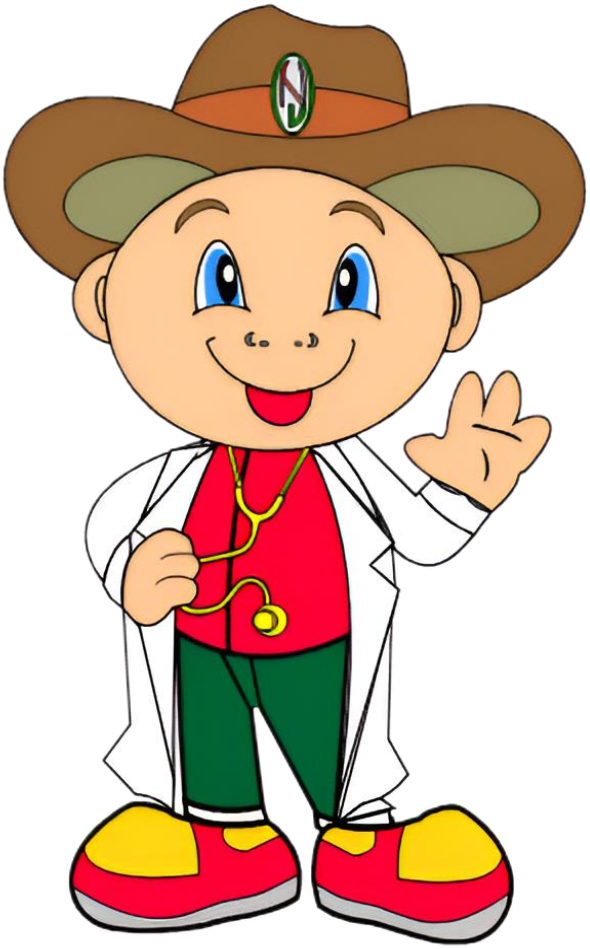
POLITICA INSTITUCIONAL DE ADMINISTRACIÓN DEL RIESGO



HOSPITAL SAN VICENTE DE ARAUCA E.S.E

INTRODUCCIÓN:

La Administración del Riesgo comprende el conjunto de elementos de control y sus interrelaciones, que permiten a la institución evaluar e intervenir en aquellos eventos, tanto internos como externos, que puedan afectar ya sea de forma positiva o negativa el logro de sus objetivos institucionales. Esta política contribuye a consolidar el Sistema de Control Interno y a fomentar una cultura de autocontrol y autoevaluación en el interior del Hospital San Vicente de Arauca ESE.

Teniendo en cuenta que la gestión del riesgo es estratégica para el cumplimiento de los objetivos institucionales y de sus procesos, este documento establece la política marco que orientará la toma de decisiones relativas a la administración del riesgo. La política está alineada y armonizada con el Modelo Integrado de Planeación y Gestión (MIPG), la Guía para la Gestión del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 06 de noviembre de 2022), la norma ISO 31000:2018 Gestión del riesgo — Directrices, siguiendo normatividad de la Supersalud adoptando. Asimismo, la visión del riesgo no solo como una amenaza, sino también como una oportunidad para optimizar resultados.

En un entorno caracterizado por la rapidez de los cambios, la creciente complejidad de la economía, las altas expectativas de la comunidad y los avances tecnológicos, el Hospital San Vicente de Arauca ESE reconoce la necesidad de contar con una estructura organizacional preparada y de una alta capacidad de respuesta para gestionar los riesgos de forma oportuna y efectiva.

1. OBJETIVO GENERAL:

Determinar los lineamientos internos del Hospital San Vicente de Arauca ESE que permitan la implementación de herramientas para la identificación y gestión efectiva de los riesgos institucionales, así mismo, facilitar la toma de decisiones estratégicas, minimizando los impactos negativos derivados de amenazas del entorno o debilidades en los procesos, y potenciando oportunidades que generen valor a la gestión, asegurando el cumplimiento de los objetivos y la satisfacción de los usuarios y demás grupos de interés.

OBJETIVOS ESPECIFICOS:

1. Fortalecer las competencias y el compromiso del talento humano en la adopción de acciones orientadas al cumplimiento de sus funciones con un enfoque preventivo de gestión del riesgo.
2. Analizar el contexto interno y externo del hospital para impulsar la mejora continua en la gestión institucional.
3. Fortalecer la toma de decisiones mediante la aplicación de metodologías de identificación, valoración y tratamiento de los riesgos dentro del hospital.
4. Diseñar estrategias que permitan proteger los recursos institucionales, minimizando el impacto de riesgos potenciales.
5. Proporcionar herramientas para la identificación, análisis y evaluación de los riesgos, estableciendo roles y responsabilidades claras para cada servidor en la gestión del riesgo.

2. ALCANCE:

La Política de Gestión del Riesgo del Hospital San Vicente de Arauca ESE se aplica a todas las acciones y procedimientos ejecutados por los servidores públicos en el ejercicio de sus funciones. Abarca los distintos procesos, planes, programas y proyectos institucionales, con un enfoque en la prevención y control de riesgos de gestión, fiscales, de corrupción y de seguridad de la información, garantizando la integridad y eficiencia de la entidad.

3. TERMINOS Y DEFINICIONES:

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Consecuencia: efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento, o un beneficio.

Control: Medida que permite reducir o mitigar un riesgo.

Efecto: Es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Factores de Riesgo Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP): hacen relación a todas las posibles pérdidas que pueden afectar a la empresa a causa de operaciones o acciones que están relacionadas con actividades o procesos terroristas o para financiar la proliferación de armas a gran escala, o para ocultar intencionalmente de Activos.

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Son las consecuencias que puede ocasionar a la organización la materialización del riesgo, que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas**.**

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.

Riesgo residual: Resultado de aplicar la efectividad de los controles al riesgo inherente.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo. Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, que transforma elementos de entrada en elementos de salida para generar un valor.

Plan Anticorrupción y de Atención al Ciudadano - PAAC: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Riesgo Fiscal: Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Riesgos estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

Riesgos gerenciales: Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

Riesgos operacionales: Probabilidad que una entidad presente desviaciones en los objetivos misionales, como consecuencia de deficiencias, inadecuaciones o fallas en los procesos, en el recurso humano, en los sistemas tecnológicos, legal y biomédicos, en la infraestructura, por fraude, corrupción y opacidad, ya sea por causa interna o por la ocurrencia de acontecimientos externos, entre otros.

Riesgo de Crédito. 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.

Riesgos de Liquidez: 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).

Riesgos tecnológicos: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Riesgos de cumplimiento: Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

Riesgo de imagen o reputación: Posibilidad de toda acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de una entidad, tales como el impacto de la publicidad negativa sobre las prácticas comerciales, conducta o situación financiera de la entidad. Tal publicidad negativa, ya sea verdadera o no, puede disminuir la confianza pública en la entidad, dar lugar a litigios costosos, a una disminución de su base de usuarios, clientes, negocios o los ingresos, entre otros.

Riesgos de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

Gestor público: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales".

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique).

Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.

b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

Lavado de Activos o LA: es el delito tipificado en el artículo 323 del Código Penal Colombiano. El que adquiera, resguarde, invierta, transporte, transforme, almacene conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias psicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, o vinculados con el productos de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho.

4. CONTEXTO ESTRATÉGICO

De acuerdo con la política de planeación establecida por el Departamento Nacional de Planeación (DNP), el contexto en el que opera el Hospital San Vicente de Arauca ESE está detalladamente descrito en su Plan de Desarrollo Institucional. Este instrumento de planificación estratégica define la misión y visión institucional, los objetivos estratégicos que guían su gestión y un análisis integral de los factores que impactan su funcionamiento.

Antes de proceder con la identificación de los riesgos asociados a los procesos, es fundamental realizar un diagnóstico detallado del entorno en el que se desarrolla la actividad hospitalaria. Este análisis debe considerar factores internos, como la disponibilidad de recursos, la capacidad operativa y la cultura organizacional, así como factores externos, incluyendo el contexto socioeconómico, normativo, político y ambiental. Comprender este entorno permite establecer una base sólida para identificar riesgos relevantes, anticipar posibles escenarios y definir estrategias de mitigación alineadas con los objetivos institucionales y las necesidades de los usuarios y demás grupos de interés.

4.1. CONTEXTO EXTERNO

4.1.1. MARCO LEGAL Y NORMATIVO:

- Constitución Política, artículos 209 y 269 Carta magna de la República de Colombia. Artículo 209: Fundamentos en los principios de los servidores públicos. Artículo 269: Funciones y procedimientos de Control Interno.

- Ley 87 de 1993 Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones Lineamientos generales del ejercicio de Control Interno.

- Decreto 1499 de 2017 Por medio del cual se modifica 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 Integración en un solo el Sistema de Gestión los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en el Modelo Integrado de Planeación y Gestión MIPG.

- Ley 1474 de 2011, Artículo 73 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública Relacionado con la prevención de los riesgos de corrupción, mapa de riesgos de corrupción.

- Decreto 1083 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Se establece los ámbitos de aplicación del Sistema de control interno y la administración del riesgo.

- CIRCULAR EXTERNA 20211700000004-5 DE 2021 15-09-2021 por la cual se imparten instrucciones generales relativas al código de conducta y de buen gobierno organizacional, el sistema integrado de gestión de riesgos y a sus subsistemas de administración de riesgos.

- NTC ISO 31000 versión vigente Gestión del Riesgo, Principios y Directrices.

- Guía de auditoría interna basada en riesgos para entidades públicas - Versión Actualizada.

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP). Versión Actualizada.

4.2. CONTEXTO INTERNO

5. RESPONSABILIDADES:

Las responsabilidades para lograr el cumplimiento de la política y el despliegue de la metodología institucional están definidas mediante el Esquema de las líneas de defensa del Modelo Integrado - MIPG y en el Hospital San Vicente de Arauca ESE, se acogen según la siguiente tabla:

Tabla 1

Responsabilidades frente al riesgo (Líneas de defensa)

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	**Alta Dirección Comité institucional de coordinación de control interno**	• Aprobar la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad y evaluar su aplicación. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. • Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo. • Evaluar el estado del sistema de control interno, acorde con la información generada por parte de las instancias de 2ª línea identificadas y la actividad de control definida que materializa la línea de reporte en cada caso, acorde con el tema del cual son responsables, a fin de generar acciones y una toma de decisiones con enfoque preventivo.
	Comité de Gestión y Desempeño Institucional	• Asegurar la implementación y articulación de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo en diferentes ámbitos institucionales. • Generar recomendaciones de mejora a la política de administración del riesgo para su inclusión y aprobación en el Comité Institucional de Coordinación de Control Interno. • Realizar seguimiento y análisis periódico a los riesgos institucionales y proponer mejoras a su estructura.
1ª Línea	**Líderes y/o Responsables de Procesos**	• Identificar y valorar los riesgos que pueden afectar el proceso, los programas, proyectos, planes y procedimientos a su cargo y actualizarlo cuando se requiera. • Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso y reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Informar a la Oficina Asesora de Planeación o quien haga sus veces (como 2ª línea de defensa) sobre los riesgos materializados en los procesos, programas, proyectos y planes a su cargo. En caso de la materialización de un riesgo no identificado, este debe ser incluido en el mapa de riesgo del proceso correspondiente. • Establecer y aplicar las acciones de mejora requeridas frente al mapa de riesgos correspondiente, una vez se genera el informe de materialización del riesgo.
2ª Línea	**Oficina Planeación**	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para una adecuada definición de la política de administración del riesgo, el establecimiento de los riesgos al proceso de Direccionamiento acorde con el esquema de procesos actual, o bien el que lo actualice o sustituya cuando existan cambios en dicho esquema de operación. • Identificar cambios en el entorno (interno o externo) que afecten el apetito del riesgo en la entidad • Consolidar el mapa de riesgos institucional, con un enfoque para el análisis de los riesgos de mayor criticidad frente al logro de los objetivos y presentarlo periódicamente ***(anualmente)*** ante la Línea Estratégica para su análisis y toma de decisiones correspondiente. • Informar a la 1ª línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado para que sea identificado e incluido en el mapa de riesgo del proceso correspondiente.
	Gestión de TIC'S	• Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de la Información en la entidad. • Asesorar a los líderes de proceso en la identificación de los riegos de seguridad de la información. • Supervisar la respuesta a incidentes sobre violaciones de la seguridad, informando a la Línea Estratégica sobre sus consecuencias y acciones implementadas. • Generar informes ***(anualmente)*** sobre fugas de información y los medios externos identificados. • Proponer a la Línea estratégica medidas y mecanismos para mejorar la gestión de seguridad de la información.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
2ª Línea	**Gestión de talento humano**	El **AREA DE TALENTO HUMANO DEL HOSPITAL,** cuatrimestralmente consolidará el avance sobre PIC, Bienestar, Incentivos y temas de convivencia laboral, mediante un análisis de variables relacionadas con la ejecución de cada uno de estos mecanismos, que permita generar alertas en la ejecución de recursos. En el tema de convivencia generar información sobre quejas reiteradas de acoso laboral, conflictos internos que no ha sido posible resolver y aquellos que llegan a instancia disciplinaria.
	Atención al usuario	• **El AREA DE ATENCIÓN AL USUARIO** trimestralmente, evalúa la prestación del servicio a los grupos de valor, mediante el análisis de las PQRSD y la evaluación de percepción de los usuarios por los diferentes medios de atención, generando alertas en semáforo sobre incumplimiento en términos, reiteraciones de consultas, quejas, denuncias y tutelas que se hayan presentado o que estén en curso. • El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Coordinador de Servicio al Ciudadano como líder del proceso de gestión del Servicio al Ciudadano.
2ª Línea	**Defensa jurídica**	• El Líder de Defensa Jurídica trimestralmente, verifica el seguimiento a la gestión judicial adelantada por los abogados asignados, generando información sobre alertas en los procesos que se encuentran abiertos y las cuantías asociadas. • El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Director Jurídico como líder del proceso de Defensa Jurídica.
	Gestión de TIC'S	• El Líder de la oficina TIC´S trimestralmente verifica el avance en los programas y proyectos desagregados por tema y recursos asociados, generando alertas sobre retrasos o posibles incumplimientos, a fin de tomar las acciones o intervenciones necesarias. La fuente para el análisis son los informes de los supervisores o interventores de los programas o proyectos • El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Jefe

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		de TIC como líder del proceso de Tecnologías de la Información.
3ª Línea	**Asesor de Control Interno o quien haga sus veces**	• Llevar a cabo la evaluación independiente a los riesgos registrados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional Coordinador de Control Interno. Para esto tendrá en cuenta los resultados de los seguimientos aplicados por parte de la Oficina Asesora de Planeación, así como del oficial de seguridad, a fin de contar con información de base para sus evaluaciones y generar recomendaciones a estas instancias. • Generar recomendaciones y/o alertas con alcance preventivo a la línea estratégica, a fin de incorporar acciones inmediatas a los temas críticos identificados. • Asesorar y acompañar a toda la Alta Dirección en la incorporación de estrategias y metodologías para la gestión de riesgo, acorde con las actualizaciones en materia de riesgos corrupción, fiscales, de lavado de activos y otros que se definan en normas nacionales.

Fuente: Elaboración propia.

Todos los Servidores, Contratistas de Apoyo y Funcionarios del Hospital San Vicente de Arauca ESE son responsables de la correcta ejecución de sus funciones, incorporando los valores establecidos en el Código de Integridad. Su compromiso se orienta a la reducción de los riesgos que puedan surgir en el desarrollo de sus actividades y a garantizar la eficacia de los controles integrados en los procesos, subprocesos, procedimientos, actividades y tareas a su cargo.

Los responsables de los procesos tienen la obligación de identificar situaciones que puedan afectar el desarrollo de las actividades o comprometer el logro de los objetivos institucionales. Para ello, deben establecer controles adecuados, evaluar su pertinencia y asegurar su implementación con el fin de mitigar los riesgos. Estos controles deben formalizarse y comunicarse al Proceso de Administración del Sistema Integrado de Gestión, permitiendo así la actualización continua de los mapas de riesgos.

En el caso de los procesos misionales, sus responsables deben identificar los riesgos que puedan impactar cada uno de los instrumentos de política formulados, determinando controles eficaces que reduzcan tanto la probabilidad de ocurrencia como su impacto.

Asimismo, los responsables de los procesos deben garantizar la disponibilidad de los recursos necesarios (físicos, financieros y de talento humano) para la implementación y sostenimiento de los controles establecidos, evitando la materialización de los riesgos.

Finalmente, deben mantener evidencia documentada de la aplicación de los controles definidos para los riesgos identificados, asegurando la trazabilidad y eficacia de la gestión del riesgo dentro del hospital.

6. CONDICIONES GENERALES:

6.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El Hospital San Vicente de Arauca ESE se compromete a integrar la administración del riesgo en todos sus procesos y niveles organizativos, garantizando la identificación, evaluación, tratamiento y seguimiento de aquellos riesgos que puedan afectar la seguridad del paciente, la calidad del servicio y el cumplimiento de los objetivos institucionales, mediante la aplicación oportuna de medidas de control, el impulso de la mejora continua y la promoción de una cultura organizacional basada en la prevención, el autocontrol y la toma de decisiones informada.

6.2. METODOLOGÍA APLICADA:

La metodología aplicada para la administración del riesgo en el Hospital San Vicente de Arauca ESE se fundamenta en los lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, complementados con los requisitos de la norma ISO 31000:2018. Por ende, la implementación del Sistema de Gestión del Riesgo en el Hospital San Vicente de Arauca ESE se llevará a cabo siguiendo la metodología establecida en la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP), en su versión vigente. Esta metodología contempla el desarrollo de las siguientes acciones:

6.2.1. TIPOLOGÍAS DE RIESGOS

- **Riesgo en Salud**
  Se refiere a la probabilidad de que eventos adversos afecten la salud de la población atendida, incluyendo la aparición de enfermedades, complicaciones o cualquier situación que comprometa el bienestar de los pacientes.

- **Riesgo Operacional**
  Es la posibilidad de pérdidas debido a fallas en los procesos internos, personas, sistemas o por eventos externos que afecten la continuidad y calidad de los servicios de salud.

- **Riesgo Actuarial**
  Involucra la incertidumbre asociada a las estimaciones y proyecciones financieras relacionadas con los costos de atención en salud, incluyendo desviaciones en la frecuencia y severidad de los eventos que generan gastos.

- **Riesgo De Crédito**
  Es la probabilidad de que una contraparte incumpla sus obligaciones financieras, afectando la liquidez y estabilidad financiera de la entidad de salud.

- **Riesgo De Liquidez**
  Se refiere a la posibilidad de que la entidad no pueda cumplir con sus obligaciones financieras de manera oportuna debido a la falta de recursos líquidos disponibles.

- **Riesgo de Lavado de Activos y Financiación del Terrorismo**
  Es la probabilidad de que la entidad sea utilizada, de manera directa o indirecta, para el lavado de activos o la financiación de actividades terroristas, lo que puede generar sanciones legales y reputacionales.

- **Riesgo de Seguridad de la Información**
  Involucra la posibilidad de que la información sensible de la entidad sea comprometida en términos de confidencialidad, integridad o disponibilidad, afectando la confianza y operación de los servicios de salud.

- **Riesgo de Gestión**
  Son aquellos que pueden afectar el cumplimiento de los objetivos estratégicos, la eficiencia operativa y la calidad del servicio en la institución. Se derivan de fallas en los procesos internos, deficiencias en la toma de decisiones, falta de planeación, problemas en la asignación de recursos y baja capacidad de respuesta ante situaciones imprevistas.

- **Riesgo Fiscal**
  Hace referencia a la probabilidad de que la entidad incurra en situaciones que afecten la sostenibilidad financiera, generando impactos negativos en la estabilidad económica del hospital. Este tipo de riesgo está asociado con la ejecución presupuestal, la gestión de ingresos y egresos, así como el cumplimiento de las obligaciones financieras.

- **Riesgo de Corrupción**
  El riesgo de corrupción hace referencia a la posibilidad de que, dentro del Hospital San Vicente de Arauca ESE, ocurran acciones u omisiones que comprometan la transparencia, la ética y la legalidad en la gestión institucional. Estos riesgos pueden materializarse en situaciones como abuso de poder, conflictos de interés, fraude, sobornos o cualquier otra práctica que afecte la integridad y confianza en la entidad.

  Nota: Los riesgos de corrupción deben ser analizados en los niveles moderado, mayor y catastrófico teniendo en cuenta lo significativo para la institución de estos riesgos, es decir que los niveles de impacto menor y leve no aplican.

A. Para los riesgos diferentes a los Riesgos Fiscales, Riesgos de Corrupción y Riesgos de Seguridad de la Información.

1) Identificación de Riesgos
   - Análisis del contexto estratégico
   - Análisis de Objetivos Estratégicos y de los procesos
   - Identificación de los puntos de riesgo.
   - Identificación de áreas de impacto.
   - Identificación de áreas de factores de Riesgo.
   - Descripción del Riesgo.
2) Valoración de Riesgos.
   - Análisis de Riesgos.
   - Evaluación del riesgo.

- Estrategias para combatir el riesgo.
- Herramientas para la gestión del riesgo.
- Monitoreo y revisión.

B. Para los riesgos relacionados con posibles Riesgos Fiscales

- Identificación de riesgos fiscales (puntos de riesgo de control y situaciones inmediatas)
- Identificación de áreas de Impacto.

  Nota: *el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público.*

- Valoración del riesgo fiscal.
- Valoración de controles.
- Nivel de riesgo (riesgo residual).
- Estrategias para combatir el riesgo.

C. Para los riesgos relacionados con posibles actos de Corrupción

- Definición de Riesgos de Corrupción
- Valoración de los Riesgos de Corrupción (cálculo de la probabilidad e Impacto)
- Valoración de Controles – diseño de controles.
- Tratamiento de Riesgo de Corrupción.
- Monitoreo
- Seguimiento de los Riesgos de Corrupción

Nota: El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo, de acuerdo a la tabla de valoración de impacto definida en la guía para la administración del riesgo definida por el DAFP, en la versión que se encuentre vigente

D. Para la Identificación de riesgos relacionados con riesgos de seguridad de la información.

- Identificación de los activos de seguridad de la información.
- Identificación de Riesgos relacionados con Pérdida de la Confidencialidad, Pérdida de la Integridad, Pérdida de disponibilidad

Nota: Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el “Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas” donde se encuentran las siguientes tablas necesarias para este análisis:

Tabla de amenazas comunes.

Tabla de amenazas dirigida por el hombre

Tabla de vulnerabilidades comunes

- Valoración del riesgo.
- Controles asociados a la Seguridad de la Información.

6.2.2. TRATAMIENTO.

Para la gestión de riesgos, se implementan diferentes estrategias de respuesta, las cuales se aplican según la frecuencia y gravedad del riesgo evaluado, considerando las características de cada medida, el análisis costo-beneficio y los siguientes lineamientos:

1) **Aceptar**: Se aceptan aquellos riesgos cuya frecuencia es baja y cuyo impacto es leve, siempre que no comprometan la institucionalidad, el cumplimiento normativo, la seguridad de las personas o la integridad de los bienes. No obstante, los riesgos asociados a corrupción son inaceptables en cualquier circunstancia.

2) **Reducir:** Para los riesgos con una frecuencia media o alta, se deben diseñar e implementar medidas preventivas y controles que disminuyan la probabilidad de ocurrencia.

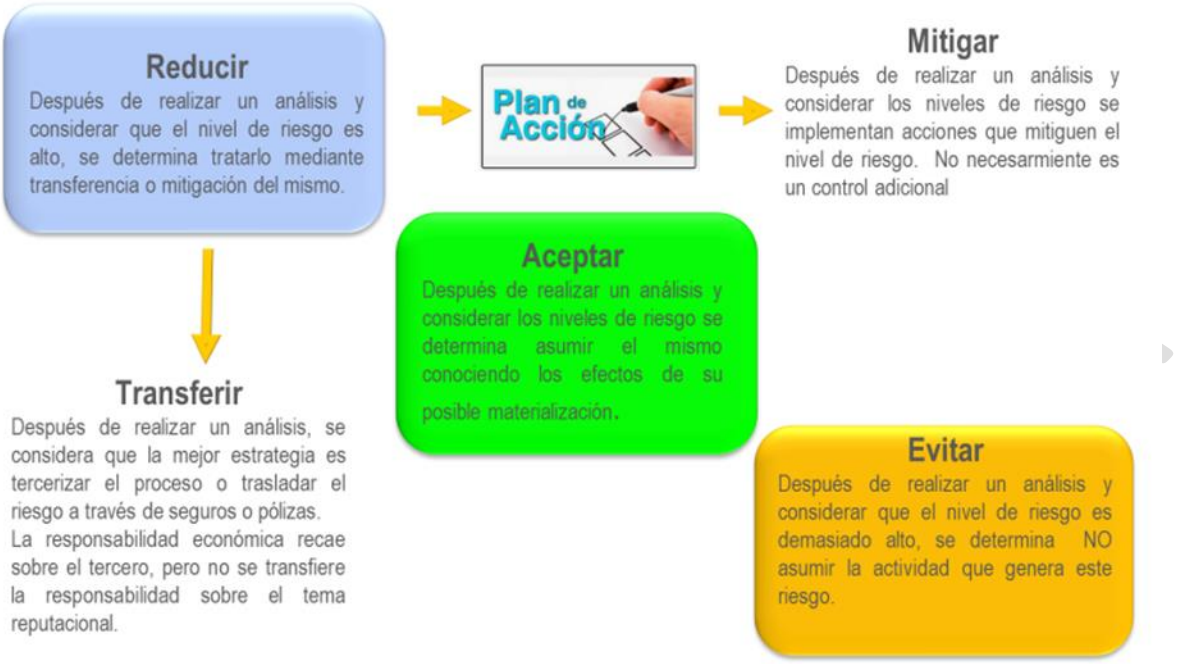
   En los casos en que los riesgos presenten un impacto alto o catastrófico para la entidad, se deben establecer controles y estrategias de mitigación dirigidas a reducir la gravedad de sus efectos y daños en caso de materialización.

   Si el impacto es moderado, se realizará un análisis costo-beneficio para determinar la magnitud de los efectos y definir la respuesta más adecuada.

3) **Evitar o eliminar:** Los riesgos con una probabilidad de ocurrencia alta y un impacto catastrófico deben evitarse en la medida de lo posible. Para ello, se debe eliminar la actividad que origina el riesgo, siempre que sea viable según la Constitución y la normativa vigente.

   Cuando la eliminación de la actividad no sea factible, se implementarán todas las medidas necesarias para su tratamiento y control.

   Para los riesgos calificados como catastróficos, se deben diseñar planes de emergencia (si implican daños a personas o bienes) o planes de contingencia (si afectan únicamente la prestación del servicio), con el objetivo de minimizar sus consecuencias.



Fuente: Guía de Administración del Riesgo y Diseño de Controles en Entidades Públicas versión 6.

6.3. FRECUENCIA DE ACTUALIZACIÓN

El proceso de actualización de la gestión del riesgo se realizará anualmente mediante el formato de gestión del riesgo establecido por el Hospital San Vicente de Arauca ESE, conforme a las responsabilidades definidas en la presente política.

Los responsables de los procesos deberán garantizar la actualización de los riesgos identificados, la correcta implementación de los controles establecidos y el seguimiento continuo de su efectividad. Para ello, se documentará el proceso en el Formato de Mapa de Riesgos del Hospital San Vicente de Arauca ESE.

La Política de Administración del Riesgo será revisada cuando sea necesario, por solicitud del Representante de la Alta Dirección, tomando en cuenta las recomendaciones y directrices del Comité Institucional de Coordinación de Control Interno. Así mismo, se ajustará en caso de modificaciones metodológicas o cambios normativos que lo exijan.

6.4. MONITOREO, SEGUIMIENTO Y EVALUACIÓN

El Monitoreo, seguimiento y evaluación de las acciones de control y las implementadas para el tratamiento de los riesgos se llevará a cabo de manera cuatrimestral, siendo responsabilidad de la primera línea de defensa (líderes de proceso), la verificación del cumplimiento de las acciones de control, la realización de informe de autocontrol y el reporte del mismo a Planeación como coordinador de la segunda línea de defensa quien con los demás miembros de esta línea de defensa adelantará la verificación y validación de las evidencias, solicitará

los ajustes correspondientes y finalmente realizará informe de autoevaluación que someterá a mesa técnica con la Línea Estratégica de Defensa, a través del Comité Institucional de Gestión y Desempeño, y a su vez, remitirá a la tercera línea para que adelanté el verificación, monitoreo y seguimiento, solicite los ajustes necesarios y realice el informe de evaluación independiente, que se someterá a análisis y toma de decisiones de nivel directivo a través del Comité Institucional de Coordinación de Control Interno.

Para garantizar la trazabilidad y efectividad del proceso de Administración de Riesgos, este deberá ser documentado en todas sus etapas. Para ello, se contará con un sistema de información que facilite su gestión, actualización y consulta.

6.5. EVALUACIÓN DE LA GESTIÓN DEL RIESGO

La Comité Institucional de Coordinación de Control Interno será el encargado de evaluar la gestión del riesgo, realizando un seguimiento periódico a los avances en la implementación de las acciones definidas. Esta evaluación se llevará a cabo a través de informes de monitoreo, seguimiento y/o auditorías internas y de los informes de autocontrol, autoevaluación y evaluación independiente generados por la primera, segunda y tercera líneas de defensa, con el objetivo tomar decisiones sobre el tratamiento adoptado, prevenir la materialización de los riesgos y generación de las acciones correspondientes sobre la identificación de riesgos materializados.

6.6. COMUNICACIÓN Y CONSULTA

Con el propósito de fortalecer la cultura organizacional en torno a la gestión del riesgo en el Hospital San Vicente de Arauca ESE, la comunicación y divulgación, de la Política de Administración de Riesgos, de los riesgos identificados y los controles definidos para su mitigación estarán a cargo de los Líderes de Proceso, como primera línea de defensa. Estos responsables deberán garantizar la socialización y asignación de responsabilidades sobre los riesgos asociados al proceso y las medidas de control establecidas, a su equipo de trabajo, asegurando que todos los funcionarios y contratistas de apoyo bajo su cargo conozcan y apliquen las acciones correspondientes. Igualmente cada líder de proceso deberá adelantar el Monitoreo e informe de autocontrol y reportar cuatrimestralmente a la segunda línea de defensa.

7. DOCUMENTOS/ REGISTROS:

- MATRIZ DE RIESGO INSTITUCIONAL
- MAPA DE RIESGO POR PROCESOS
- MATRIZ DE RIESGO DE CORRUPCIÓN

8. CONTROL DEL DOCUMENTO:

El presente documento deberá reposar en la siguiente ruta: Z:\BIBLIOTECA HSVA\1. MANUAL DE DOCUMENTOS HSVA\1. PROCESOS ESTRATEGICOS\1. GESTION DIRECCIONAMIENTO ESTRATGICO\1.2 PLANEACIÒN\POLITICA

CONTROL DE CAMBIOS				
VERSION	**FECHA APROBACIÓN**			**MOTIVO**
	DIA	**MES**	**AÑO**	
01				Creación del documento.
02	31	01	2021	Política de administración de riesgo resolución No. 20496 del 25 de octubre del 2021
03	13	10	2022	Actualización de la política de Administración de Riesgo conforme a los lineamientos de la circular externa CIRCULAR EXTERNA 20211700000004-5 DE 2021 y a la guía de Administración de riesgo versión 05 del DAFP.
04	08	04	2025	Actualización según la versión 06 de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) y la norma ISO 31000:2018. Cambio de codificación GDE-PL-DE-PO-001 ahora DE-PL-PO-01.

ELABORÓ Y/O ACTUALIZÓ:	**REVISÓ:**	**APROBÓ:**
NOMBRE: Ana María Ibarra	**NOMBRE:** Sergio Botia Valencia	**NOMBRE:** Comité institucional de gestión y desempeño
CARGO: Profesional de planeación	**CARGO:** Profesional especializado planeación	Acta No. 02 del 2025
FECHA: 14/02/2025	**FECHA:** 17/02/2025	**FECHA:** 08/04/2025