HOSPITAL LOCAL DE AGUACHICA

PLAN TRATAMIENTO DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Enero - 2025

INTRODUCCIÓN

La Empresa Social Del Estado Hospital Local De Aguachica, es una institución prestadora de servicios de salud de baja complejidad, de carácter público con el objetivo de prestar servicios de salud correspondientes al Primer nivel de atención, con carácter de servicio público a cargo del Estado y para ejecutar programas, proyectos y actividades de educación y promoción de la salud, prevención, tratamiento y rehabilitación de la enfermedad, ofreciendo a quien lo demande servicios de salud, satisfaciendo las necesidades de la población que atiende mediante el mejoramiento continuo de los servicios y la gestión administrativa, garantizando atención humanizada con calidad con la participación ciudadana conforme alo establecido por la Ley y sus reglamentos.

La Empresa Social Del Estado Hospital Local De Aguachica, define su política de Administración del Riesgo alineada con los objetivos estratégicos aplicable a todos los procesos, procedimientos, planes y metas fijados para la Sede principal, centros y puestos urbanos o rurales, para prevenir mitigar y controlar los potenciales riesgos que puedan afectar la gestión y el funcionamiento de la ESE, tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión (MIPG), según lo dispuesto en el Decreto 1499 de 2017, y en lo referente a las líneas de defensa, enfocado bajo los lineamientos de la Guía para la administración del riesgo versión 5 de 2020 y demás bibliografía dispuesta por el Departamento Administrativo de la Función Pública, relacionada con este tema, (DAFP), la cual articula los riesgos de gestión, corrupción y seguridad digital.

De manera individual se identifican, analizan, valoran y tratan los riesgos que pueden afectar la misión y el cumplimiento de los objetivos institucionales en el marco de los procesos, mediante:

- La identificación y documentación de riesgos de gestión (financieros, contractuales,jurídicos, entre otros), corrupción y de seguridad digital en los programas, proyectos, planes, metas y en general en los procedimientos de su competencia.
- El establecimiento de acciones de control para detectar, prevenir y corregir los riesgos identificados.

- La actuación correctiva y oportuna para mejorar el ejercicio de identificación y valoración del riesgo ante la materialización de los mismos,

Lo anterior con el fin de proteger los bienes y recursos institucionales, alcanzar mejores resultados y mejorar la prestación de los servicios habilitados conforme a la normatividad en salud vigente, que ofrece a los usuarios en aspectos fundamentales generación de valor público, eje fundamental del que hacer en la ESE Hospital Local De Aguachica, En este marco se define esta metodología y se determinan las acciones para prevenir, reducir y mitigar el riesgo al igual que se establecen los planes de contingencia ante la materialización del riesgo.

MARCO NORMATIVO

El marco regulatorio respecto de la Planeación, ejecución y control del riesgo en vista de la necesidad de establecer estrategias y políticas que permitan la ejecución de las acciones hacia la evolución de las organizaciones de manera controlada; hace necesario indicar la siguiente necesidad.

- Constitución Política de Colombia de 1991.
- **Ley 134 de 1994** por la cual se dictan normas sobre mecanismos de participación ciudadana.
- **Ley 720 de 2001** por medio de la cual se reconoce, promueve y regula la acción voluntaria de los ciudadanos colombianos.
- **Ley 1437 de 2011** por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo). Y derechos constitucionales a la participación contenidos en los Artículos 2, 3 y 103, derecho a la participación, a la información Artículos 20, 23 y 74 y a la participación en el control del poder político Artículo 40, así como del derecho a vigilar la gestión pública Artículo 270.
- **Ley 019 de 2012** Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **Ley 1474 de 2011** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, artículo 73.

- **Ley 1712 de 2014** se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1757 de 2015** se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática.
- **Decreto 1757 de 1994** por el cual se organizan y establecen las modalidades y formas de participación social en la prestación de servicios de salud, conforme a lo dispuesto en el numeral 11 del artículo 40 del Decreto Ley 1298 de 1994.
- **Decreto 2693 de 2012** Establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
- **Decreto 103 de 2015** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y sedictan otras disposiciones.
- **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.
- **Decreto 767 de 2022** Por el cual se establecen los lineamientos generales de la Políticade Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Resolución 1519 de 2020** Por la cual se definen los estándares y directrices para publicar la información señalada en el **Conpes 3649 de 2010** Política Nacional de Servicio al Ciudadano.
- **Conpes 3650 de 2010** Importancia Estratégica de la Estrategia de Gobierno en Línea.
- **Conpes 3654 de 2010** Política de rendición de cuentas de la Rama Ejecutiva a los ciudadanos.
- Estrategias para la Construcción del Plan Anticorrupción y de atención al ciudadano.
- Guías para la administración del riesgo y el diseño de controles en entidades públicas - Versión 4 y 5, expedidas por el Departamento Administrativo de la Función Pública.

TÉRMINOS Y DEFINICIONES

- **Activo**: En el contexto de seguridad digital 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 una organización**.**
- **Apetito al Riesgo**: Es el nivel de riesgo que la La Empresa Social Del Estado Hospital Local De Aguachica, puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de los Procesos Directivos y de Mejora. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la ESE, deba o desee gestionar.
- **Áreas de Impacto**: Consecuencia económica o reputacional a la cual se ve expuesta la ESE en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.
- **Cadena de valor**: Es la interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios (procesos misionales).
- **Capacidad de Riesgo**: Es el máximo valor del nivel de riesgo que la ESE, puede soportar y a partir del cual se considera por los Procesos Directivos y de Mejora que nosería posible el logro de sus objetivos.
- **Caracterización de proceso**: Estructura que permite identificar los rasgos distintivos de los procesos. Establece su objetivo, la relación con los demás procesos, los insumos, los activos, su transformación a través de las actividades que desarrolla y las salidas del proceso, se identifican los proveedores y clientes o usuarios, que pueden ser internos o externos.
- **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 noconstituyen 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 puedepresentar el riesgo.
- **CICCI:** Comité Institucional de Coordinación de Control Interno**.**

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la Institución, sus grupos de valor y demás partes interesadas.
- **Control**: Medida que permite reducir o mitigar un riesgo. Los responsables de implementar y monitorear los controles son los líderes de proceso.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Estrategia para Combatir el Riesgo** (Tratamiento): Decisión que se toma frente a un determinado nivel de riesgo. Se analiza frente al riesgo residual, esto para procesos enfuncionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente y puede ser:
    - **Reducir:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.
    - **Transferir o Trasladar**: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
    - **Mitigar**: Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo. No necesariamente es un control adicional.
    - **Aceptar:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.
    - **Evitar:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.
- **Evento**: Riesgo materializado. Los eventos de riesgo son aquellos incidentes que generan o podrían generar pérdidas a la ESE.
- **Factores de Riesgo**: Son las fuentes generadoras de riesgos. Pueden ser: Procesos, Talento Humano, Recursos Científicos y Tecnológicos, Infraestructura y Eventos externos (Terceros).

- **Impacto**: Las consecuencias que puede ocasionar la materialización del riesgo.
- **Indicadores Clave de Riesgo** (Un indicador de riesgos clave, también conocido como KRI de sus siglas en inglés Key Risk Indicators): Es una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos.
- **Integridad**: Propiedad de exactitud y completitud.
- **Gestión del Riesgo**: Proceso efectuado por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. La gestión de riesgos no es estática, se integra en el desarrollo de la estrategia, la formulación de los objetivos de la ESE, a través de la toma de decisiones cotidiana.
- **Mapa de procesos:** Es la representación gráfica de los procesos estratégicos, misionales, de apoyo, de evaluación y sus interacciones. Constituye la razón de ser de la entidad, sintetiza los principales propósitos estratégicos y los valores esenciales que deben ser conocidos, comprendidos y compartidos por todas las personas que hacen parte de la entidad.
- **Mapa de Riesgos**: Documento con la información resultante de la gestión del riesgo, administrado por la segunda línea de defensa.
- **Modelo de operación por procesos:** El modelo de operación por procesos es el estándar organizacional que soporta la operación de la entidad pública, integrando las competencias constitucionales y legales que la rigen con el conjunto de planes y programas necesarios para el cumplimiento de su misión, visión y objetivos institucionales. Pretende determinar la mejor y más eficiente forma de ejecutar las operaciones de la entidad.
- **Nivel de Riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo es Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
- **OCI:** Oficina de Control interno

- **Objetivo del proceso:** Es el resultado que se espera lograr para cumplir la misión y visión; determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto, debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción.
- **Objetivos estratégicos:** Identifican la finalidad hacia la cual deben dirigirse los recursosy esfuerzos para dar cumplimiento al mandato legal aplicable a cada entidad; estos objetivos institucionales se materializan a través de la ejecución de la planeación anualde cada entidad.
- **Plan Anticorrupción y de Atención al Ciudadano**: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las Instituciones y entidades del orden nacional, departamental y municipal.
- **Planeación institucional:** Las estrategias de la entidad generalmente se definen por parte de la alta dirección y obedecen a la razón de ser que desarrolla la misma, a los planes sectoriales, las políticas específicas que define el Gobierno nacional, departamental o municipal enmarcadas dentro del Plan Nacional de Desarrollo. En este contexto la entidad define su planeación institucional. **L**a planeación institucional hace uso de los procesos estratégicos, misionales, de apoyoy evaluación para materializarla o ejecutarla; por lo tanto, la administración del riesgo no puede verse de forma aislada.
- **Política de Administración del Riesgo**: Declaración de la dirección y las intenciones generales respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.
- **Política de Prevención del Daño Antijurídico**: Solución de los problemas administrativos que generan litigiosidad e implica el uso de recursos públicos para reducir los eventos generadores del daño antijurídico.
- **Probabilidad**: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de1 año.
- **Puntos de Riesgo:** Son actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios que pueden ocurrir eventos de riesgo

operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

- **Riesgo**: Efecto que se causa sobre los objetivos de las ESE, debido a eventos potenciales, que hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de Corrupción**: Posibilidad que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **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 eventoy sus consecuencias. (ISO/IEC 27000).
- **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, dentrode unas escalas de severidad.
- **Riesgo Residual**: Nivel de Riesgo que permanece luego de tomar medidas preventivasy/o correctivas para el tratamiento del riesgo.
- **Severidad**: Nivel de un riesgo, dado por una probabilidad y un impacto. En cada nivel se define el tratamiento y los niveles de responsabilidad.
- **TIC**: Tecnologías de la Información y las Comunicaciones.
- **Tolerancia del Riesgo**: Es el valor de la máxima desviación admisible del nivel de riesgocon respecto al valor del apetito de riesgo determinado por la ESE.
- **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede serexplotada por una o más amenazas.

OBJETIVOS DEL PLAN

El objetivo principal de este plan busca establecer la clara metodología para hacer una administración a la medida de los potenciales riesgos por medio de la identificación, manejo y seguimiento de los mismos.

Como objetivos específicos se formularon:

- Acceder a información consistente, confiable y real para realizar una correcta toma de decisiones.
- Hacer partícipes y responsables a los funcionarios de la entidad de la magnitud y relevancia de mantener información confiable.
- Generar un ambiente de autogestión con relación a la integridad y seguridad de la información.

ROLES Y RESPONSABILIDADES

Anualmente los líderes de proceso con sus respectivos equipos de trabajo, identifican y/o validan los riesgos de gestión, corrupción y seguridad digital asociados al logro de los objetivos de los procesos, como un ejercicio que se desarrolla de manera anual. Los riesgos que se identifican son abordados conforme a lo dispuesto en este Lineamento y en la medida en que se controlan se espera vayan desapareciendo del Mapa o Matriz de Riesgo como medio para propiciar el logro de los objetivos del control a los mismos.

Las actividades de control se orientan a prevenir y detectar la materialización de éstos, porconsiguiente, su efectividad depende de qué tanto se están logrando los objetivos estratégicos y de proceso, correspondiendo a la primera línea de defensa elestablecimiento de actividades de control, de acuerdo con la cultura del autocontrol, los líderes de los procesos junto con su equipo de trabajo, realizarán monitoreo y evaluación de manera permanente, con el fin de analizar el estado de sus procesos frente a los controles establecidos. Los resultados de este monitoreo, se evidenciará en los comités de alto nivel como el Comité Coordinador de Control Interno, en adelante el CICCI o el comité competente de conocer el tema, de acuerdo al proceso que aplique.

El Gerente y el Subgerente, en conjunto con el equipo de trabajo, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, adelantar el monitoreo, ya que su importancia radica en la necesidad de llevar a cabo un seguimiento constante ala gestión del riesgo y a la efectividad de los controles establecidos.

SEGUIMIENTO A LAS ACCIONES DE CONTROL DEL RIESGO EN CASA PROCESO

Según la periodicidad definida para cada riesgo, se verificará el cumplimiento de las acciones, analizando los resultados dejando evidencia del avance, así como las observaciones frente a las desviaciones para establecer las acciones inmediatas para su control preventivo, detectivo o correctivo.

- Se documentarán las acciones de corrección o prevención en el plan de mejoramiento.
- Se actualizará el Mapa de Riesgo anualmente teniendo en cuenta el resultado delas evaluaciones de las acciones y/o ubicación del riesgo.

Para el **Tratamiento del Riesgo,** se puede identificar entre los siguientes criterios teniendo en cuenta su valoración**:**

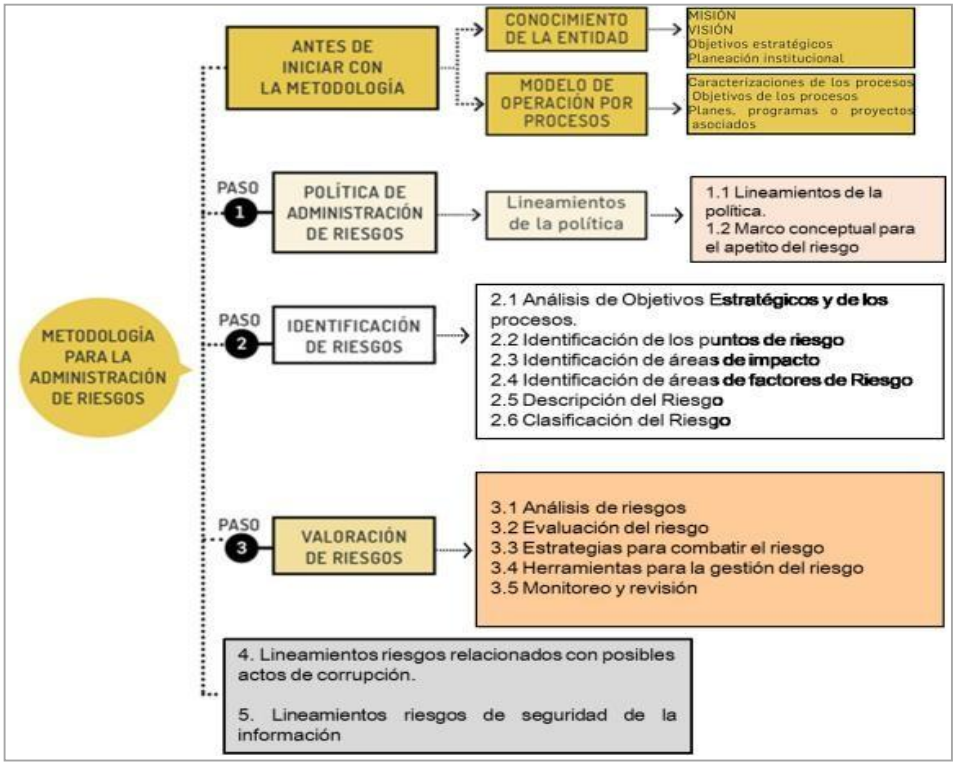
- **Aceptar el riesgo:** No se adopta ninguna medida que afecte la Probabilidad o el impacto del riesgo (Ningún Riesgo de Corrupción podrá ser aceptado).
- **Reducir el riesgo**: Se adoptan medidas para reducir la Probabilidad o el Impacto del riesgo, o ambos, por lo general conlleva a la implementación de Controles. El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo. Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.
- **Evitar el riesgo**: Se adoptan las actividades que dan ligar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo.
- Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

- **Compartir el riesgo**: Se reduce la Probabilidad o el Impacto del riesgo, o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de Corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

METODOLOGÍA

La Empresa Social del Estado Hospital Local de Aguachica, aplicará la metodología establecida por el Departamento Administrativo dela Función Pública, descrita en la Guía para la administración de riesgos y el diseño de controles en entidades públicas.

Figura 1: Pasos básicos para la administración del Riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública

La metodología para la gestión de la Política de Administración del riesgo, se desarrolla a través de tres (3) pasos básicos:

- **Paso 1. Política de Administración del riesgo**
- **Paso 2. Identificación de riesgos**
- **Paso 3. Valoración de riesgo**

PASO No. 1: POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Alta Dirección, se compromete a administrar adecuadamente los riesgos a los que se encuentra expuesta y que pueden interferir en el logro de la misión, los objetivos institucionales y su imagen ante grupos de valor y demás partes interesadas; lo anterior, atendiendo los lineamientos definidos a través de la metodología establecida para su identificación, valoración, control y monitoreo; determinando a su vez, las acciones necesarias de control detectivas y preventivas de manera oportuna, para evitar su materialización y así mismo, mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables.

La administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión, además del conocimiento desde el punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada.

La Empresa Social Del Estado Hospital Local De Aguachica, se compromete a prevenir los potenciales riesgos que afectan la gestión, fundamentada en la aplicación de controles enmarcados en el modelo integrado de planeación y gestión, la guía de administración del riesgo y el diseño de controles**.**

Atendiendo esta metodología para la administración del riesgo, a continuación, se documentan los aspectos institucionales estratégico (misión, visión, objetivos institucionales y planeación institucional); por otra parte, es esencial operar por procesos, con el fin de contemplar la información asociada a los mismos.

MISION

Prestamos servicios de atención primaria en salud con enfoque integral, orientado a la seguridad del paciente, la atención humanizada y la satisfacción de los usuarios y sus familias. Contamos con tecnología avanzada en cada uno de nuestros procesos, con talento humano idóneo, altamente calificado, autónomo, responsable, estratégico, competitivo y motivado a brindar un servicio con calidad.

VISION

El Hospital Local de Aguachica E.S.E, será para el 2030, una empresa líder en la prestación Primaria en Salud con un modelo de atención integral en salud humanizada y de alta calidad, con acciones asociadas en la promoción y mantenimiento de la salud en cada curso de vida, en la atención integral materno perinatal, educación e investigación docencia servicio y la gestión de riesgo en salud de forma oportuna, accesible, garantizando la seguridad y satisfacción en los usuarios y sus familias.

- **Objetivos Institucionales**

Prestar servicios de salud, integrales, con atención humanizada, centrada en el usuario y su familia con énfasis en la promoción y mantenimiento de la salud y mejoramiento de niveles de salud; integrando el direccionamiento estratégico a la gestión por procesos y a la gestión del talento humano, mediante el mejoramiento continuo de los atributos de calidad y el fortalecimiento de la satisfacción de las necesidades y expectativas de las personas.

Gestionar el desarrollo Integral del Talento Humano, mediante el fomento de la cultura y el clima organizacional, el fortalecimiento de las competencias y el bienestar laboral.

- **Objetivo Estratégico social**

Orientar el desarrollo de la Empresa Social del Estado El Hospital Local de Aguachica, hacia el mejoramiento de la Gestión Organizacional a través de la implementación del Sistema Integral de Garantía de Calidad, encaminado hacia resultados que evidencien el progreso en la calidad en la Prestación de Servicios de Salud Seguros, con Calidez, Sistema Integral de Gestión y Control, Desarrollo Organizacional, la Sostenibilidad Financiera y la Responsabilidad Social y Ambiental.

- **Objetivos estratégicos en la Prestación de servicios y humanización**

Prestar servicios de salud, integrales, con atención humanizada, centrada en el usuario y su familia con énfasis en la promoción y mantenimiento de la salud y mejoramiento de niveles de salud, integrando el direccionamiento estratégico a la gestión por procesos y a la gestión del talento humano, mediante el mejoramiento continuo de los atributos de calidad y el fortalecimiento de la satisfacción de las necesidades y expectativas de las personas.

Gestionar el desarrollo Integral del Talento Humano, mediante el fomento de la cultura y el clima organizacional, el fortalecimiento de las competencias y el bienestar laboral.

- **Objetivos estratégicos Sistema Gestión de la Calidad**

Además de ejecutar procesos asistenciales y de apoyo bajo un marco general del cumplimento de las normas y de garantía de la calidad, se quiere establecer una línea clarade atención centrada en la seguridad del paciente, que permita además de mejorar su condición de salud y vida, fidelizarlo como usuario en la Institución.

- **Objetivos estratégicos Operatividad Financiera y Administrativa**

Garantizar la auto sostenibilidad financiera y rentabilidad social de la E.S.E., mediante la optimización de los recursos humanos, físicos, tecnológicos y financieros, y la evaluación permanente del riesgo fiscal y financiero, que faciliten el buen funcionamiento de los procesos organizacionales.

Gestionar a través de recursos propios y proyectos de inversión contar con la infraestructura hospitalaria adecuada acorde a los lineamientos y requisitos legales del sistema obligatorio de garantía de la calidad en salud; siempre en pro del usuario de La Empresa Social Del Estado Hospital Local De Aguachica.

- **Objetivos estratégicos Sistema de información**

En el mediano plazo contar con un sistema de información integral que articule en tiempo real y de manera eficiente la información generada tanto del área asistencial

como del área administrativa y que a su vez de respuesta oportuna a las necesidades de nuestros clientesy actores del sistema.

Institucionalidad desde el MIPG

Figura 2. Esquema general del modelo integrado de planeación y gestión (MIPG)

El modelo integrado de planeación y gestión (MIPG) es un marco de referencia para dirigir,planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, este modelo tiene el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad ycalidad en el servicio.

El MIPG opera a través de 7 dimensiones (talento humano, direccionamiento estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y,finalmente, control interno) que agrupan las políticas de gestión y desempeño institucional y que, implementadas de manera articulada e interrelacionada, permitirán que el modelo funcione y opere adecuadamente, tal como se observa en la siguiente figura.

Por otro lado, para aprender, determina las siguientes responsabilidades por otro lado para aprender, determina las siguientes responsabilidades en relación con las líneas de defensa establecidas en el Modelo Integrado de Planeación y gestión y gestión – MPG, conforme a la imagen anterior.

CADENA DE VALOR

Figura 3: Cadena de valor Público

Es importante definir la cadena de valor en sí misma, este modelo propuesto y difundido por Michael Porter, constituye para la Empresa Social Del Estado Hospital Local De Aguachica, uno de los instrumentos más ricos y populares para el análisis interno. El concepto de cadena de valor se refiere a la desagregación Institucional en las actividades básicas que es preciso llevar a cabo para generar un servicio o bien, es el conjunto de actividades que se desarrollan sucesivamente para generar valor a la gestión y generar resultados que impacten en la calidad de vida de los grupos de valor, por tanto; la importancia de controlar sus riesgos, tal como se observa en la imagen.

LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La gestión integral del riesgo es un proceso que permite identificar y administrar los eventos potenciales que pueden afectar el logro de la estrategia, la ejecución de acciones, actividades, procedimientos y procesos en general. El ciclo de la gestión integral de riesgos comprende acciones de identificación, medición, control, monitoreo, comunicación y divulgación de los riesgos, los cuales se deben gestionar garantizando lo siguiente:

- La adopción de una metodología para la gestión del riesgo.
- La identificación de riesgos relevantes, atendiendo su posible incidencia sobre losobjetivos estratégicos, sostenibilidad y la continuidad de la gestión.

Esta política para la gestión del riesgo se encuentra alineada con los objetivos estratégicos de La Empresa Social Del Estado Hospital Local De Aguachica aplicable a todos los procesos, procedimientos, planes y metas para prevenir mitigar y controlar los riesgos.

En cuanto al riesgo de corrupción, se puede decir que es una actividad difícil de detectar. Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa aquí descritas. **Reporte de la gestión del riesgo de corrupción** De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento.

- **Seguimiento de riesgos de corrupción**

Seguimiento: La Oficina Asesora de Control Interno, debe adelantar seguimiento a la gestión de los riesgos institucionales. En este sentido, es necesario que en sus procesos de auditoría interna se analicen las causas, los riesgos, la efectividad de los controles incorporados en el mapa de riesgos institucional y el cumplimiento de las acciones planteadas.

Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro delos diez (10) primeros días del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro delos diez (10) primeros días del mes de enero de la siguiente vigencia a la ejecución del plan.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. (Ver matriz de seguimiento a los riesgos de corrupción) En especial deberá adelantar las siguientes actividades:

- **Verificar** la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad. * Seguimiento a la gestión del riesgo.
- **Revisión** de los riesgos y su evolución.
- **Asegurar** que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada. 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.

OBJETIVO DE LA POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO

Aportar al control de los procesos en el marco del cumplimiento de la misión y al logro de los objetivos institucionales, mediante la identificación de los Riesgos, la asignación de responsables de la Gestión, funcionamiento y prestación de los servicios de La Empresa Social Del Estado Hospital Local De Aguachica, conforme a lo establecido en la Dimensión 7 del MIPG (Líneas de Defensa) y lineamientos para el tratamiento, manejo y seguimiento a los riesgos de gestión, corrupción, y seguridad digital.

ALCANCE DE LA POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO

La Política Institucional para la Administración del Riesgo aplica a todos los procesos del modelo de operación por procesos, a los planes institucionales y programas, a los procesos y acciones a cargo de los servidores públicos y contratistas de prestación de servicios directos e indirectos de La Empresa Social Del Estado Hospital Local De Aguachica, en el cumplimiento de sus funciones, obligaciones y actividades, tanto en la Sede Principal como en sus Centro y Puestos Urbanos o Rurales.

La Política de administración del Riesgo involucra el contexto, identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y análisis.

MARCO CONCEPTUAL PARA EL APETITO DEL RIESGO

Para determinar la capacidad de riesgo en La Empresa Social Del Estado Hospital Local De Aguachica, se considera el apetito del riesgo, a fin de contar con mayores elementos de juicio para su análisis:

Para determinar la capacidad de riesgo se debe aplicar los valores de probabilidad e impacto, con la participación y aprobación de la dirección, de acuerdo con las competencias del CICCI, teniendo en cuenta los siguientes valores:

- **Valor máximo** de la escala que resulta de combinar la probabilidad y el impacto.
- **Valor máximo** que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable, puede ser resistido antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad de riesgo”.

- De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo que se esté analizando, es el máximo valor del nivel de riesgo que se puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos.

DETERMINACIÓN DEL APETITO DE RIESGO

Luego de determinada la capacidad de riesgo por parte de la alta dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión.

Este valor se denomina “apetito de riesgo”, dado que equivale al nivel de riesgo que La Empresa Social Del Estado Hospital Local De Aguachica, puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que se debe o se desea gestionar.

TOLERANCIA DE RIESGO

La tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado.

Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la alta dirección y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa institucionalmente, y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

ASEGURAMIENTODEL AMBIENTE DE CONTROL DEL RIESGO DESDE EL MIPG

En cumplimiento del artículo 73 de la Ley 1474 de 2011, relacionado con la prevención de los riesgos de corrupción, la Identificación del riesgo también se hará a partir del desarrollo de las otras dimensiones tales como Gestión del Talento Humano, Direccionamiento Estratégico y Planeación, Gestión con Valores para Resultados, etcétera, de conformidad con los siguientes conceptos aplicables a La Empresa Social Del Estado Hospital Local De Aguachica.

IDENTIFICACIÓN DEL RIESGO

La Empresa Social Del Estado Hospital Local De Aguachica, la identificación de riesgos tiene como objetivo establecer cuáles son los riesgos asociados a su operación, lo que permite determinar cuáles están identificados, controlados y cuáles no. Para ello se debe tener en cuenta el contexto estratégico en el que se opera, objetivos estratégicos y de procesos, puntos de riesgo operativo, áreas de impacto y factores de riesgo.

El objetivo de la identificación del riesgo es conocer los sucesos que se pueden producir Institucionalmente, y las consecuencias que puedan tener sobre sus objetivos, por tanto, en cada proceso se debe reconocer el concepto de “administración del riesgo”, la política y la metodología definida, los involucrados y el entorno del proceso, tal como a continuación se establece.

ANÁLISIS OBJETIVOS ESTRATÉGICO

La Empresa Social Del Estado Hospital Local De Aguachica, como prestadora de servicios de salud desde lo dispuesto en el Sistema obligatorio de Garantía de la Calidad articulado con MIPG, cuenta con el programa de seguridad del paciente, ya que es éste la razón de ser, los procesos, protocolos, guías y demás documentos estandarizados obedecen a este sistema con enfoque a habilitación y acreditación, sistema de información y auditoría para el mejoramiento de la calidad, en cuanto a la gestión administrativa y su funcionamiento se cuenta con el Manual de Procesos y procedimientos documentados y está planeado su actualización para la próxima vigencia, enfocado a los objetivos, alcance (caracterización), para lo cual ya se adelantó la respectiva socialización y asistencia técnica a los líderes de procesos y referentes de programas, para lo cual se alineará con la misión y visión, para asegurar que contribuya a los objetivos estratégicos.

El grupo de trabajo profesional, es el responsable de la identificación, monitoreo, reporte y socialización del riesgo asociados a sus procesos, la consecuencia económica o reputacional a la cual se expone en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional, para su manejo se adelantan los respectivos planes de mejora.

La identificación y calificación de las acciones de control para los riesgos conforme a los requerimientos de la metodología, se incorporan al Mapa o Matriz de Riesgo por procesos con toda la información recopilada, conforme a lo establecido en este lineamiento, para su gestión y tratamiento, así como los factores o fuentes generadoras del riesgo.

Los siguientes son los aspectos que se tienen en cuenta en atención a la implementación de esta metodología.

- Los Insumos, corresponden a los recursos financieros, humanos y materiales empleados para la prestación de los Servicios habilitados de La Empresa Social Del Estado Hospital Local De Aguachica Procesos: Son las actividades realizadas para elaborar o transformar en un resultado intermedio o final.
- Productos: Servicios prestados demandados por la población para satisfacer las necesidades y expectativas o responder a las causas específicas de un problema.
- Resultados o efectos: Cambios en el comportamiento o en el estado de los beneficiarios como consecuencia de recibir los productos, bienes o servicios.
- Impacto: Cambios en las condiciones de vida en la población objetivo. Mayor valor público en términos de bienestar prosperidad general y calidad de vida de la población.
- 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.

IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Son las fuentes generadoras de riesgos y pueden estar relacionadas con el Proceso, Talento humano, Tecnología, Infraestructura, Dotación, evento adverso o incidente.

FACTOR	DEFINICIÓN	DESCRIPCIÓN
PROCESOS	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
TALENTO HUMANO	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Pérdida activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
TECNOLOGÍA	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
INFRAESTRUCTURA	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
EVENTO EXTERNO	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Las causas por las cuales se puede generar el riesgo y tipos de causa corresponden a:

- Causa inmediata: Circunstancia o situación evidente sobre la cual se presenta el riesgo, no constituye la causa principal o base para que se presente el riesgo.
- Causa raíz: Es la causa principal o básica, corresponde a las razones por la cual se puede presentar el riesgo, es la base para la definición de

controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o subcausas que pueden ser analizadas.

CLASIFICACIÓN DEL RIESGO

Permite agrupar los factores de riesgo identificados, se clasifica cada uno de los riesgosen las siguientes categorías.

Tabla 3: Clasificación del riesgo

CLASIFICACIÓN		FACTORES DE RIESGO
EJECUCIÓN Y ADMINISTRACIÓNDE PROCESOS	Pérdidas derivadas de errores en la ejecución y administración de procesos.	**PROCESOS**
FRAUDE EXTERNO	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	**EVENTO EXTERNO**
FRAUDE INTERNO	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas en las cuales está involucrado por lo menos 1 participante interno, y son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.	**TALENTO HUMANO**
FALLAS TECNOLÓGICAS	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	**TECNOLOGÍA**
RELACIONESLABORALES	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.	**PUEDE ASOCIARSE A VARIOS FACTORES**

USUARIOS, PRODUCTOS Y PRÁCTICAS	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.	
DAÑOS A ACTIVOS FIJOS/EVENTOS EXTERNOS	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.	**INFRAESTRUCTURA EVENTO EXTERNO**

DESCRIPCIÓN DEL RIESGO

Para la redacción de los riesgos de gestión, corrupción y seguridad de la información, se adoptan los esquemas propuestos por 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, así:

RIESGO DE CORRUPCIÓN

Es necesario que, en la descripción del riesgo concurran los componentes de su definición, considerando además la probabilidad de fraude y corrupción:

Ejemplo: Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

Los riesgos de corrupción se establecen sobre procesos.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la guía de lineamientos descripción riesgo de corrupción.

RIESGOS DE SEGURIDAD DIGITAL O DE LA INFORMACIÓN

Los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos se basa en la afectación de tres criterios en un activo, y por lo tanto su redacción corresponderá a:

Ejemplo:

Pérdida de integridad
Pérdida de disponibilidad
Pérdida de confidencialidad

Identifique los activos de información (solo aplican para riesgos de seguridad de la información).

Un activo es cualquier elemento que tenga valor para la entidad, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: aplicaciones de la organización, servicios web – redes, información física o digital, Tecnologías de información TI -Tecnologías de operación TO que se utilizan para la gestión y funcionamiento en el entorno digital.

De igual manera, permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

Los pasos a seguir para identificar los activos de información, corresponden a los siguientes pasos:

Paso No. 1: Listar los activos por cada proceso
Paso No. 2 Identificar el dueño de los activos
Paso No. 3 Clasificar los activos
Paso No. 4 Clasificar la información
Paso No. 5 Determinar la criticidad del activo
Paso No 6 Identificar si existe infraestructura crítica cibernética

Para la identificación y valoración de activos se debe sensibilizar al personal de cada proceso donde aplique la gestión del riesgo de seguridad de la información para que sea realizada por la **Primera Línea de defensa – líderes de proceso**, con la orientación del Profesional universitario de sistemas y su Personal de Apoyo en su calidad de responsables de la seguridad digital y seguridad de la información de La Empresa Social Del Estado Hospital Local De Aguachica.

Para la Sensibilización sobre este tema el Departamento Administrativo de la Función Pública, ha recomendado a todas las entidades la sección 3.1.6 del “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas” del Ministerio de Tecnologías de la Información y las Comunicaciones.

En cuanto a los demás riesgos aplicables a la ESE, se considerará lo siguiente:

Los Riesgos relacionados con la seguridad y salud en el trabajo, se intervendrán de acuerdo con lo establecido en el Plan de Trabajo Anual en Seguridad y Salud en el Trabajo; (Decreto 612 de 2018), para la vigencia y normatividad aplicable.

Para la gestión de los riesgos de contratación, se tendrá en cuenta el Documento Conpes 3714 de 2011 y los lineamientos de Colombia Compra Eficiente.

Los riesgos defensa jurídica, Serán administrados bajo la metodología de prevención del daño antijurídico de la Agencia Nacional de Defensa Jurídica del Estado donde el Comité de Conciliación anualmente aprobará la Política de Prevención del Daño Antijurídico, el representante legal de la ESE, expedirá el documento mediante el cual se adopte la Política de Prevención del Daño Antijurídico e impartirá las directrices para su divulgación y el Secretario Técnico del Comité de Conciliación junto con su grupo de apoyo, brindará la información y prestará la colaboración necesaria para realizar el respectivo seguimiento y evaluación.

PASO 3. VALORACIÓN DEL RIESGO

La valoración permite establecer la probabilidad de ocurrencia del riesgo y el nivel de impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE), y a través de la evaluación del riesgo se busca confrontar los resultados del análisis del riesgo inicial, frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL), para establecer el movimiento en la matriz de calor y determinar el plan de acción (opción de tratamiento) acorde con las estrategias para combatir el riesgo.

PROBABILIDAD

Para estimar el Nivel de riesgo inicial los valores determinados para la probabilidad y el impacto o consecuencia se cruzan conforme a lo establecido en la Matriz de calificación del riesgo, Niveles de Aceptación del Riesgo, con el fin de determinar la zona de riesgo en el cual se ubica el riesgo identificado con la participación de los responsables de los diferentes procesos.

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

Tabla 4: Criterios para definir los Niveles de Probabilidad del Riesgos

Tabla 1. CRITERIOS PARA DEFINIR NIVEL DE PROBABILIDAD		
Criterios	**FRECUENCIA DE LA ACTIVIDAD**	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	**20%**
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	**40%**
media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al añoy máximo 5000 veces por año.	**80%**
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año.	**100%**

Criterios de análisis para estimar la probabilidad:

A continuación, se desarrolla conceptualmente este tema, para contar con mayores elementos de juicio para su análisis, iniciando con las siguientes definiciones:

N**ivel de Riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la ESE y el impacto en el cumplimiento de sus objetivos.

Apetito de riesgo: Es el nivel de riesgo que la ESE puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la Alta Dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la ESE debe o desea gestionar.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la ESE.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que la ESE puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos Institucionales.

Los niveles de aceptación de los riesgos identificados, variarán según la celda en la que se ubica el riesgo residual en la matriz de calor (niveles de severidad), los valores determinados para la probabilidad y el impacto se cruzan conforme a lo establecido en la siguiente Matriz de calificación del riesgo, con el fin de determinar la zona de riesgo en el cual se ubica el riesgo.

En el caso de los **Riesgos de Corrupción**, estos no pueden ser aceptados, en cumplimiento de la consigna **"tolerancia cero a los hechos de corrupción".** De igual manera, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto Bajo y Muy Bajo.

IMPACTO

A través de la siguiente tabla, se establecen los criterios para definir el nivel de impacto para riesgos de GESTIÓN y SEGURIDAD DE LA INFORMACIÓN.

Tabla 5 Criterios para definir el Nivel de Impacto del Riesgo

Criterio	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Leve 20%	Afectación menor a 10SMLMV	El riesgo afecta la imagen de algún área de la ESE
Menor 40%	Afectación Entre 10 y50 SMLMV	El riesgo afecta la imagen de la ESE internamente, de conocimiento general nivel interno, de junta directiva y/o de proveedores
Moderado 60%	Afectación Entre 50 y100 SMLMV	El riesgo afecta la imagen Institucional con algunos usuarios derelevancia frente al logro de los objetivos.
Mayor 80%	Afectación Entre 100 y500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catástrófico 100%	Afectación Mayor a500 SMLMV	El riesgo afecta la imagen de la ESE a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente:https://www.funcionpublica.gov.co/web/eva/bibliotecavirtual//document_library/bGsp2IjUBdeu/view_file/34316499

Por otra parte, la siguiente tabla indica los criterios para calificar el impacto en riesgos deCORRUPCIÓN.

MATRIZ DE CALIFICACIÓN DEL NIVEL DE SEVERIDAD DEL RIESGO (ZONA DE RIESGO – MAPA DE CALOR)

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen cuatro (4) zonas de severidad en la matriz de calor (BAJO, MODERADO, ALTO, EXTREMO). A través de esta, tabla se define la zona de riesgo inicial (RIESGO INHERENTE).

Análisis preliminar (riesgo inherente): Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (tal como se observa en la Tabla Matriz de calor (niveles de severidad del riesgo)

Tabla 7 Matriz de calor (Criterios de probabilidad frente al Impacto del riesgo)

NIVEL DE RIESGO								
Criterio Probabilidad			I M P A C T O					NIVELES DE RIESGO
P R O B A B I L I D A D	5	Muy Alto 100%	Alto	Alto	Alto	Alto	Extremo	
	4	Alto 80%	Moderado	Moderado	Alto	Alto	Extremo	Extremo
	3	Media 60%	Moderado	Moderado	Moderado	Alto	Extremo	Alto
	2	Bajo 40%	Bajo	Moderado	Moderado	Alto	Extremo	Moderado
	1	Muy Bajo 20%	Bajo	Bajo	Moderado	Alto	Extremo	Bajo
		Medición Impacto	Lere	Menor	Moderado	Mayor	Catastrófico	

Fuente: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-

/document_library/bGsp2IjUBdeu/view_file/34316499

Cruzando los datos de probabilidad e impacto definidos se tiene: zona de riesgo alto y Extremo, a continuación, se ilustra el nivel de riesgo para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción, se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos. En tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para los riesgos de gestión y de seguridad de la información.

NIVEL DE RIESGO							
	Criterio Probabilidad		ALTERNATIVAS DE I M P A C T O				
NIVELES DE PROBABILIDAD	5	Muy Alto 100%	Alto	Alto	Alto	Alto	Extremo
	4	Alto 80%	Moderado	Moderado	Alto	Alto	Extremo
	3	Media 60%	Moderado	Moderado	Moderado	Alto	Extremo
	2	Bajo 40%	Bajo	Moderado	Moderado	Alto	Extremo
	1	Muy Bajo 20%	Bajo	Bajo	Moderado	Alto	Extremo
		Medición Impacto	Leve	Menor	Moderado	Mayor	Catastrófico

ZONA DE RIESGO DE CORRUPCIÓN

Tabla 8 Matriz de calor (niveles de severidad del riesgo de Corrupción)

Fuente: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499

Es importante recordar que, el riesgo inherente es aquel con el cual se enfrenta la entidad antes de implementar controles, y el riesgo residual, es aquel que permanece a pesar de haberlos implementado.

Criterios para hacer el análisis de Impacto: El impacto se debe analizar y calificar a partirde las consecuencias identificadas en la fase de descripción del riesgo.

EVALUACIÓN DEL RIESGO – VALORACIÓN DE CONTROLES

Las actividades de control, independientemente al Tipo de riesgo, tendrán una adecuada combinación para prevenir que la situación de riesgo se origine y en caso de que la situación de riesgos se presente, esta debe ser detectada de manera oportuna. Se deben seleccionar actividades de control preventivas y detectivas que por sí solas ayuden a la mitigación de las causas que originan los riesgos.

DESCRIPCIÓN DE CONTROLES

Para una adecuada redacción del control, se debe tener en cuenta la siguiente estructura.

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza laactividad.

- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.

- **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

Importante tener claro que los atributos de formalización se recogerán de manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad. Hay que tener en cuenta que el movimiento en la matriz de calor acorde con el tipo de control si son Preventivos y Detectivos disminuyen la Probabilidad del Riesgo y por ende el Control Correctivo.

Nivel de riesgo (Riesgo residual): Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica la medición de uno de los controles, el siguiente control se aplicará con la medición resultante luego de la aplicación del primer control.

Resultados de la evaluación del diseño del control El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado. Resultados de la evaluación de la ejecución del control

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría interna o control interno.

EVALUACIÓN DEL RIESGO:

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Análisis preliminar (riesgo inherente):

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen4 zonas de severidad en la matriz de calor (tal como se observa en la Tabla Matrizde calor (niveles de severidad del riesgo)

Tabla 10: Matriz de calor (niveles de severidad del riesgo)

NIVEL DE RIESGO							
Criterio Probabilidad			I M P A C T O				NIVELES DE RIESGO
P R O B A B I L I D A D	5	Muy Alto 100%	Alto	Alto	Alto	Alto	Extremo	
	4	Alto 80%	Moderado	Moderado	Alto	Alto	Extremo	Extremo
	3	Media 60%	Moderado	Moderado	Moderado	Alto	Extremo	Alto
	2	Bajo 40%	Bajo	Moderado	Moderado	Alto	Extremo	Moderado
	1	Muy Bajo 20%	Bajo	Bajo	Moderado	Alto	Extremo	Bajo
		Medición Impacto	Leve	Menor	Moderado	Mayor	Catastrófico	

Fuente:https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-

Cruzando los datos de probabilidad e impacto definidos se tiene: zona de riesgo alto yExtremo.

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

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso se aplica el criterio experto.

Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control: Para una adecuada redacción del control se debe entender su tipología y atributos para su valoración. Teniendo en cuenta lo siguiente:

El Responsable del Proceso o Actividad verifica que la información, hecho, proceso resultado o acción suministrada, ejecutada o vista corresponda con los requisitos del proceso expuesto al Riesgo.

A través de una lista de chequeo, o cualquier otro medio de uso común en el proceso de auditoría (Autocontrol, Supervisión, o Auditoría) que contenga el parámetro de evaluación o están los requisitos de información se cruce, confronte o verifique contra la información física suministrada por el auditado.

En cuanto al análisis y evaluación de los controles para la mitigación de los riesgos y establecer su solidez, dado que la calificación de riesgos inherentes y residuales se efectúa al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles.

TRATAMIENTO DEL RIESGO

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluarlas opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establece la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será acepta, evitar, compartir o reducir el riesgo y se analiza frente al riesgo residual, El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Tabla 11: Tratamiento del riesgo por Niveles de Aceptación

NIVEL DE ACEPTACIÓN DEL RIESGO	TRATAMIENTO DEL RIESGO	MEDIDAS
REDUCIR ALTO MODERADO	Después de realizar un análisis, y considerar que elnivel de riesgo es ALTO o MODERADO, se determina tratarlo mediante acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, Compartir**:** después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el proceso a través de seguros o pólizas de responsabilidad. La responsabilidad económica recae sobre el tercero , pero no setransfiere la responsabilidad sobre el tema reputacional. **1. Mitigar:** después de realizar un análisis y considerarlos niveles de riesgo, se implementan acciones que mitiguen el nivel del riesgo (plan de acción). No necesariamente es un control adicional. **2.** Se hace seguimiento **PERIÓDICO** y se registransus avances.	Generar plan de acción bajo la medida para mitigarel riesgo

	3. Riesgos de Corrupción: Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo de Corrupción. Con seguimiento periódico para evitar su materialización.	
ACEPTAR BAJO	Se **ASUMIRÁ** el riesgo y se administra y controla por medio de las actividades propias del proceso asociado a los reportes de ley periódicos para evaluar su desempeño. Después de realizar un análisis y considerar los niveles de riesgo, conociendo los efectos de su posible materialización.	En este caso, no es necesario indicar plan de acción
	En este caso, se acepta el riesgo y se administra por medio de las actividades propias del proceso asociado ysu control. **Riesgos de Corrupción:** Ningún riesgo de corrupción podrá ser aceptado, su seguimiento será periódico para evitar su materialización.	
EVITAR EXTREMO	Después de realizar un análisis y considerar que el nivelde riesgo es EXTREMO, se determina NO asumir la actividad que genera este riesgo. Se debe incluir el riesgo tanto en el Mapa de riesgodel Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan **MITIGAR** lamaterialización del riesgo. Se monitorea **PERIODICAMENTE**.	

	Riesgos **de Corrupción: EVITAR** Se desautorizan las actividades que dan lugar al riesgo de corrupción, prohibiendo iniciar o continuar con la actividad que causa el riesgo. **TRANSFERIR O COMPARTIR** una parte del riesgo de corrupción para reducir la probabilidad o el impacto del mismo, con seguimiento periódico para evitar su materialización.	

ESTRATEGIAS DE COMUNICACIÓN E INFORMACIÓN

Las estrategias de comunicación, socialización o divulgación utilizados para dar a conocer la Política de Administración de Riesgos contenida en este Lineamiento, cubrirá todos los niveles de la ESE, acorde con lo dispuesto en el MIPG; Dimensión 5: Información y comunicación, haciendo uso de ayudas tecnológicas para socialización virtual, en carteleras, correos Institucionales, Página Web de La Empresa Social Del Estado Hospital Local De Aguachica, con el fin de construir una relación de confianza entre la ESE y sus Grupos de valor, coadyuvando así el fortalecimiento de los controles institucionales, en las distintas etapas de la gestión del riesgo para:

Identificar puntos críticos sobre los procesos Misionales, Estratégicos y de Apoyo que permitan mejorar la presentación del servicio y satisfacer las necesidades de los ciudadanos.

Realizar una valoración sobre la probabilidad e impacto de los riesgos para determinar el nivel de riesgo al que está expuesta La Empresa Social Del Estado Hospital Local De Aguachica.

Diseñar y ejecutar controles que atiendan la(s) causa(les) que generan los riesgos.

MAPA DE RIESGOS

Los riesgos identificados y priorizados en La Empresa Social Del Estado Hospital Local De Aguachica, se integran en el Mapa de Riesgos de la vigencia 2025, sobre los cuales la Alta Gerencia orientará su accionar para controlar su ocurrencia y mitigar su impacto cuando ello se presente. Este cubre todos los

Procesos de las áreas estratégicas, asistenciales, administrativas de apoyo y de Control, incluyendo en la matriz los riesgos de gestión, riesgo de corrupción y riesgos de seguridad digital, entreotros.

La consolidación del mapa de riesgos institucional se lleva a cabo a través de la Oficina de Planeación o quien haga sus veces. Para tal fin, se cuenta con una estructura independiente para riesgos de gestión y de seguridad de la información, y una estructura para riesgos de corrupción, consolidados en el Mapa o Matriz de Riesgo.

La aprobación de la Matriz o Mapa de Riesgo se realiza en el CICCI.

Una vez publicado y durante la vigencia 2025, se podrán realizar los ajustes y las modificaciones necesarias orientadas a optimizar la administración del Riesgo. En este caso, deberán relacionarse en el historial de cambios del mapa los ajustes, modificacioneso inclusiones realizadas.

La Oficina Asesora de Control Interno de Gestión, debe adelantar seguimiento a la gestión de los riesgos institucionales. En este sentido, es necesario que en sus procesos de auditoría interna se analicen las causas, los riesgos, la efectividad de los controlesincorporados en el mapa de riesgos institucional y el cumplimiento de las accionesplanteadas.