POLÍTICA DE GESTIÓN DEL RIESGO

1. INTRODUCCIÓN

El Hospital Departamental San Antonio de Padua de La Plata Huila, es una Empresa Social del Estado que en cumplimiento a las normas constitucionales y legales que rigen el estado colombiano, enmarca la política de Administración de riesgo, en un sistema integrado de riesgos, siendo la principal fuente metodológica los lineamientos que establece el Departamento Administrativo de la función pública, a través de la Guía para la administración del riesgo y el diseño de controles en entidades públicas. En cumplimiento a directrices que imparte la Superintendencia Nacional de Salud el cual implica tener en cuenta los riesgos que hace referencia la circular externa 20211700000004-5 de 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.

La Política de Administración del riesgo es la expresión del compromiso del equipo directivo de la ESE Hospital Departamental San Antonio de Padua de La Plata Huila frente a la identificación, tratamiento, control de los riesgos y oportunidades, que influencian los resultados de la gestión y permiten el cumplimiento de las metas establecidas en el Plan Estratégico de Gestión Institucional y en los Planes de Acción.

Así mismo, la política involucra, mediante un ámbito estratégico y el modelo de las líneas de defensa, a todos los colaboradores de la entidad, soportándose en los mecanismos de comunicación disponibles, y cubriendo todas las responsabilidades institucionales, cada proceso y las propias de cada colaborador, los niveles de aceptación de riesgo, los ciclos de establecimiento y seguimiento, los niveles de calificación, la identificación de riesgos de gestión, de corrupción y seguridad digital, entre otros, que hacen parte fundamental del lenguaje y herramientas disponibles para la administración de riesgos.

2. JUSTIFICACIÓN DE LA POLÍTICA

La ESE Hospital Departamental San Antonio de Padua de La Plata Huila orientado al cumplimiento de los objetivos afronta factores internos y externos que crean inseguridad sobre el cumplimiento de los objetivos institucionales; para ejercer control en los eventos que pueden materializar los riesgos o promover aquellos que conllevan al éxito; la alta dirección, responsables de procesos, colaboradores y todos los servidores públicos deben reconocer y desarrollar el proceso de la gestión de riesgos: identificar, analizar, evaluar, tratar y monitorear los riesgos según sea el contexto de cada proceso.

Dicha política tiene como finalidad suministrar herramientas y mecanismos que brinden estrategias preventivas y correctivas que contribuyan a la prevención y control eficaz del mismo. Buscando fortalecer las disposiciones ya establecidas para la protección y seguridad de todo el entorno.

3. Objetivo General

Crear una cultura en la Empresa Social del Estado el Hospital Departamental San Antonio de Padua de identificación, valoración, análisis y control de los riesgos que pueden generar impactos o consecuencias al sistema de Planeación y gestión para el logro de los objetivos del Direccionamiento estratégico de la Entidad.

3.1 Objetivos Específicos

1. Promover una cultura ética para la prevención, detección e investigación de los riesgos de la entidad.

2. Identificar de manera razonable, los impactos negativos generados a partir de la identificación de riesgos y su priorización.

3. Promover las buenas prácticas, medidas preventivas y controles que puedan impactar en el logro de los objetivos institucionales, suscitando que la gestión del riesgo sea una parte integral de la planeación y ejecución de los procesos.

4. Incluir dentro de los procesos y procedimientos de la entidad las acciones necesarias para minimizar los riesgos de las actividades que se desarrollan.

5. Tomar una posición de "Cero Tolerancia" al fraude y a cualquier acto de corrupción que se genere en la Entidad.

6. Promover una cultura de transparencia, que integre los diferentes sistemas de gestión orientados a la identificación, detección, evaluación, mitigación, monitoreo, investigación, prevención y corrección de conductas relacionadas con la corrupción.

7. Dar cumplimiento a la legislación vigente.

4. META

Inicia en la Identificación del Riesgos, aplicando La Política de Administración del Riesgo a los Planes de direccionamiento, procesos estratégicos, misionales, de apoyo y de evaluación, y a todas las acciones ejecutadas por los colaboradores de la ESE Hospital Departamental San Antonio de Padua de La Plata Huila, para su respectiva clasificación y valoración, termina en la construcción de la matriz donde se establece un plan de acción con sus respectivos controles para prevenir y mitigar los riesgos identificados.

5. ALCANCE

Abarca todos los procesos, proyectos, actividades, servicios y planes que la política de la organización cubre y regula para la identificación, evaluación, tratamiento y seguimiento de riesgos, desde la gestión planificada y a todas las actividades que se desarrollan para el cumplimiento de la misión de la entidad.

6. VALORES Y PRINCIPIOS ORIENTADORES

6.1 PRINCIPIOS

Los valores y principios de la política de gestión del riesgo son fundamentales para asegurar que la entidad pueda gestionar la incertidumbre y proteger sus activos y objetivos.

Integrada: La gestión de riesgos debe ser parte integral de todas las actividades de la organización, incluida la planificación estratégica y la gestión de cambios.

Estructurada y sistemática: Se debe aplicar un enfoque sistemático, estructurado y oportuno para gestionar los riesgos, asegurando resultados confiables.

Adaptada: El proceso de gestión de riesgos debe adaptarse al contexto interno y externo de la organización, y ser proporcional a los riesgos y objetivos.

Participativa: La participación de las partes interesadas (como colaboradores y líderes) permite una mayor conciencia y una toma de decisiones más informada.

Mejora continua: El proceso debe ser mejorado continuamente a través del aprendizaje y la experiencia, lo que permite una gestión de riesgos más eficaz.

6.2 VALORES

Honestidad: Actuar con transparencia, rectitud y veracidad en todas las actividades relacionadas con la gestión de riesgos.

Respeto: Tratar con dignidad a todas las personas, reconociendo su valor sin importar su condición.

Compromiso: Demostrar una disposición permanente para comprender y resolver las necesidades, buscando siempre mejorar el bienestar.

Diligencia: Cumplir las funciones con atención, prontitud y eficiencia para optimizar el uso de los recursos.

Justicia: Actuar con imparcialidad, equidad y sin discriminación, garantizando los derechos de todos.

7. DEFINICIONES

Activo: Son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apetito de riesgo: Es el máximo nivel de riesgo que los miembros de la junta directiva están dispuestos a aceptar.

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

Confidencialidad: propiedad de la información que la hace no disponible, es decir divulgada a individuos, entidades o procesos no autorizados.

Controles: Medidas prudenciales, preventivas y correctivas que ayudan a contrarrestar la exposición a los diferentes riesgos. Entre estas se encuentra la implementación de políticas, procesos, prácticas u otras estrategias de gestión.

Cultura de autocontrol: Concepto integral que agrupa todo lo relacionado con el ambiente de control, gestión de riesgos, sistemas de control interno, información, comunicación y monitoreo. Permite a la entidad contar con una estructura, unas políticas y unos procedimientos ejercidos por toda la organización (desde la Junta Directiva y la Alta Gerencia, hasta los propios empleados), los cuales pueden proveer una seguridad razonable en relación con el logro de los objetivos de la entidad.

Cronograma: Son las fechas establecidas para implementar las acciones por parte del grupo de trabajo.

Evaluación del Riesgo: Resultado obtenido en la matriz de calificación, evaluación y respuesta a los riesgos.

Controles existentes: especificar cuál es el control que la entidad tiene implementado para combatir, minimizar o prevenir el riesgo.

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 SGSSS o sus obligaciones. Dentro de este conjunto de acciones se incluye, entre otros, el ciclo general de gestión de riesgo.

Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.
Indicadores: se consignan los indicadores diseñados para evaluar el desarrollo de las acciones implementadas.

Integridad: propiedad de exactitud y completitud.

Línea estratégica: define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección, el equipo directivo, incluyendo el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.
Opciones de Manejo: Opciones de respuesta ante los riesgos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual Acciones: es la aplicación concreta de las opciones de manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de manejo del riesgo.

Política de administración del riesgo: Lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.

Primera línea de defensa: a cargo de gestionar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, está a cargo de los gerentes públicos y los líderes de procesos.

Probabilidad: entendida como la posibilidad de ocurrencia del riesgo; ésta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: No. de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Responsables: Son las dependencias o áreas encargadas de adelantar las acciones propuestas.

Riesgo de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de imagen o reputacional: Percepción agregada que sobre una organización tienen los agentes relacionados con ella, sean estos clientes, accionistas, grupos de interés, partes vinculadas o público en general, la cual tiene el potencial de afectar la confianza en la entidad, influenciando su volumen de negocios, y su situación general. Esta puede variar por factores tales como el desempeño, escándalos, menciones en prensa, entre otros.
Riesgo inherente: Nivel de riesgo propio de la actividad, cuya evaluación se efectúa sin considerar el efecto de los mecanismos de mitigación y de control.

Riesgo residual: Nivel de riesgo que resulta luego de la aplicación de las medidas de control o mitigación existentes a los riesgos inherentes. Opciones de Manejo: Opciones de respuesta ante los riesgos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual

Acciones: es la aplicación concreta de las opciones de manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de manejo del riesgo.

Política de administración del riesgo: Lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.

Primera línea de defensa: a cargo de gestionar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, está a cargo de los gerentes públicos y los líderes de procesos.

Riesgo: Posibilidad que ocurra un evento que pueda afectar negativamente el cumplimiento de la operación de una Entidad y que atenten contra los objetivos del SGSSS.

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.

Riesgos de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.

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

Riesgos financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

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

Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

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

Riesgo de Lavado de Activos y Financiación del Terrorismo: es la posibilidad que en la realización de las operaciones de una entidad, estas puedan ser utilizadas por organizaciones criminales como instrumento para ocultar, manejar, invertir o

aprovechar dineros, recursos y cualquier otro tipo de bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos de recursos vinculados con las mismas.

Segunda línea de defensa: asiste y guía a la línea estratégica y a la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)

Tercera línea de defensa: provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera línea y la segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Está conformada por la Oficina de Control Interno o Auditoría Interna.

Tolerancia al riesgo: preparación de la organización o de la parte involucrada para soportar el riesgo después del tratamiento de este con el fin de lograr sus objetivos.

Tratamiento al riesgo: es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

Valoración del Riesgo: es el resultado de determinar la vulnerabilidad de la entidad al riesgo, luego de confrontar la evaluación del riesgo con los controles existentes.

Vulnerabilidad: es una debilidad, atributo, causa o falta de control que permitiría a explotación por parte de una o más amenazas contra los activos.

Atención en Salud: Servicios o tecnologías en salud suministrados a los individuos y a la comunidad para promover, mantener, monitorizar o restaurar el estado de salud.

Conflicto de interés: Se considera que existe un conflicto de interés cuando por una situación de control, influencia directa o indirecta entre entidades, personas naturales o jurídicas, se realicen operaciones, transacciones, decisiones, traslado de recursos, situaciones de ventaja, mejoramiento en la posición de mercado, competencia desleal, desviaciones de recursos de seguridad social, o cualquier

situación de hecho o de derecho que desequilibre el buen funcionamiento financiero, comercial o de materialización del riesgo al interior del sector. Estos desequilibrios tienen su fundamento en un "interés privado" que motiva a actuar en contravía de sus obligaciones y puede generar un beneficio personal, comercial o económico para la parte que incurre en estas conductas.

Seguridad del Paciente: Es el conjunto de elementos estructurales, procesos, instrumentos y metodologías basadas en evidencias científicamente probadas que propenden por minimizar el riesgo de sufrir un evento adverso en el proceso de atención de salud o de mitigar sus consecuencias.

8. REPONSABLES

Los roles y responsabilidades están dadas bajo la operatividad de las líneas de defensa dadas en la siguiente tabla:

LINEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
ESTRATEGICA	ALTA DIRECCION	1.- Establecer objetivos institucionales alineados con el propósito fundamental, metas, y estrategias de la entidad 2.- Promover el reporte de la identificación y prevención del riesgo 3.- Apoyar los canales de comunicación, propiciar espacios y asignar los recursos necesarios para la prevención o control de los riesgos. 4.- Garantizar el cumplimiento de los planes de la entidad
	COMITÉ COORDINADOR DE CONTROL INTERNO.	1.- Revisar la política de administración del riesgo por lo menos una vez al año para su Actualización y validar su eficacia a la gestión del riesgo institucional. se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta 2.- Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. 3.- Garantizar el cumplimiento de los planes de la entidad

SEGUNDA Línea Seguimiento y Monitoreo	**OFICINA DE PLANEACION**	1.- Capacita, Acompaña, genera recomendaciones, define metodología. 2.- Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. 3.- Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al [ogro de los objetivos). 4.-linea de reporte: Monitoreo y seguimiento.
TERCERA Línea de defensa Evaluación independiente	**OFICINA DE CONTROL INTERNO**	1.- Asesora de forma cordinada con la oficina de Planeacion a la primera línea de defensa en la identificación de riesgos institucionales, de corrupción, y de seguridad de la información y diseño de controles. 2.-Llevar a cabo la evaluación independiente a los riesgos registrados en el mapa de riesgos de conformidad con el plan anual de auditoria interna reportar los resultados al comité institucional coordinación de control interno. 3.-Recomendar a la línea estratégica mejoras a la política de administración de riesgos.

9. ESTRATEGIA

La Empresa Social del Estado el Hospital Departamental San Antonio de Padua, para identificar, evaluar, controlar, prevenir y mitigar los riesgos que puedan afectar el logro de sus objetivos y, especialmente, el cumplimiento de los objetivos del SGSSS y sus obligaciones contractuales. Para efectos de la implementación del sistema integrado de riesgos a continuación se describe cada uno de los subsistemas de Administración de Riesgos:

9.1 CICLO GENERAL DE GESTIÓN DE RIESGOS:

9.1.1.- POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Administración de riesgo debe ser extensiva y aplicable a todos los procesos, en articulación con los líderes de procesos que buscan identificar los riesgos que puedan afectar los objetivos institucionales; con el fin de prevenir y mitigar los mismos a través de la implementación de mecanismos de control y prevención que promuevan la mejora continua, en todos los niveles de la entidad.

9.1.2.- METODOLOGÍA APLICADA

Se Adopta para la Administración del Riesgo en la ESE Hospital Departamental San Antonio de Padua de La Plata Huila, la metodología establecida por el Departamento Administrativo de la Función Pública - DAFP; la 'Guía de Administración del Riesgo y Diseño de controles de las entidades públicas, VERSIÓN 5 de diciembre de 2020 como la herramienta conceptual y metodológica para la valoración de los riesgos en la ESE, aplicando los siguientes pasos básicos.

9.1.2.1. 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 ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

En la etapa de identificación del riesgo dentro de la matriz de riesgo institucional debemos identificar el proceso macro de la institución, el proceso, identificar cada

riesgo con un número determinado, el tipo de riesgo a tratar y las características del mismo.

9.1.2.2 Tipo de Riesgo: Mediante el mapa de Riesgos institucional de ESE Hospital Departamental San Antonio de Padua de La Plata Huila, busca consolidad los Riesgos de Gestión, así mismo los riesgos de corrupción y seguridad digital que permitan además de identificar, analizar, controlar, monitorear hacer seguimiento los riesgos más probables de materializar.

9.1.2.2.1 -Riesgo de Salud: Se entiende por 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. El evento, es la ocurrencia de la enfermedad, traumatismos o su evolución negativa, desfavorable o complicaciones de esta; y las causas, son los diferentes factores asociados a los eventos.

9.1.2.2.2 -**Riesgo Operacional**: El Riesgo Operacional corresponde a la 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.

9.1.2.2.3 -**Riesgo Operacional**: (proceso) Son aquellos riesgos identificados en cada uno de los procesos de la entidad según el mapa de procesos.

Estos riesgos se deben alinear a los objetivos estratégicos o de procesos, identificando las vulnerabilidades y mayores impactos.

Estos riesgos pueden ser:
- Estratégicos
- Gerenciales
- Operativos
- Financieros
- Tecnológicos de cumplimiento
- De imagen o reputacional

A parte de los anteriores, se deben tener en cuenta los siguientes procesos relevantes para el cumplimiento de las funciones de la entidad, así estos sean tercerizados:

- Atención ambulatoria
- Atención hospitalaria y quirúrgica
- Atención de Urgencias
- Atención de Apoyo Diagnóstico y Terapéutico
- Referencia y Contrarreferencia
- Sistemas de información en salud o Calidad
- Gestión del talento humano
- Gestión Financiera
- Gestión administrativa y legal

9.1.2.2.4 -**Riesgos de Corrupción**: Según la Guía para la administración del riesgo en su versión 5 el riesgo de corrupción es la posibilidad de que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado. Es por ello que para que se identifique un riesgo de corrupción debe tener en cuenta las siguientes definiciones:

- Acción u omisión
- Uso de poder
- Desviar la gestión de lo público
- Beneficio privado

9.1.2.2.5 -Riesgos de Seguridad digital: Los riesgos a mencionar son los riesgos que identificados en la política de seguridad digital y de la seguridad y privacidad de la información. Para identificar los riesgos de seguridad digital se debe identificar el tipo de activo que se describen a continuación:

- Hardware
- Software
- Red
- Personal
- Lugar
- Organización

9.1.2.2.6 - Riesgo Actuarial: Se entiende por riesgo actuarial la posibilidad de incurrir en pérdidas económicas debido a no estimar adecuadamente el valor de los contratos según los diferentes tipos de contratos (cápita, evento, Grupo Relacionado de Diagnóstico, Pago Global Prospectivo entre otros) por venta de servicios, de tal manera que estos resulten insuficientes para cubrir las obligaciones futuras que se acordaron.

9.1.2.2.7 -Riesgo de Crédito: El Riesgo de Crédito corresponde a 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.

9.1.2.2.7-El Riesgo de Liquidez: corresponde a 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).

9.1.2.3- **Riesgo de mercado de capitales:** El Riesgo de Mercado de Capitales corresponde a 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, por causa de las variaciones en los parámetros del mercado tales como la tasa de interés, la tasa de cambio o cualquier otra variable de referencia que afecte los precios del mercado financiero y asimismo los estados financieros de la entidad.

9.1.2.4.-Análisis de objetivos estratégicos y de los procesos:
Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso. La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características. Para este punto se tendrá en cuenta la plataforma estratégica del Hospital San Antonio de Padua de La Plata determinada.

9.1.2.5.-Identificación de los puntos de riesgo:
Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo. Consultar Cadena Valor establecida en la figura 9 de la metodología Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 DAFP.

9.1.2.6.-Identificación de áreas de impacto:
El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

9.1.2.7.-Identificación de áreas de factores de riesgo: son las fuentes generadoras de riesgos. En la Tabla 1 Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 DAFP, encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

9.1.2.8.-Descripción del riesgo: la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad. Consultar Figura 10 Estructura propuesta para la redacción del riesgo Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 DAFP.

9.1.2.9.-Clasificación del riesgo: Permite agrupar los riesgos identificados.

9.1.2.10.-Clasificación del riesgo: 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. Es así como para la evaluación y medición de cada uno de los riesgos identificados, la entidad debe contar con información suficiente, completa y de calidad para generar los mejores pronósticos.

Riesgo residual: En la valoración del riesgo se debe establecer la probabilidad e impacto para establecer la zona de riesgo inicial o Riesgo inherente.

Probabilidad: Para determinar la probabilidad se debe tener en cuenta la posibilidad de que el riesgo ocurra y la exposición al riesgo de la entidad durante el periodo de un año, para definir los criterios de probabilidad se tiene en cuenta la gráfica tomada de la Guía de administración del riesgo y diseño de controles en su versión 5.

Impacto. En la determinación del nivel de impacto cuando este es económico y reputacional al mismo tiempo se toma el más alto de los dos para establecer la zona de riesgo.

Zona de riesgo. Una vez estipulada la probabilidad y el impacto del suceso que puede generar riesgo a la entidad se determina el nivel de riesgo inherente, un nivel de riesgo sin haber aplicado ninguna media para mitigarlo, la ubicación de estas dos posiciones puede determinar la zona de riesgo en el Mapa de calor.

9.1.2.11.-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 por 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 competente.

9.1.2.12.-Actividades de control: Es importante a la hora de establecer un control que debe contar con un responsable de su ejecución, cada causa de riesgo debe contar con al menos asignado un control, el control debe tener un soporte documental, se debe especificar como se ejecuta el control, y la periodicidad. Descripción del control: Para la descripción del riesgo se debe tener en cuenta que en la oración se debe identificar el responsable de ejecutar el control, la acción que determina lo que debe realizar en el control y detallar el control identificado. Ver gráfica 7. Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 DAFP.

Tipo de controles:

Se identifican tres tipos de controles (Preventivos, correctivos y detectivos) de acuerdo con el ciclo del proceso.

- **Control preventivo:** Se presenta en el ciclo de entrada (recursos que se requieren en el proceso), el control ataca la probabilidad de ocurrencia del riesgo.

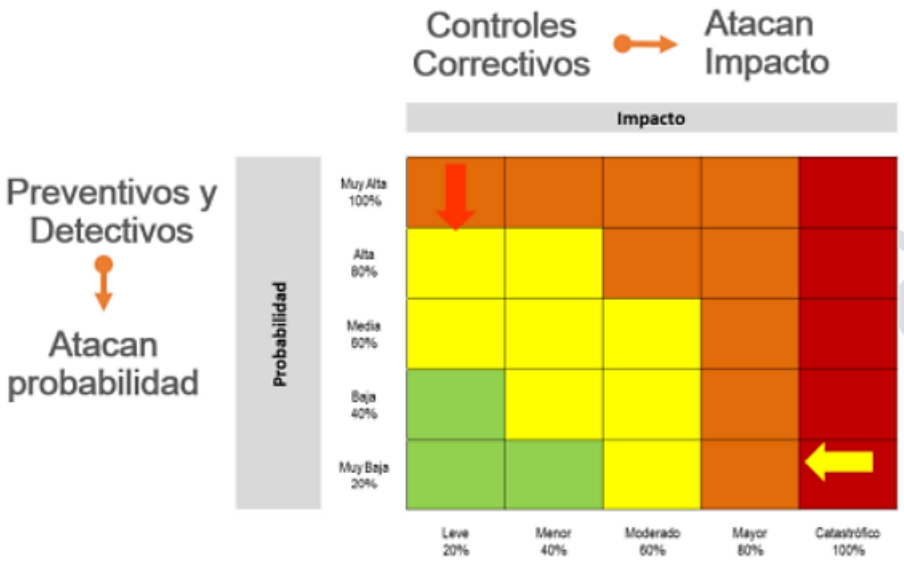
- **Control detectivo:** Hace referencia a aquellas actividades que permiten transformar las entradas de los productos o servicios, estos detectan cuando ocurre algo en el proceso lo devuelve a los controles preventivos, atacan la probabilidad de ocurrencia del riesgo.

- **Control correctivo:** Son aquellos controles que se encuentran en los procesos de salida del producto y/o servicio y atacan ante la materialización del riesgo. Asimismo, se debe identificar la forma como se ejecutan los controles:

- **Control manual:** Ejecutado por personas.

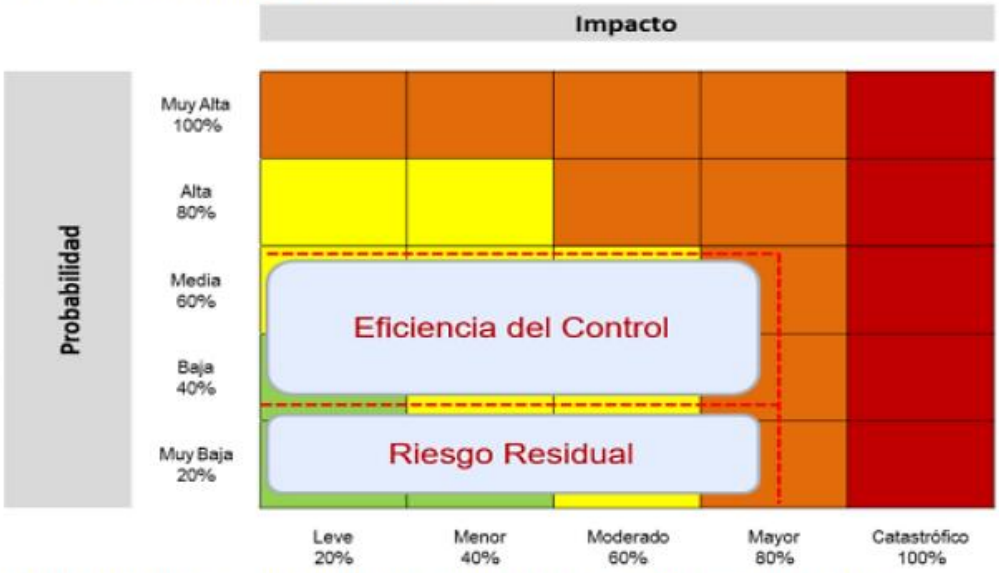
- **Control automático**: Ejecutado por un sistema.

Gráfica 8. Tipo de control- como actúa en el riesgo



FUENTE: Guía de Administración del Riesgo y diseño de controles versión 5. DAFP.

Gráfica 9. Eficiencia de los controles



FUENTE: Guía de Administración del Riesgo y diseño de controles versión 5. DAFP.

Tratamiento de riesgos

En esta etapa la primera línea de defensa teniendo en cuenta el nivel del riesgo inherente, que acción es la más adecuada para su tratamiento, estas acciones pueden ser:

Reducir el riesgo: Una vez analizado el nivel del riesgo y se puede considerar que es alto el tratamiento se puede hacer mediante el siguiente tratamiento: reducir compartir (tercerizar el proceso a través de pólizas o seguros) o reducir mitigar (implementación de acciones que mitiguen el nivel del riesgo).

Aceptar el riesgo: Una vez analizado el nivel del riesgo se puede determinar si se puede asumir conociendo los efectos de su posible materialización.

Evitar el riesgo: Una vez analizado el riesgo se puede considerar que este es demasiado alto, por lo cual se determina NO asumir la actividad.

9.1.2.13.-Nivel de aceptación del riesgo en la entidad: Acorde con los riesgos residuales aprobados por los líderes de procesos y socializados en el comité institucional de coordinación de control interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados. Los riesgos residuales de gestión y seguridad digital que se encuentren en zona de riesgo bajo, pueden estar dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida; para los riesgos asociados a posibles actos de corrupción no se puede incluir la aceptación del riesgo.

9.1.2.14.-Riesgos y nivel de confianza Organizar los riesgos de acuerdo con su categoría e identificar el nivel de confianza y aceptabilidad. Una vez analizada la información y sustraer la lista de actividades claves de éxito se asocian con los riesgos por categorías según el mapa de riesgos institucional, de este modo se puede identificar a quien corresponde la gestión del riesgo y su nivel de aceptación. La segunda línea de defensa efectúa el monitoreo y seguimiento a las actividades ejecutadas por la primera línea de defensa; el asesor de control interno establecerá el nivel de confianza, evaluando objetivamente las evidencias y su fuente de información (líneas de reporte).

En el seguimiento de las actividades claves de éxito y sus respectivos controles debe tener en cuenta los criterios de confiabilidad y la calificación debe ser razonable y objetiva, según las evidencias presentadas en la evaluación de confianza en función del aseguramiento. Ver tabla 3.

Tabla 3. Criterios de evaluación del nivel de confianza

2ª línea Identificada	CRITERIOS DE EVALUACION NIVEL DE CONFIANZA DE LA ACTIVIDAD DE CONTROL				TOTAL	NIVEL DE CONFIANZA
	Objetivo y Alcance (20%)	Prácticas y Metodologías (30%)	Ejecución por parte del responsable (30%)	Comunicación de Resultados (20%)		
Coordinación de Atención al Usuario	4 x 0,2= 0,8	3 x 0,3= 0,9	5 x 0,3= 1,5	1 x 0,2= 0,2	3,4	Media

Alto	Entre 4 y 5
Medio	Entre 3 y 3,9
Bajo	Entre 1 y 2,9

Fuente. Control interno (2019) esquema líneas de defensa. Departamento Administrativo de la Función Pública.

Se califica en la escala de 1 a 5 donde 1 NO cumple y 5 cumple plenamente con el criterio y se multiplica por el porcentaje % correspondiente a cada aspecto.

Proveedores de aseguramiento:

Utilizar el modelo de las líneas de defensa como proveedores del aseguramiento, así mismo incluir proveedores externos que brinden el servicio de auditoría puesto que estas aportan información vital en materia del riesgo de la entidad.

Actividades de aseguramiento externas son:
- Auditoría de habilitación
- Auditorías de Inspección Vigilancia y control
- Auditorías de las Empresas Aseguradoras de Planes y Beneficios.
- Auditorías de la SUPERSALUD
- Auditorías Contraloría del Departamento deL Huila
- Auditorías entes de control.
- Seguimiento a la gestión documental y archivo.
- Auditorías del Sistema de Seguridad y Salud en el Trabajo.
- Revisoría fiscal.

9.1.2.15.-Resultados del mapa de aseguramiento: Una vez completo el mapa de aseguramiento se debe establecer los niveles de confianza teniendo en cuenta la siguiente descripción (Ver tabla 4)

Tabla 4. Resultados del mapa de aseguramiento

Alta	La Oficina de Control Interno o quien haga sus veces confiará en los resultados de la actividad de control que realiza la 2ª línea de defensa y basado en sus informes, auditará la efectividad de dicha actividad de control, evitando evaluar los controles de la 1ª línea.
Media	La Oficina de Control Interno o quien haga sus veces deberá auditar y generar hallazgos y recomendaciones a actividad de control que realiza la 2ª línea de defensa, para su mejora y evaluará los aspectos que considere relevantes de la 1ª línea de defensa.
Baja	La Oficina de Control Interno o quien haga sus veces deberá auditar y generar hallazgos y recomendaciones a la actividad de control que realiza la 2ª línea de defensa, para su mejora y evaluará los controles de 1ª línea de defensa que corresponderían a la 2ª línea de defensa.

Fuente. Control interno (2019) esquema líneas de defensa. Departamento Administrativo de la Función Pública.

Ejemplo de mapeo general

Gráfica 10. Ejemplo de mapeo general

Aspectos Clave de Éxito	Coord. Atención al Usuario	Secretaria General	Director Técnico (DDO)	Oficial de Seguridad TIC	Oficina de Planeación	Oficina de Control Interno
Gestión de Recursos Físicos		Alto				
Asesoría Integral			Bajo			x
Planeación Estratégica					Alto	
Gestión TIC´S				Alto		
Servicio al Ciudadano	Medio					x

Fuente. Control interno (2019) esquema líneas de defensa. Departamento Administrativo de la Función Pública.

Cuando los niveles de confianza son bajos el asesor de control interno deberá desempeñar auditorías basadas en riesgos a la primera línea de defensa, entre tanto la entidad deberá realizar planes de mejora que mejoren la gestión del riesgo.

9.1.2.16.-Revisión y actualización del mapa: Realizar la revisión y actualización al mapa de aseguramiento deberá realizarse periódicamente y actualizarse al menos una vez al año, de acuerdo con la evaluación de nivel de confianza provista por los proveedores de los servicios de aseguramiento.

9.1.2.17.-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, las entidades deberán 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.

Seguimientos mapa de riesgos

Es importante determinar el seguimiento del riesgo de acuerdo con el riesgo residual.

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento - Controles
Riesgos de Gestión, y Seguridad digital	Baja	Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Moderada	Se realiza seguimiento a los controles con periodicidad TRIMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Alta	Se realiza seguimiento a los controles con periodicidad BIMESTRAL y se registran sus avances en el módulo de riesgos- SGI
	Extrema	Se realiza seguimiento a los controles con periodicidad MENSUAL y se registra en el módulo de riesgos – SGI.
Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento MENSUAL y se registra en el módulo de riesgos – SGI.	

Fuente: Oficina Asesora de Planeación

10. MARCO LEGAL

- 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.

- LEY 489 DE 1998. Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Artículos 27,28 y 29, Crea el Sistema de Control Interno con el objeto de integrar en forma armónica, dinámica, efectiva, flexible y suficiente el funcionamiento del Control Interno de las instituciones públicas.

- DECRETO 2145 DE 1999, por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del Orden Nacional y territorial y se dictan otras disposiciones. Modificado parcialmente por el Decreto 2593 de 2000. Define el S N C I las instancias de

articulación y sus competencias, la Unidad Básica del mismo su operatividad y el fortalecimiento del 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.

- DIRECTIVA PRESIDENCIAL 09 DE 1999, la cual define los lineamientos para la implementación de la política de lucha contra la corrupción por parte del Programa Presidencial de Lucha contra la Corrupción, creado mediante el Decreto 2405 de 1998, tiene como propósito central coordinar, tanto la implementación de las iniciativas gubernamentales para hacerle frente a este flagelo, como su articulación con aquellas que en el mismo sentido adelanten los organismos de control y la sociedad civil.

- DECRETO 1537 DE 2001, por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el Sistema de Control Interno, en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno. Establece en el artículo 4º que todas las entidades de la Administración Pública deben contar con una política de Administración de Riesgos tendiente a darle un manejo adecuado a los riesgos, con el fin de lograr de la manera más eficiente el cumplimiento de sus objetivos y estar preparados para enfrentar cualquier contingencia que se pueda presentar. Así mismo establece la Administración de Riesgos, como proceso permanente e interactivo entre la Administración y las Oficinas de Control Interno, con miras a establecer acciones efectivas, representadas en acciones de control, acordadas entre los responsables de las áreas o procesos y dichas oficinas.

- Decreto 4485 de 2009: Por el cual se adopta la actualización de la NTCGP 1000-2009. Numeral 4.1 Requisitos generales literal g) "establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder". Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.

- 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 No. 943 de 2014 " Por el cual se actualiza el Modelo Estándar de Control Interno" compilado en el Decreto 1083 de 2015, adopta el Modelo Estándar de Control Interno para el Estado Colombiano - MECI 2014, el cual establece el componente de Evaluación Independiente como un conjunto de elementos de control que garantizan el examen autónomo y objetivo del Sistema de Control Interno, la gestión y los resultados de la entidad pública por parte de la Oficina de Control Interno, Unidad de Auditoría Interna o quien haga sus veces.

• Decreto 648 de Abril 17 de 2017 "Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública". Establece cono función del Comité Institucional de Coordinación de Control Interno, como órgano asesor e instancia decisoria en los asuntos de control interno, hacer sugerencias y seguimiento a las recomendaciones basado en la priorización de los temas críticos según la gestión de riesgos de la Administración.

• 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.

• Guía para la Administración del Riesgo, DAFP, septiembre de 2020 versión 05.

11. MARCO SITUACIONAL

La Política de Administración del riesgo es la expresión del compromiso del equipo directivo de la Empresa Social del Estado el Hospital Departamental San Antonio de Padua frente a la identificación, tratamiento, control de los riesgos y oportunidades, que influencian los resultados de la gestión y permiten el cumplimiento de las metas establecidas en el Plan Estratégico de Gestión Institucional y en los Planes de Acción. Así mismo, la presente política involucra, mediante un ámbito estratégico y el modelo de las líneas de defensa, a todos los colaboradores de la entidad, soportándose en los mecanismos de comunicación disponibles, y cubriendo todas las responsabilidades institucionales, las de cada proceso y las propias de cada servidor, los niveles de aceptación de riesgo, los ciclos de establecimiento y seguimiento, los niveles de calificación, la identificación de riesgos de gestión, de corrupción y seguridad digital, entre otros, que hacen parte fundamental del lenguaje y herramientas disponibles para la administración de riesgos.

12. EVALUACIÓN

12.1 Acciones ante riesgos materializados

Ante la materialización de un riesgo se deberá medir el impacto y las consecuencias que puede ocasionar afectaciones a los objetivos de la Entidad, se revisarán y ajustarán los controles asociados determinando el grado de efectividad, eficiencia o eficacia, que garantice la mitigación de la ocurrencia. Para adelantar el análisis del riesgo y sus controles se deben considerar los siguientes aspectos:

• **Calificación del riesgo:** se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.

• **Bajo el criterio de probabilidad**: el riesgo se debe medir a partir de la cantidad de veces que se ejecuta cada una de sus acciones.

Se deberán tomar las medidas encaminadas a prevenir la ocurrencia como primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de ajustes en los controles y acciones emprendidas.

12.2 Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

• Informar a las autoridades de la ocurrencia del hecho de corrupción.
• Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
• Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
• Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

• Determinar la efectividad de los controles.
• Mejorar la valoración de los riesgos.
• Mejorar los controles.

• Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
• Determinar si se adelantaron acciones de monitoreo.
• Revisar las acciones del monitoreo.

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla "acciones de respuesta a riesgos".

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	Líder de Proceso	• Informar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y marcar en el SGI la alerta de posible materialización. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Identificar las acciones correctivas necesarias y documentarlas en el *plan de mejoramiento*.

Tipo de Riesgo	Responsable	Acción
		• Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	• Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Informar a discreción los posibles actos de corrupción al ente de control.
Riesgos de Gestión y Seguridad digital	Líder de Proceso	• Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo. • Proceder de manera inmediata a aplicar el *plan de contingencia o de tratamiento de incidentes de seguridad de la información* que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. • Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. • Dar cumplimiento al procedimiento plan de mejoramiento.

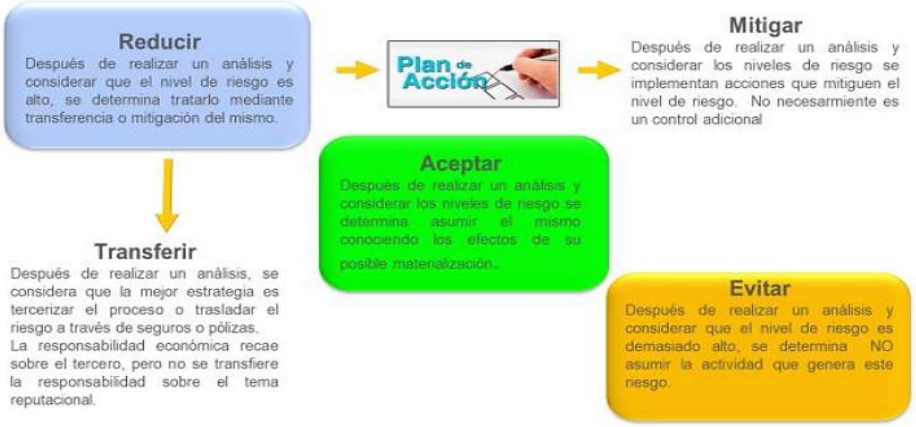
Tipo de Riesgo	Responsable	Acción
Riesgos de Gestión y Seguridad digital	Oficina de Control Interno	• Informar al líder del proceso sobre el hecho encontrado • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. • Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.
Riesgos de continuidad de negocio	Comité de crisis	• Activar el plan de continuidad de negocio

13. ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCIÓN

Estrategias para combatir el riesgo: decisión que se toma frente a un determinado nivel de riesgo, 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. En la figura 19 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos. Se plasma en un plan de acción que va inmerso en la matriz de riesgo.

Figura 19 Estrategias para combatir el riesgo



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

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique:

i) responsable,
ii) ii) fecha de implementación, y
iii) iii) fecha de seguimiento.

14. INDICADORES DE SEGUIMIENTO A LOS OBJETIVOS ESTABLECIDOS

Los indicadores de la política de gestión del riesgo miden la efectividad del proceso de gestión de riesgos para identificar, evaluar, mitigar y controlar riesgos

$$\frac{Número\ de\ Riesgos\ Materializados\ en\ la\ vigencia}{Total\ de\ Riesgos\ priorizados\ en\ la\ vigencia}$$

$$\frac{Número\ de\ planes\ de\ mejora\ priorizados}{Total\ de\ riesgos\ materializados\ en\ la\ vigencia}$$

15. REFERENCIAS BIBLIOGRÁFICAS

1.- Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 05 de octubre del 2020 Departamento Administrativo de la Función Pública. (DAFP)

2.- CIRCULAR EXTERNA 20211700000004-5 DE 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.

PLANIFICACIÓN DE LOS CAMBIOS

VERSIÓN	FECHA	COMENTARIO
01	20/03/2019	Proyección primera versión
02	25/01/2021	Segunda versión Res. 203 de 10 de agosto 2021
03	04/06/2021	Actualización tercera versión
04	06/08/2023	Actualización cuarta versión
05	20/10/2025	Actualización quinta versión, alineando Plataforma Estratégica, Plan Desarrollo Institucional 2024 - 2028 y lineamientos del instructivo de elaboración de documentos institucionales, codificación nueva según nuevo mapa de procesos institucional.

Elaborado por: **Nombre: ANA RUTH** **Cargo:** Asesor Control Interno	**Fecha:** 20/03/2019
Actualizado por: **Nombre**: **MARLENY RAMON OPRINA** **Cargo:** Control Interno **Firma:**	**Fecha:** 02/10/2025
Revisado por: **Nombre**: **NELSON FELIPE TIERRADENTRO Q** **Cargo:** Apoyo Profesional Planeacion Agremiado **Firma:**	**Fecha:** 07/10/2025
Aprobado por: **Nombre: JOSÉ ANTONIO MUÑOZ PAZ** **Cargo:** Gerente **Firma:**	**Fecha:** 20/10/2025