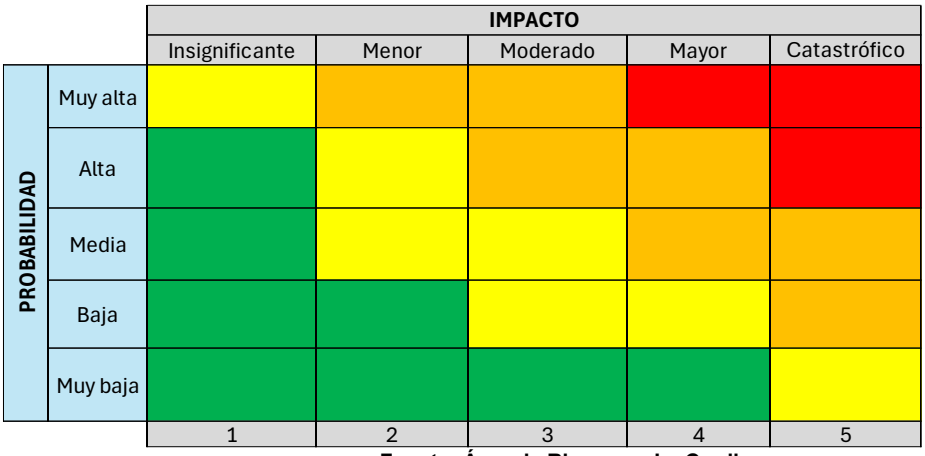
5.6. Nivel de Tolerancia al Riesgo en La Cardio:

La gestión de riesgos debe estar integrada con todas las políticas y procesos de La Cardio; razón por la cual se deben estructurar los procesos considerando siempre la presente política.
Anualmente se debe realizar una evaluación de los riesgos de la organización, partiendo de los objetivos estratégicos y definiendo si los planes de tratamiento implementados son suficientes y efectivos.

Con lo anterior, La Cardio, establece que los riesgos residuales ubicados en las zonas de riesgo Alta y Critica, deben contar con un plan de tratamiento y ser gestionados de manera prioritaria, propendiendo por el crecimiento, la competitividad y la continuidad de La Cardio. Estos riesgos serán monitoreados por la Junta Directiva y/o por el Comité de Auditoría y Riesgos según corresponda y con la frecuencia definida.

La gestión de riesgos de La Cardio debe orientarse a la creación y protección de valor; así como en todos los casos los riesgos que se asumen deben partir de información suficiente y veraz y encontrarse dentro de lo calculado en el apetito de riesgo.

Los riesgos de La Cardio deben ser clasificados de acuerdo con su impacto (insignificante, menor, moderado, mayor y catastrófico) y probabilidad (muy baja, baja, media, alta y muy alta). Las zonas de riesgo en nivel inherente y residual establecidas son: baja (verde), media (amarilla), alta (naranja) y critica (roja), cómo se detalla en el siguiente mapa.



Fuente: Área de Riesgos – La Cardio.

Todos los colaboradores deben actuar de acuerdo con los lineamientos enmarcados en el Código de Gobierno, Ética y Transparencia de La Cardio.

La Cardio no tolerará situaciones o conductas relacionadas con los tres tipos principales de fraude (pirámide del fraude o esquema de fraude) por parte de sus colaboradores, clientes, usuarios, contratistas y proveedores. Para tal efecto, La Cardio implementa un programa de control de fraude y corrupción.

La Administración propenderá por la instauración de las tres líneas de defensa para una correcta definición del Sistema de Control Interno y así facilitar la Gestión integral de riesgos.

Toda actualización de la presente política debe ser aprobada por la Junta Directiva.

Copia no controlada

6. DOCUMENTOS PARA EL DESARROLLO DE LA POLÍTICA

- Reglamento del Comité de Auditoría y Riesgos.
- Programa de Gestión Integral de Riesgos.
- Instructivo Módulo de Riesgos
- Política y Manual del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT.
- Manual SICOF
- Manual Subsistema de Riesgo Financiero.
- Manual Subsistema Riesgo Actuarial.
- Manual de Riesgos del Subsistema Clínico.
- Manual Subsistema de Riesgo Operacional.

7. MEDICIONES PARA LA ADHERENCIA A LA POLÍTICA

- La definición y cuantificación del apetito de riesgo deberá considerar los siguientes aspectos que La Cardio no se encuentra dispuesta a asumir:

  - Violar o incumplir las leyes.
  - Afectar negativamente la reputación.
  - Comprometer la continuidad de la operación.
  - Comprometer la seguridad del paciente.
  - Comprometer la seguridad de todos los colaboradores.

- Para la definición de indicadores se deberá considerar los siguientes aspectos:
  - Ser definidos para los diferentes subsistemas de riesgo.
  - Ser definidos para los riesgos con mayor impacto en el proceso y para los riesgos en nivel residual en zona Alta y/o Crítica.
  - Contribuir en la gestión de las causas generadoras de los riesgos.
  - Contar con unos límites mínimos y/o máximos en sus resultados que generen señales de alerta y estén alineados con el apetito de riesgo.
  - Tener una periodicidad definida para su seguimiento y reporte.
  - Definir específicamente las fuentes de información con las cuales se construye el indicador.

Copia no controlada