MANUAL DE GESTIÓN DEL RIESGO

PLANEACIÓN ESTRATÉGICA

Hospital César Uribe Piedrahita
¡Cuidamos de ti!

CONTENIDO

1. OBJETIVO GENERAL:

Describir los componentes del Sistema de Gestión de Riesgos, así como servir de guía para la implementación de la Política de Gestión del Riesgo en el marco del Sistema de Gestión del Riesgo – SGR - y el Sistema Integrado de Gestión -SIG- de la ESE.

1.1. OBJETIVOS ESPECIFICOS*:*

- ✓ Describir los componentes del Sistema de Gestión del Riesgo – SGR - de la ESE Hospital César Uribe Piedrahita y el glosario de definiciones de conceptos asociados al SGR.
- ✓ Describir el alcance de las etapas del ciclo general de gestión del riesgo.
- ✓ Describir los responsables de procesos y las actividades a realizar en el marco del Sistema de Gestión del Riesgo.
- ✓ Describir el formato matriz de riesgos por proceso para la identificación, clasificación, análisis, valoración del riesgo, validación de controles, seguimiento, monitoreo y evaluación de los riesgos.
- ✓ Describir los lineamientos para la toma de acciones de mejora continua.
- ✓ Establecer los criterios para la construcción de planes de acción o mejora que permitan mejorar los procesos frente a la gestión de riesgos (Tratamiento de los riesgos).

2. ALCANCE:

Inicia con la definición y cumplimiento del marco normativo para la administración y gestión del riesgo, hasta la evaluación de la eficacia de las estrategias definidas para implementar como tratamiento de los riesgos identificados en la transversalidad del macro y sub procesos analizados según la estructura organizacional de la Entidad.

3. DEFINICIONES:

ADMINISTRADOR: De acuerdo con el artículo 22 de la Ley 222 de 1995, "son administradores el representante legal, el liquidador, el factor, los miembros de juntas 0 consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones". El administrador debe obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios.

ANÁLISIS DE RIESGO: El uso sistemático de la información disponible para determinar cuan frecuentemente puede ocurrir eventos especificados y la magnitud de las consecuencias.

APETITO DE RIESGO: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

CANAL ANTICORRUPCIÓN: Herramienta diseñada para prevenir y detectar eventos de fraude, opacidad o corrupción, además de monitorear oportunamente las irregularidades que involucren a colaboradores, proveedores, clientes y terceros.

CIBERCRIMEN: Actividades ilícitas que se llevan a cabo para robar, alterar, manipular, enajenar o destruir información o activos (como dinero, valores o bienes desmaterializados) de compañías, valiéndose de herramientas informáticas y tecnológicas.

COHECHO: Delito que comete un particular, que ofrece a un funcionario público o persona que participa en el ejercicio de la función pública dádiva, retribución o beneficio de cualquier clase para sí o para un tercero, para que ejecute una acción contraria a sus obligaciones, o que omita o dilate el ejercicio de sus funciones.

COLUSIÓN: Pacto o acuerdo ilícito, es decir, acuerdo anticompetitivo para dañar a un tercero en procesos de contratación pública.

CONCUSIÓN: Acción realizada por un funcionario público en abuso de su cargo, para inducir a otra persona a dar o prometer a él mismo o a una tercera persona, el pago de dinero u otra utilidad indebida.

CONDUCTA IRREGULAR: Hace referencia a incumplimientos de leyes, regulaciones, políticas internas, reglamentos o expectativas de las organizaciones respecto a la conducta, ética empresarial y comportamientos no habituales

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

CONSECUENCIA: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento.

CONTRAPARTE(S): Son aquellas personas naturales o jurídicas con las cuales la organización y sus filiales y subordinadas tiene vínculos comerciales, de negocios, contractuales o jurídicos de cualquier orden. Es decir, accionistas, socios, colaboradores o empleados de la empresa, clientes y proveedores de bienes y servicios.

CONTROL DE RIESGOS: Parte de la administración de riesgos que involucra la implementación de políticas, estándares, procedimientos para minimizar los riesgos adversos.

CORRUPCIÓN: Obtención de un beneficio particular por acción u omisión, uso indebido de una posición o poder, o de los recursos o de la información.

CICLO GENERAL DE GESTIÓN DE RIESGO: Son las etapas que incorpora un Subsistema de Administración de Riesgos para cada uno de los tipos o categorías de riesgo identificadas.

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.

CONSECUENCIA: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

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 funcionarios), los cuales pueden proveer una seguridad razonable en relación con el logro de los objetivos de la entidad.

CORRUPCIÓN PÚBLICA: Cuando en el acto de Corrupción intervienen funcionarios públicos y/o la acción reprochable recaiga sobre recursos públicos.

DENUNCIA: Es la puesta en conocimiento ante la entidad de una conducta posiblemente irregular, indicando las circunstancias de tiempo, modo y lugar.

ESTAFA: Es un delito contra el patrimonio económico, donde una persona denominada estafador, genera una puesta en escena y se aprovecha de la buena voluntad para presentar negocios inexistentes y obtener algún beneficio como sumas de dinero.

EVENTO: Incidente o situación que ocurre en la empresa durante un intervalo particular de tiempo. Presencia o cambio de un conjunto particular de circunstancias.

EVALUACIÓN DEL RIESGO: Proceso de comparación de resultados del análisis del riesgo con los criterios técnicos para determinar si el riesgo, su magnitud (nivel) o ambos son aceptables o tolerables.

FACTORES DE RIESGO: Fuentes generadoras de eventos tanto internas como externas a la entidad y que pueden o no llegar a materializarse en pérdidas. Cada riesgo identificado puede ser originado por diferentes factores que pueden estar entrelazados unos con otros. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura, los acontecimientos externos, entre otros.

FAVORITISMO: Preferencia dada al "favor" sobre el mérito o la equidad, especialmente cuando aquella es habitual o predominante.

FRAUDE: Cualquier acto ilegal caracterizado por ser un engaño, ocultación o violación de confianza, que no requiere la aplicación de amenaza, violencia o de fuerza física, perpetrado por individuos y/u organizaciones internos o ajenos a la entidad, con el fin de apropiarse de dinero, bienes o servicios.

FRAUDE EXTERNO: Se define como los actos realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

FRAUDE INTERNO: Se define como todos aquellos actos que de forma intencional buscan la apropiación indebida de activos o busca causar las pérdidas que se ocasionan por actos cometidos con la intención de defraudar, malversar los activos o la propiedad de la entidad. Estos actos son realizados por al menos un empleado o administrador de la Entidad.

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.

GOBIERNO ORGANIZACIONAL: Es el conjunto de normas, procedimientos y órganos internos aplicables a cualquier tipo de entidad, mediante los cuales se dirige y controla la gestión de estas de conformidad con las disposiciones contenidas en el Articulo 2.5.2.3.4.1. del Decreto 682 de 2018. Tiene como objeto la adopción de mejores prácticas para garantizar que la gestión de las entidades se realice bajo los principios de trasparencia, eficiencia, equidad, y propender por la calidad en la prestación de los servicios de salud centrados en el usuario; además proporciona herramientas técnicas y jurídicas que permitan el balance entre la gestión de cada órgano y el control de dicha gestión.

HURTO: Delito consistente en tomar con ánimo de lucro cosas muebles ajenas contra la voluntad de su dueño, con el propósito de obtener provecho para sí o para otro.

IDENTIFICACIÓN DEL RIESGO: Proceso para encontrar, reconocer y describir el riesgo. Implica la identificación de las fuentes de riesgo, los eventos, sus causas y consecuencias potenciales.

IMPACTO: Consecuencias o efectos que puede generar la materialización del Riesgo de Corrupción en la entidad.

INFORMACIÓN PRIVILEGIADA: Aquella que está sujeta a reserva, así como la que no ha sido dada a conocer al público existiendo deber para ellos.

IMPACTO: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

INCERTIDUMBRE: Corresponde a aquella situación sobre la cual no se conoce con seguridad si ocurrirá y, de ocurrir, cómo se comportará en el futuro.

MAPA DE RIESGOS: Herramienta metodológica que permite hacer un inventario de los riesgos de forma ordenada y sistemática, haciendo la descripción de cada uno de estos y estableciendo las posibles consecuencias.

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 poder ser 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.

OPACIDAD: Falta de claridad o transparencia, especialmente en la gestión pública.

PECULADO: Conducta en la que incurren los servidores públicos cuando se apropian o usan indebidamente de los bienes del Estado en provecho suyo o de un tercero y cuando dan o permiten una aplicación diferente a la prevista en la Constitución o en las leyes a tales bienes, a las empresas o instituciones en que se tenga parte, a los fondos parafiscales y a los bienes de particulares cuya administración, tenencia o custodia se le haya confiado por razón o con ocasión de sus funciones.

PIRATERÍA: Obtención o modificación de información de otros, sin la debida autorización, ya sea una página web, una línea telefónica, computador o cualquier Sistema informático de una 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 entidades del orden nacional, departamental y municipal.

POLÍTICA PARA LA GESTIÓN DEL RIESGO: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

PREVARICATO POR ACCIÓN: Actuación voluntaria de un funcionario público para proferir resolución, dictamen y/o conceptos contrarios a la ley.
PREVARICATO POR OMISIÓN: Actuación voluntaria de un funcionario público para dejar de ejecutar o cumplir con un acto propio de sus funciones.
PROBABILIDAD / POSIBILIDAD: Oportunidad que algo suceda.
REPUTACIÓN: 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 tal como el desempeño, escándalos, menciones en prensa, entre otros.
RIESGO: Cualquier evento, amenaza, acto u omisión que en algún momento pueda comprometer el logro de los objetivos de la entidad.
RIESGO INHERENTE: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
RIESGO RESIDUAL: El resultado de aplicar la efectividad de los controles al riesgo inherente.
RIESGO NETO GLOBAL: Resultado de la combinación de cada uno de los riesgos residuales de la entidad, teniendo en cuenta la importancia relativa que a cada categoría de riesgo le haya asignado la entidad.
RIESGO ESTRATÉGICO: Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
RIESGOS DE IMAGEN: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
RIESGOS OPERATIVOS: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
RIESGOS FINANCIEROS: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
RIESGOS DE CUMPLIMIENTO: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
RIESGOS DE CORRUPCIÓN: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

RIESGOS DE TECNOLOGÍA: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

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.

SEGMENTACIÓN: Es el proceso por medio del cual se lleva a cabo la separación de elementos en grupos homogéneos al interior de ellos y heterogéneos entre ellos. La separación se fundamenta en el reconocimiento de diferencias significativas en sus características (variables de segmentación).

SOBORNO: Ofrecimiento de dinero u objeto de valor a una persona para conseguir un favor o un beneficio personal, o para que no cumpla con una determinada obligación o control.

SOBORNO TRANSNACIONAL: El que dé u ofrezca a un servidor público extranjero, en provecho de este o de un tercero, directa o indirectamente, cualquier dinero, objeto de valor pecuniario u otra utilidad a cambio de que este realice, omita o retarde cualquier acto relacionado con el ejercicio de sus funciones y en relación con un negocio o transacción internacional.

SUBSISTEMA DE ADMINISTRACIÓN DEL RIESGO DE CORRUPCIÓN, LA OPACIDAD Y EL FRAUDE – SICOF: Conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por el máximo órgano social u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

- ✓ Mejorar la eficiencia y eficacia en las operaciones de las entidades sometidas a inspección y vigilancia evitando situaciones de Corrupción, Opacidad y Fraude. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.
- ✓ Prevenir y mitigar la ocurrencia de actos de Corrupción, Opacidad y Fraudes, originados tanto al interior como al exterior de las organizaciones.
- ✓ Realizar una gestión adecuada de los Riesgos.

TRÁFICO DE INFLUENCIAS: Utilización indebida, en provecho propio o de un tercero, de influencias derivadas del ejercicio del cargo público o de la función pública, con el fin de obtener cualquier beneficio de parte de servidor público en asunto que éste se encuentre conociendo o haya de conocer. Incluye el ejercicio indebido de influencias por parte de un particular sobre un servidor público en

asunto que éste se encuentre conociendo o haya de conocer, con el fin de obtener cualquier beneficio económico.
VANDALISMO: Acciones físicas que atenten contra la integridad de los elementos informáticos, la infraestructura, entre otros, cuya finalidad es causar un perjuicio, por ejemplo, la paralización de las actividades, como medio de extorsión o cualquier otro.

4. CONDICIONES GENERALES:

La Alta Dirección de la ESE, debe llevar a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- ✓ Socializar anualmente la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado.
- ✓ Capacitar al grupo de trabajo de cada dependencia en la herramienta para la gestión del riesgo.
- ✓ Liderar las mesas de trabajo de identificación del riesgo.
- ✓ Liderar las mesas de trabajo para determinación del análisis de impacto de la prestación de los servicios, documentación de los escenarios de riesgo y plan de continuidad del buen funcionamiento institucional.
- ✓ Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología.
- ✓ Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en la herramienta para la gestión del riesgo.
- ✓ Elaborar el mapa de riesgos institucional con toda la información respectiva, a partir de la información construida con los equipos de trabajo.
- ✓ Una vez aprobado por el CICCI, socializar los resultados de las mesas de identificación y recordar a los líderes la importancia de socializarlos al interior de sus procesos.
- ✓ Revisar que el cargue de información en la herramienta de gestión de riesgo esté acorde con lo aprobado.
- ✓ Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso, con los riesgos altos, extremos y de corrupción.

Por su parte, los líderes de proceso tienen la responsabilidad de:

- ✓ Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.
- ✓ Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados.

Desde Planeación estratégica se debe garantizar:

a) Fomentar acciones de interacción, articulación, alineación y complementación entre el Plan Estratégico Institucional, la planeación operativa y los procesos que permitan el diseño de procedimientos estructurados con el enfoque de la gestión de riesgos y el fortalecimiento de los controles en las diferentes etapas del ciclo de gestión de riesgos y la planeación, ejecución, seguimiento, control y evaluación de la gestión institucional.

b) Equipos de trabajo comprometidos: Responsables de la definición, identificación y caracterización de los riesgos, su valoración y definición de controles por procesos y estructuración de planes de acción que permitan la adecuada y oportuna administración del riesgo. De manera transversal y de especial relevancia es el actuar de los trabajadores, y contratistas de la institución frente a su compromiso con las buenas prácticas y la gestión bajo los principios de transparencia y ética.

c) Monitoreo y seguimiento de la gestión del riesgo. El seguimiento, control y evaluación de los riesgos por proceso y de manera integral con la participación de todos los niveles de la institución como responsables del sistema de gestión del riesgo..

d) Formación y actualización permanente. Compromiso institucional de ofrecer a sus líderes de proceso, trabajadores, capacitación y actualización en la administración del riesgo, así como alcanzar el aprendizaje y apropiaciones de herramientas y procedimientos requeridas para la gestión del riesgo como una línea de aprendizaje y actualización permanente, a través de inducción, entrenamiento, acompañamiento, actividades lúdicas, entre otros.

e) Contar con una política de gestión de los riesgos de la ESE, debidamente aprobada, socializada y evaluada.

5. DESCRIPCIÓN GENERAL:

La ESE Hospital César Uribe Piedrahita, debe tener la capacidad institucional 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.

Tanto el Sistema Integrado de Gestión de Riesgos como los Subsistemas que lo componen deben contar al menos con los siguientes elementos mínimos:

i) Ciclo General de Gestión de Riesgos,
ii) Políticas de Gestión de Riesgos,
iii) Procesos y Procedimientos,
iv) Documentación,
v) Estructura Organizacional,
vi) Infraestructura Tecnológica y
vii) Divulgación de la Información y Capacitaciones.

En este contexto, la ESE debe gestionar todos los riesgos a los que esté expuesta dentro de su operación y su gestión dependerá de la discrecionalidad y organización que se establezca para su tratamiento.

Sin embargo, se contemplan como mínimo, los siguientes riesgos priorizados y sus respectivos subsistemas:

1. Riesgo en Salud
2. Riesgo Operacional
3. Riesgo Actuarial
4. Riesgo de Crédito
5. Riesgo de Liquidez
6. Riesgo de Mercado de Capitales
7. Riesgo de Grupo
8. Riesgo de Lavado de Activos y Financiación del Terrorismo.

9. Riesgos de Corrupción, opacidad y fraude
10. Riesgos Informaticos

Cabe recordar que, el 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.

Los lineamientos específicos se encuentran publicados en la **Circular Externa** 009 **de 2016** (expedida por la SNS) y **Circular Externa** 5-5 **de 2021** (expedida por la SNS), y las normas que la modifiquen, sustituyan o eliminen.

5.1. CICLO GENERAL DE GESTIÓN DE RIESGOS.

Para cada una de las categorías de riesgo se incluyen las siguientes etapas en los Subsistemas de Administración de Riesgos:

a) Identificación de riesgos: Consiste en reconocer, explorar exhaustivamente y documentar todos los riesgos internos y externos que podrían afectar tanto los objetivos de la entidad como la salud de los usuarios a su cargo, en los casos que aplica, identificando sus causas, efectos potenciales y la posible interrelación entre los diferentes tipos de riesgos, para lo cual se recomienda la utilización de normas técnicas nacionales o internacionales.
Para esta identificación, las entidades podrán seleccionar las metodologías y técnicas que consideren más adecuadas, dentro de las que se encuentran estudios científicos encuestas, entrevistas estructuradas con expertos, talleres, lluvia de ideas, técnicas de escenarios, entre otros.

b) Evaluación y medición de riesgos: Es la valoración de los efectos asociados a los riesgos que han sido identificados, considerando la frecuencia y la severidad de su ocurrencia. También se deberá considerar el análisis de los riesgos inherentes y residuales, y su participación en el riesgo neto global. Se

entenderá por valoración del riesgo, la medida cualitativa o cuantitativa de su probabilidad de ocurrencia y su posible impacto.

En la medida que avance el plan de implementación del modelo de Supervisión Basada en Riesgos, las entidades deberán contar con evaluaciones cuantitativas relacionadas con la probabilidad de ocurrencia de los riesgos identificados y su impacto, en la medida de lo posible. Independientemente de contar con modelos cuantitativos o cualitativos, estos deben estar sustentados y documentados técnicamente.

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. Si la entidad no cuenta con este recurso se deben establecer mecanismos para tener estimaciones consistentes para cada uno de los riesgos asumidos y deberá documentar las hipótesis y supuestos de sus modelos, así como la información que se tuvo en cuenta para su cálculo, mientras logra obtener la información requerida y necesaria.

c) Selección de estrategias para el tratamiento y control de los riesgos: Una vez identificados y evaluados los riesgos, deben compararse con los límites (tolerancia) de riesgos aprobados por la instancia definida en el Gobierno Organizacional de la entidad y su política de riesgos, siempre dentro del marco normativo establecido. Todo riesgo que exceda los límites o desviaciones aceptadas, debe ser objeto de actividades de mitigación y control a fin de regresar al nivel de riesgo tolerado, conforme la estrategia adoptada. En cuanto a los riesgos en salud, estos límites hacen referencia a los máximos permitidos por la normatividad vigente, estándares internacionales y sin perjuicio de lo anterior, de acuerdo con lo que establezca la entidad en sus políticas, siempre que estén en pro del beneficio de la población de su área de influencia.
Se deben determinar las acciones tendientes a gestionar los riesgos a los que se ve expuesta la entidad, de acuerdo con los niveles de riesgo determinados y las tolerancias al riesgo definidas.

Todas las acciones de gestión del riesgo deberán identificar formalmente responsables, plazos, formas de ejecución y reportes de avances, los cuales deben corresponder a la complejidad de la operación de la entidad. Asimismo,

deberán estar aprobadas por la instancia del Gobierno Organizacional que corresponda.

d) Seguimiento y monitoreo: Una vez establecidos los posibles mecanismos o un conjunto de estos, para la mitigación y control de los riesgos que se han identificado como relevantes para la entidad y después de realizar un análisis de causa y efecto para determinar los puntos más críticos a intervenir con mayor prelación, 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 ESE debe desarrollar un sistema de alertas tempranas que facilite la rápida detección, corrección y ajustes de las deficiencias en cada uno de sus Subsistemas de Administración de Riesgo para evitar su materialización.
Lo anterior, con una periodicidad acorde con los eventos y factores de riesgo identificados como potenciales, así como con la frecuencia y naturaleza de estos.

El diseño de dicho sistema de alertas debe incluir la definición de los límites máximos de exposición o niveles aceptables de riesgo previamente establecidos por la entidad teniendo en cuenta los análisis realizados, la normatividad vigente y los criterios definidos en la política de gestión de riesgo de cada entidad.

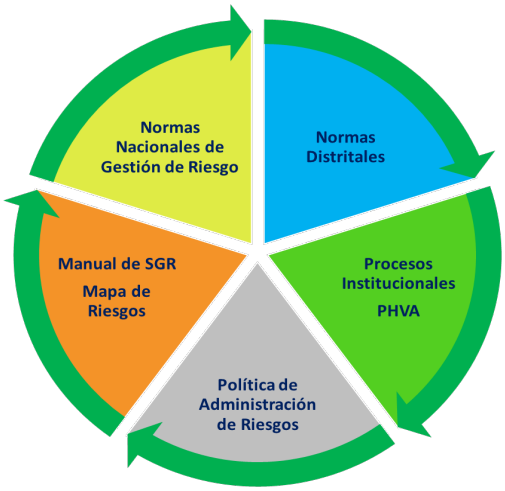
Las mediciones de riesgos esperadas, los riesgos derivados y sus controles deben ser contrastados regularmente con la realidad observada, de forma tal que permita establecer si los Subsistemas de Administración de Riesgos han logrado su mitigación y la corrección oportuna y efectiva de eventuales deficiencias. De esta manera la entidad debe contar con indicadores de gestión para hacer seguimiento a la administración de los riesgos residuales y netos, y que estos a su vez se encuentren y se mantengan en los niveles de aceptación previamente establecidos por la entidad.

De llegarse a presentar desviaciones o que se superen los límites previamente establecidos, se deben establecer planes de contingencia para intervenir y tratar los diferentes riesgos, teniendo en cuenta la variabilidad de los riesgos identificados, con el propósito de ajustar las desviaciones lo más pronto posible.

Todas las acciones y actividades incluidas en estos planes deben contener la definición de los estándares de seguimiento y monitoreo, además de contar con un responsable, plazos, periodicidad, reportes de avance y de evaluaciones periódicas sobre las estrategias seleccionadas que incluyan el monitoreo de los indicadores propuestos para el seguimiento de las acciones de gestión del riesgo planteadas, los cuales deben ser definidos mediante un cronograma y ser objeto de un proceso de seguimiento, verificación y calidad de la información. Los planes de contingencias resultantes del seguimiento a riesgos deben ser coherentes con otras medidas contingentes o planes de mejoramiento resultantes de otras actividades de control, internas o externas, a fin de lograr soluciones estructurales e integrales a las problemáticas identificadas.

En esta etapa cobra importancia la implementación de mecanismos de retroalimentación, donde se promueva la comunicación dinámica y continua, la entrega de reportes gerenciales y de monitoreo donde se evalúen los resultados obtenidos, su evolución y la ejecución de los controles y estrategias implementadas para mejorar el desempeño en la mitigación de los factores de riesgo en cada uno de los Subsistemas de Administración de Riesgo, dirigidos a todos los involucrados tanto externos como internos, en especial a los órganos de seguimiento definidos por el Gobierno Organizacional de cada entidad. Lo anterior determina la necesidad de implementar planes de mejora, en donde se desarrollen estrategias de incorporación de cambios para mejorar los resultados en la gestión de riesgos de la entidad.

El Sistema de Gestión del Riesgo – SGR en la ESE- es el conjunto ordenado de componentes relacionados entre sí que orientan la planificación, ejecución, seguimiento, control y evaluación de los riesgos en la ESE Hospital César Uribe Piedrahita. Los componentes del SGR se reflejan en la siguiente gráfica:



La normatividad aplicable en cuanto a gestión de riesgos es:

ENTIDAD	NORMATIVIDAD APLICABLE
Presidencia de la República	Estatuto Anticorrupción Ley 1474 de 2011.
Superintendencia Nacional de Salud	Supervisión Basada en Riesgos Supersalud 2015, Circular Externa 009 de 2016, Circular Externa 007 de 2017, Circular externa 004 y Circular Externa 008 de 2018, Instrucciones relativas al Código de Conducta y Buen Gobierno, Sistema Integrado de Riesgos y Subsistemas de Administración de Riesgos, Circular Externa 5-5 de 2021 sobre actualización del SARLAFT y creación del SICOF.
Ministerio de Salud	Ley 1751 de 2015, el artículo 65 de la Ley 1753 del 2015, el Plan Decenal de Salud Pública vigente y la Política de Atención Integral en Salud, Decreto 682 de 2018, Decreto 780 de 2016 Resolución 2515 de 2018, Resolución 429 de 2016 (GIRS).

Los componentes del Sistemas de gestión de Riesgos – SGR, se definen a continuación:

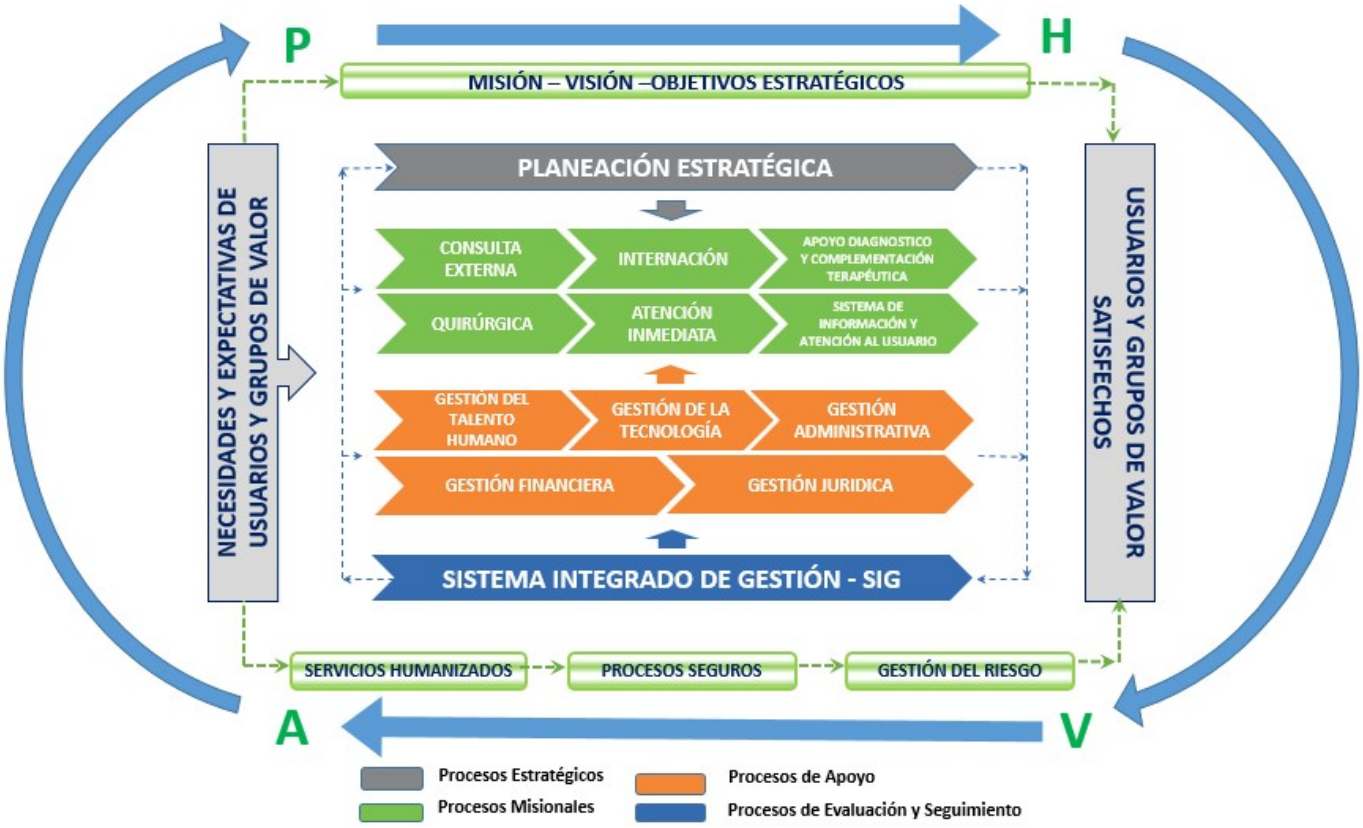
TERMINO	DEFINICIÓN
Normas Nacionales	Normas del orden nacional de entidades con competencias en el direccionamiento de la gestión de riesgos, y las específicas del sector salud.
Sistemas de Gestión Calidad	Es el sistema que maneja los lineamientos sobre actualización y mejoramiento de la documentación de los

	procesos, procedimientos e instructivos que hacen parte de la Entidad, proporciona una metodología formal y sistemática para la investigación, tratamiento y análisis de causas de problemas de calidad y/o oportunidades de mejora; realiza el seguimiento y evaluación de la gestión de la calidad en los componentes del sistema obligatorio de garantía da la calidad (SOGC) que son de obligatorio cumplimiento
Mapa de procesos	Representación gráfica de los procesos de la Entidad que son las actividades planificadas que implican la participación de un número de personas y de recursos materiales coordinados para conseguir un objetivo previamente identificado.
Ciclo PHVA	El Ciclo PHVA (Planificar-Hacer-Verificar-Actuar) es una herramienta de gestión para la mejora continua de la calidad de los procesos que contribuye al logro de los objetivos trazados.
Política de Gestión del Riesgo	Lineamientos y orientaciones de la Junta Directiva y la Gerencia para las prácticas de gestión, comunicación, consulta, establecimiento de contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.
Manual del Sistema de Gestión del Riesgo – SGR	Guía para que el colaborador pueda identificar, clasificar, analizar, valorar y realizar el seguimiento y monitoreo de los riesgos.
Mapa de Riesgos	Es una herramienta que, a partir de la información de riesgos procesada, representa gráficamente QUÉ sucede y permite visualizar los riesgos a los que la ESE está expuesta

Los procesos de la cadena de valor de la ESE Hospital César Uribe Piedrahita, cuentan con una estructura funcional alineada y articulada, representada en un Mapa de Procesos enfocado en la satisfacción de las necesidades y expectativas de los afiliados.

El mapa permite identificar los macroprocesos y procesos claramente, el sistema de Gestión del Riesgo está contenido en el proceso Integrado de Gestión.

A continuación se observa el mapa de procesos de la ESE.



La orientación del Sistema de gestión de Riesgos, se basa en la identificación de riesgos de salud, financieros y operativos que enfrentan las instituciones objeto de vigilancia, así como su capacidad para medir, gestionar y monitorear estos riesgos.

Las principales ventajas del Sistema de gestión de Riesgos según Resolución 4559 de 2018, se fijan de acuerdo a los siguientes términos:

- ✓ Fortalece la supervisión por cumplimiento mediante la implementación de la supervisión basada en riesgos.
- ✓ Es un modelo de supervisión, innovador, de carácter prudencial y activo.
- ✓ Optimiza el uso de los recursos de supervisión.

- ✓ Aumenta la probabilidad de que los eventos más importantes sean detectados a tiempo y prevenidos antes de que se materialicen.
- ✓ Incentiva a las entidades vigiladas a identificar, gestionar y monitorear sus riesgos, bajo un esquema eficiente de autorregulación.
- ✓ Impulsa una cultura de gestión de riesgos por parte de los vigilados, de manera que esta sea una política empresarial o de gobierno corporativo que se interiorice en toda la estructura organizacional, incluyendo políticas de control interno.

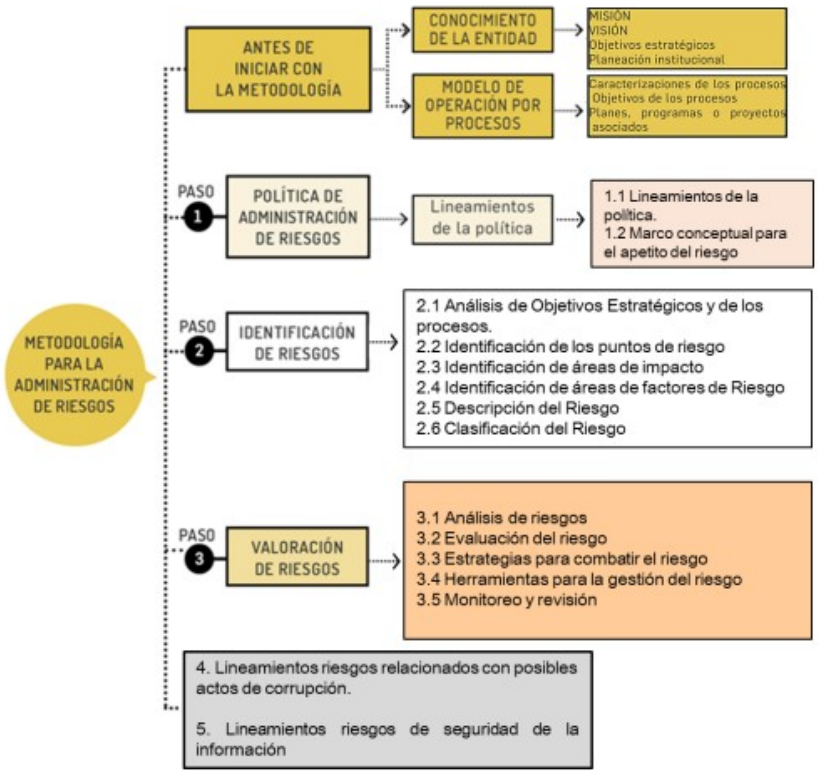
En contexto con lo anterior, las entidades sujeto de vigilancia deben tener la capacidad institucional para identificar, evaluar, controlar y mitigar los riesgos que puedan afectar el logro de sus objetivos y especialmente, el cumplimiento de los objetivos del SGSSS.

De tal manera la gestión del riesgo es un proceso efectuado por la Gerencia y por todo el personal, con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- ✓ Apoyo a la toma de decisiones
- ✓ Garantizar la operación normal de la organización
- ✓ Minimizar la probabilidad e impacto de los riesgos
- ✓ Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
- ✓ Fortalecimiento de la cultura de control de la organización
- ✓ Incrementa la capacidad de la entidad para alcanzar sus objetivos
- ✓ Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente Para la implementación del Sistema Integrado de Gestión de Riesgos como los 9 Subsistemas que lo componen, deben incluir el ciclo general de gestión de riesgos, políticas, procesos y procedimientos, documentación, estructura organizacional, infraestructura tecnológica y divulgación de la información y capacitaciones.

5.2. ENFOQUE METODOLÓGICO

La metodología utilizada es una mezcla de la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5, y las circulares externas 004/2018, 009/2016 y 5-5/2021 de la SUPERSALUD. Para la administración del riesgo en la ESE, se requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos (política de gestión del riesgo, identificación de riesgos, y valoración de riesgos) 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. A continuación y con base en la metodología del DAFP, la cual está articulada con las CE de la SUPERSALUD, dando cumplimiento a todo el ciclo exigido por ellos:



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

La responsabilidad frente a la gestión del riesgo en la ESE Hospital César UribePiedrahita, se asume de la siguiente manera:

Línea de Defensa	Responsable	Responsabilidad Frente al Riesgo
Línea Estratégica	Comité Directivo Comité de Gestión y Desempeño Institucional	• Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. • Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Recomendaciones de mejoras a la política de operación para la administración del riesgo.
	Comité institucional de coordinación de control interno	• Someter a aprobación de la Junta Directiva la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización y evaluar su eficacia frente a la gestión del riesgo institucional. • Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. • 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. • Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • 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. • Garantizar el cumplimiento de los planes de la entidad.

Primera Línea de Defensa	Líderes de Procesos. Coordinadores de servicios. Servidores Públicos.	Líderes y coordinadores: • Identificar y valorar los riesgos que pueden afectar al proceso, los programas, proyectos, planes a su cargo y actualizarlo cuando se requiera con énfasis en la prevención del daño antijurídico. • Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineado con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles • Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo • Reportar en el SGI los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. • Realizar la medición y análisis a la gestión efectiva de los riesgos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo y aplicar las acciones correctivas o de mejora necesarias. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces.

		Los servidores en general deben: • Participar en el diseño de los controles que tienen a cargo. • Ejecutar el control de la forma como está diseñado. • Proponer mejoras a los controles existentes.
Segunda Líneade Defensa	Proceso Planeación Estratégica Oficial de cumplimiento.	• 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 • Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional • Presentar al CICCI el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoracióndel riesgo • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestionelos riesgos y controles para que se generen acciones • Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del comité institucional de coordinación de control interno.

Segunda línea dedefensa	Líderes de: Planeación Estratégica, Consulta Externa, Internación, Apoyo Diagnostico y Complementación Terapéutica, Quirúrgica, Atención Inmediata, SIAU, Gestión del Talento Humano, Gestión de la tecnología, Gestión Administrativa. Gestión financiera, Gestión Jurídica, coordinadores y los supervisores de contrato de la Entidad entre Otros.	• Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo • Reportar al Proceso de Planeación Estratégica a través del SGI – Mapa de riesgos, el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención del daño antijurídico • Supervisar que la primera línea de defensa identifique, evalué y gestione los riesgos en los temas de su competencia
Tercera línea de defensa	Oficina de Control interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa • Asesorar de forma coordinada con el Proceso de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI • Recomendar mejoras a la política de administración del riesgo

Segunda línea de defensa	Líderes de proceso y coordinadores.	• Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo • Reportar al Proceso de Planeación Estratégica a través del SGI – Mapa de riesgos, el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención del daño antijurídico Supervisar que la primera línea de defensa identifique, evalué y gestione los riesgos en los temas de su competencia.
Tercera línea de defensa	Oficina de Control interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa • Asesorar de forma coordinada con el Proceso de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI • Recomendar mejoras a la política de administración del riesgo

A través de la matriz niveles de responsabilidad y autoridad (la matriz anteriormente descrita) se definen los cargos que pueden identificar, valorar, definir controles y acciones, validar y reportar los riesgos institucionales a través de la caracterización de cada uno de los procesos.

5.3. POLÍTICA DE GESTIÓN DE RIESGOS DE LA ESE

"La E.S.E Hospital César Uribe Piedrahita se compromete a controlar todos aquellos riesgos de Gestión, de Corrupción, Lavado de Activos y Financiación del Terrorismo y de Seguridad Digital, pertenecientes a cualquier subsistema que pueden impedir el cumplimiento de los objetivos estratégicos, planes, programas, proyectos y procesos institucionales, mediante una efectiva administración de los mismos, acatando la metodología aprobada para su gestión con la participación de los servidores públicos, contratistas y colaboradores responsables de identificar y analizar las acciones de control detectivas y preventivas oportunas para evitar la materialización y la actuación correctiva inmediata ante las eventualidades para mitigar las posibles consecuencias a fin de mantener al máximo los niveles de riesgo en zonas moderadas o baja".

Ver PO-01-01-001 POLITICA DE ADMINISTRACIÓN DE RIESGOS.

Su objetivo es establecer conductas de prevención, que permitan una adecuada gestión de los riesgos mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misión, visión y el logro de objetivos institucionales, reduciendo las vulnerabilidades ante las amenazas internas y externas, mejorando la capacidad institucional de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la ESE Hospital César Uribe Piedrahita.

5.4. ETAPAS DE LA GESTIÓN DEL RIESGO

5.4.1. Identificación del Riesgo

Se empieza por el análisis de los 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.

Análisis de objetivos estratégicos	Análisis de los objetivos de proceso
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso. Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).	Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero además, se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos. A continuación encontrará un ejemplo de análisis en el proceso de contratación: La entidad debe adquirir con oportunidad y calidad técnica, en no menos del 90%, los bienes y servicios requeridos para su continua operación.

Fuente: Comitte of Sponsoring Orgizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio. p. 73. 2013.

El proceso de SIG 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 SMART, cuya estructura se explica a continuación:

S ***Specific*** **(específico):** Lo importante es resolver cuestiones como: qué, cuándo, cómo, dónde, con qué, quién. Considerar el orden y los necesarios para el cumplimiento de la misión.

M ***Mensurable*** **(medible):** Para ello es necesario involucrar algunos números en su definición, por ejemplo, porcentajes o cantidades exactas (cuando aplique).

A ***Achievable*** **(alcanzable);** Para hacer alcanzable un objetivo se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudará a saber si lo que se propone es posible o cómo resultaría mejor.

R ***Relevant*** **(relevante):** Considerar recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación.

T ***Timely*** **(temporal):** Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

Después debe identificarse los puntos o actividades de riesgos dentro de cada proceso.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2017.

Cuando se identifican las actividades que porian generar los riesgos se procede a identificar lás áreas de impacto que 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.

Hay que identificar posteriormente cuales son los factores de riesgos, los cuales se clasifican asi:

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.		Hurto 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

5.4.1.1 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 que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

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

Desglosando la estructura propuesta tenemos:

- ✓ Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- ✓ Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- ✓ Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son 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 n existir más de una causa o subcausas que pueden ser analizadas.

Premisas para una adecuada redacción del riesgo

- ✓ No describir como riesgos omisiones ni desviaciones del control. Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- ✓ No describir causas como riesgos Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
- ✓ No describir riesgos como la negación de un control. Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.
- ✓ No existen riesgos transversales, lo que pueden existir son causas transversales. Ejemplo: pérdida de expedientes.

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

Teniendo en cuenta que las ESE´S deben gestionar todos los riesgos a los que estén expuestas dentro de su operación dentro del sector Salud, en la ESE Hospital César Uribe Piedrahita, los riesgos se agruparan en la tipología de riesgos de corrupción y por medio de los siguientes subsistemas de administración:

• Riesgo en Salud.
• Riesgo Actuarial.
• Riesgo de Crédito.
• Riesgo de Liquidez.
• Riesgo de Mercado de Capitales.
• Riesgo Operacional.
• Riesgo de Fallas del Mercado de Salud.
• Riesgo de Grupo. Riesgo Reputacional.
• Riesgo de Lavado de Activos y Financiación del Terrorismo.
• Riesgos de Corrupción, opacidad y fraude
• Riesgos Informaticos

5.4.1.2. Clasificación de Riesgos:

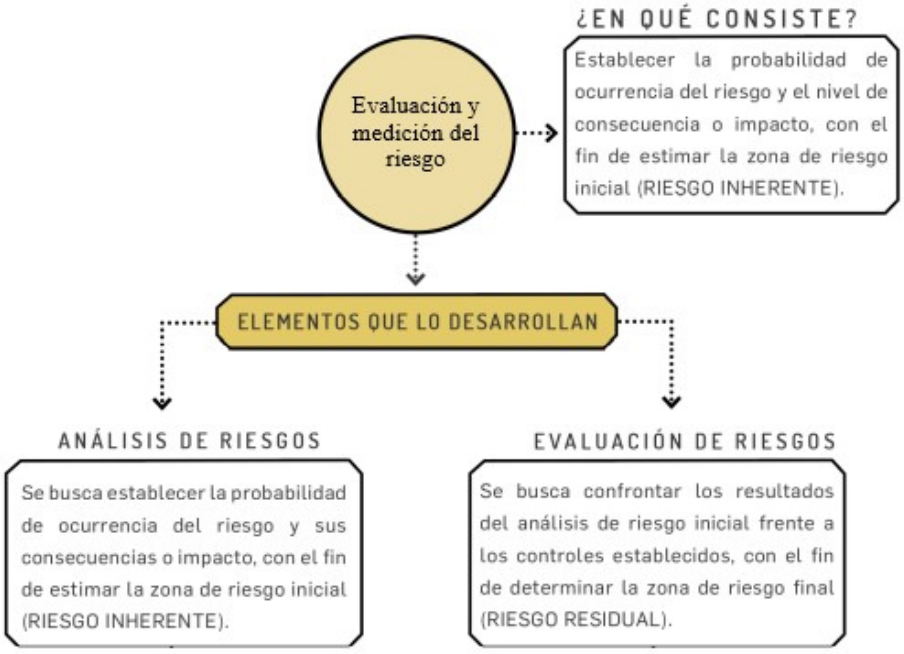
Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Ejecución y administración de procesos	Pérdidas derivadas de errores en ejecución y administración de procesos.
Fraude externo	Perdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Perdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con amino de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupciones de servicios básicos.
Relaciones laborales	Perdidas 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.
Usuarios, productos y practicas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación personal frente a estos.
Daños a activos fijos/ eventos externos	Perdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

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

La relación ente factores de riesgo y clasificación del riesgo se muestra a continuación:

5.4.2. Evaluación y medición de riesgos:



En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

Determinar la probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la próxima tabla, se establecen los criterios para definir el nivel de probabilidad.

	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 año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Determinar el impacto: Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.
Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferente niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel Frecuencia de la Actividad Probabilidad Muy Baja La actividad que conlleva el

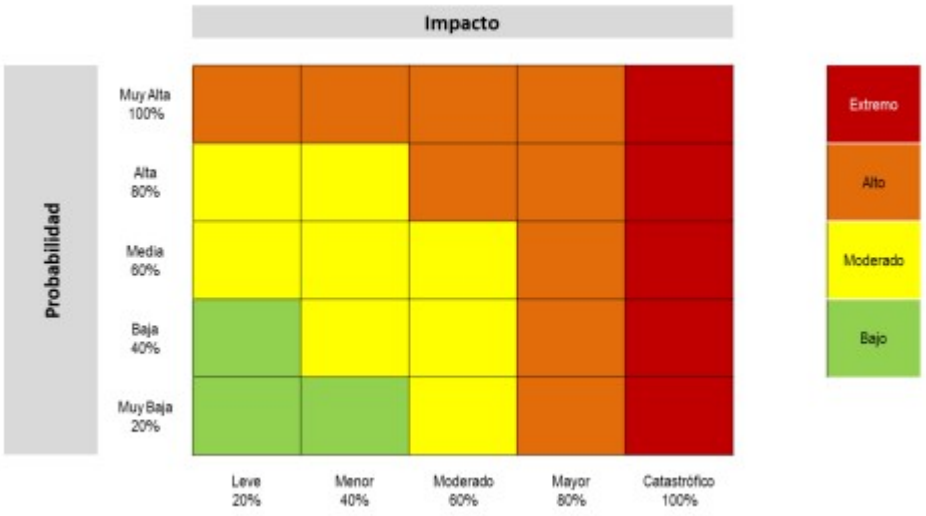
riesgo se ejecuta como máximos 2 veces por año 20% Baja La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año 40% Media La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año 60% Alta La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año 80% Muy Alta La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año 100% 40 insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado. Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis. En la siguiente tabla se establecen los criterios para definir el nivel de impacto.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo. Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto s, 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 definen 4 zonas de severidad en la matriz de calor, como se muestra a continuación:



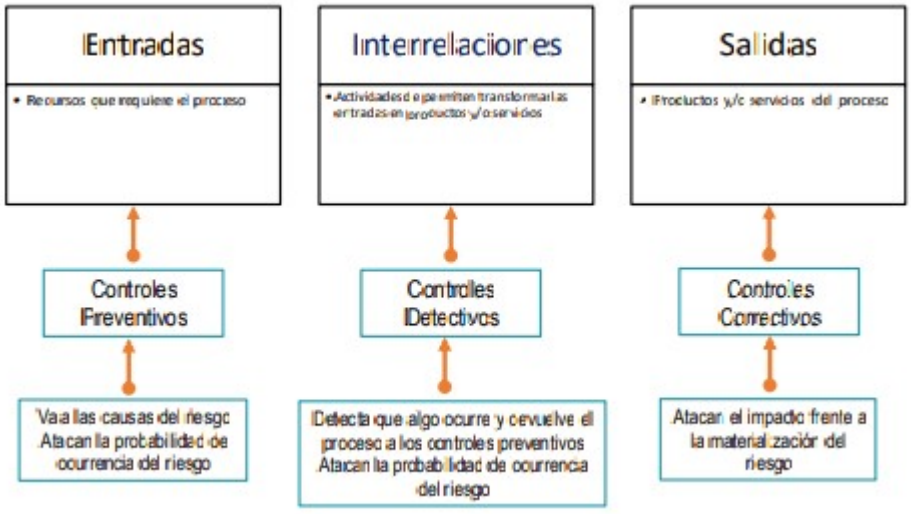
Valoración de controles: en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- ✓ 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 sí 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 propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- ✓ *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 la actividad.
- ✓ *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.

Tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura 15 se consideran 3 fases globales del ciclo de un proceso así:



Acorde con lo anterior, tenemos las siguientes tipologías de controles:

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo.

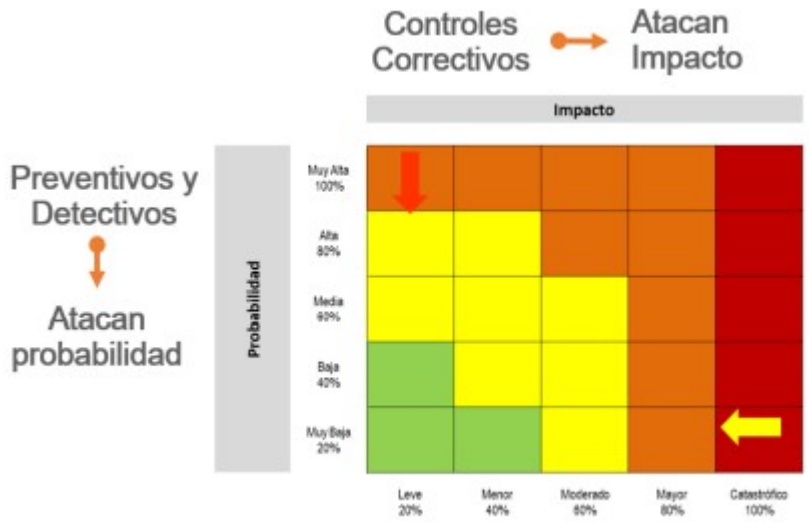
Estos controles tienen costos implícitos. Así mismo, de acuerdo con la forma como se ejecutan tenemos:
Control manual: controles que son ejecutados por personas.
Control automático: son ejecutados por un sistema.

Análisis y evaluación de los controles – Atributos: A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 6 se puede observar la descripción y peso asociados a cada uno así:

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la	25%

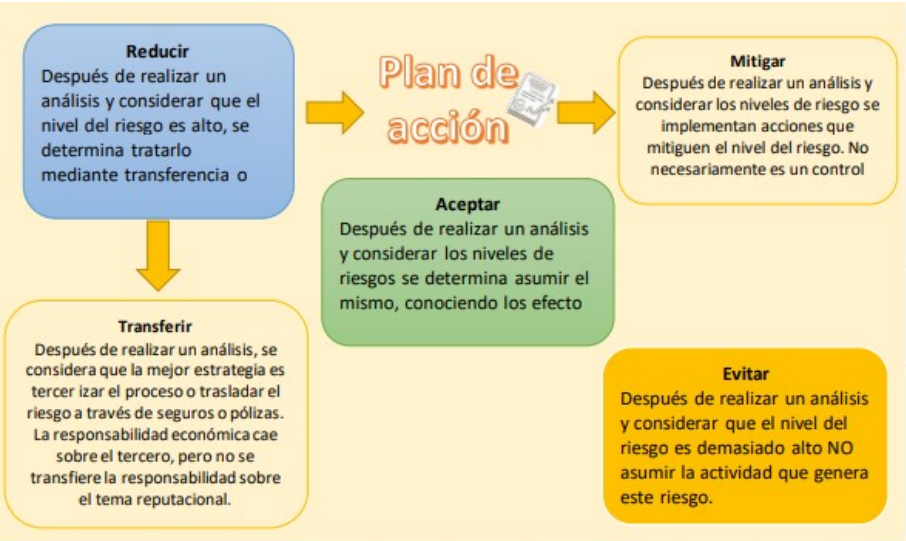
Características			Descripción	Peso
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad. Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a siguiente figura, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



5.4.3. Selección de estrategias para el tratamiento y control de los riesgos:

Las estrategias para combatir el riesgo son las decisiones 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. A continuación se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.



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

Es fundamentar implementar un plan de acción compuesto por herramientas de planificación para la gestión y control de tareas o proyectos. El plan de acción debe contar con la descripción, el responsable, la fecha de implementación, y la fecha de seguimiento.

En la política de gestión de los riesgos PO-01-01-001 se define los niveles de aceptación de riesgo y accionar frente a los riesgos materializados.

Para el control de los riesgos la ESE ha diseñado la FO-01-01-017 MATRIZ DE RIESGOS INSTITUCIONALES, en la cual se deben registrar los riesgos de cada proceso.

De acuerdo al perfil del riesgo que tiene la organización, existen diferentes indicadores que sirven para generar alertas tempranas, para ello existen dos tipos de indicadores que se ajustan a las necesidades que requiere la ESE Hospital César Uribe Piedrahita, para gestionar sus riesgos, los cuales son:

- ✓ Los indicadores clave de Riesgo - (KRI): cuantifican el perfil de riesgo de la compañía. Se constituyen de acuerdo con el nivel de relevancia en los indicadores de riesgo y de control. Por ejemplo, el volumen de operaciones, rotación de personal, número de veces que cae el sistema, etc. Cada KRI deberá ser capaz de ser medido con precisión y reflejar de manera precisa el impacto negativo que tendría sobre los indicadores de desempeño clave de la organización. Los KRI son métricas creadas para poder sintetizar objetivamente aquellos riesgos que se consideran significativos y que necesitan un tratamiento diferenciado. Estas métricas permiten llevar un registro de incidencias, monitorear su comportamiento, informar sobre su evolución, reportarlos y establecer planes de acción cuando salen de la tendencia esperada.
- ✓ Los indicadores clave de control – (KCI): Se encargan de medir la efectividad, tanto del diseño como de desempeño de un control específico. Un deterioro en un KCI puede significar un aumento en la probabilidad e impacto de un riesgo. Los indicadores KRI y KCI son fundamentales en cualquier proceso de gestión por que ofrecen información relevante para la toma de decisiones oportunas y se enfocan en la gestión de los riesgos más urgentes que tenga la organización. Estos indicadores serán

implementados en los procesos, en los cuales se tienen riesgos más críticos y de alto impacto, y propuestos por cada uno de los líderes de procesos con el propósito de elaborar una ficha técnica y posteriormente realizar la medición de manera mensual. Por último, los procesos deben reportar la medición de los indicadores en la herramienta designada (matriz de Riesgos), ya que estos servirán de análisis para la toma de decisiones de manera más predictiva y preventiva con el fin de anticiparse ante una posible materialización del riesgo y así evitar posibles pérdidas financieras.

Adicionalmente a través de la RESOLUCIÓN N°20220546 del 20 de septiembre del 2022, por la cual se modifica y articulan los comités institucionales de gestión y desempeño, gestión del riesgo y de archivo, donde se establecen las siguientes funciones en cuanto a la gestión de los riesgos de la ESE:

- ✓ Revisar y recomendar los límites de exposición de riesgos de la ESE.
- ✓ Supervisar el desempeño y cumplimiento de los objetivos de los controles establecidos para cada riesgo en la institución.
- ✓ Fomentar la comunicación con la alta gerencia sobre los riesgos de la institución. Promover la gestión del riesgo en la institución.
- ✓ Proponer ajustes a la política de gestión de riesgos y hacer seguimiento en especial a la prevención y detección de fraude y mala conducta.
- ✓ Las demás asignadas por el Gerente de la ESE Hospital César Uribe Piedrahita de Caucasia, que tengan relación directa con el desarrollo de las políticas del MIPG.

5.4.4. Monitoreo y Revisión:

El modelo integrado de planeación y gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como sigue:

Esquema de líneas de defensa:

LINEA ESTRATEGICA		
Define el marco general para la gestión del riesgo y el control A cargo de la Alta Dirección y del Comité Institucional Coordinador de Control Interno - CICCI		
PRIMERA LINEA DE DEFENSA	**SEGUNDA LINEA DE DEFENSA**	**TERCERA LINEA DE DEFENSA**
A cargo de líderes de procesos o coordinadores de áreas, programas y proyectos de la entidad, personal de apoyo Se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. Identifica, evalúa, controla y mitiga los riesgos.	A cargo de servidores con responsabilidades de monitoreo y evaluación de controles y riesgos: Jefes de planeación, supervisores, interventores, coordinadores de otros sistemas. Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente	A cargo de la oficina de control interno, Auditoria Interna o quien haga sus veces. Proporciona información sobre la efectividad del SCI, la operación de la 1ª y 2ª línea de defensa con un enfoque basado en riesgos

Según la periodicidad definida para cada riesgo el líder del mismo verifica las acciones preventivas y registra el avance junto con la evidencia en el SGI.

Analizan los resultados del seguimiento y establece acciones inmediatas ante cualquier desviación, comunica las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir. Se asegura que se documenten las acciones de corrección o prevención en el plan de mejoramiento

Los riesgos se identifican y/o validan en cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción institucional, asegurando la articulación de éstos con los compromisos de cada proceso.

5.5. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN, OPACIDAD O FRAUDE

La ESE Hospital César Uribe Piedrahita se compromete a cumplir la normas y leyes impartidas en materia de prevención y mitigación del riesgo de prácticas orientadas a Corrupción, Opacidad y Fraude, con el propósito de contribuir a la realización de los fines del Sistema General de Seguridad Social en Salud en Colombia, proteger la imagen y reputación de la entidad, promoviendo el actuar ético y transparente ante sus grupos de interés, fomentando la integridad y la cultura de legalidad bajo la filosofía de cero tolerancia, en cualquier conducta que pudiese ser considerada como Corrupción, Opacidad, Fraude o que pueda, en cualquier otra forma, ser considerada una conducta irregular.

Este documento se integra con el Código de Conducta, Buen Gobierno e Integridad de la ESE. En desarrollo de lo anterior se adopta lo siguiente:

- ✓ Realizar las debidas diligencias para conocer adecuadamente a los empleados, clientes, contrapartes y de más grupos de interés que se vinculan con la ESE Hospital César Uribe Piedrahita, dando cumplimiento a los procedimientos de vinculación establecidos por la Organización.
- ✓ Todas las denuncias asociadas a Corrupción, Opacidad y Fraude deben ser reportadas por el canal de denuncias En la página WEB (www.hcup.gov.co) de la ESE en el menú Atención al Usuario, se ingresa por el enlace de PQRSFD, en la opción crear PQRSFD, se selecciona el apartado que indica Denuncias de corrupción/ SARLAFT – FPADM, y cualquier usuario

podrá radicar alguna denuncia con respecto a actos de corrupción que identifique en la ESE.

- ✓ Es deber de la ESE Hospital César Uribe Piedrahita y sus empleados, asegurar y acatar, el cumplimiento de las disposiciones y lineamientos que prohíben la realización de actos de Corrupción, Opacidad y Fraude.
- ✓ Gestionar los riesgos de Corrupción, Opacidad y Fraude, asociados a las actividades que se desarrollen en función del objeto social y al relacionamiento con los grupos de interés.
- ✓ La ESE Hospital César Uribe Piedrahita, se abstendrá de recibir o realizar donaciones que no tengan un fin lícito o sobre las cuales exista la sospecha que servirán para encubrir conductas de Corrupción, Opacidad y fraude, o para obtener ventajas en los negocios de la entidad.
- ✓ Todo el personal de la ESE Hospital César Uribe Piedrahita se debe capacitar obligatoriamente en el sistema de administración de riesgos de Corrupción, Opacidad y Fraude de forma anual.
- ✓ Se consagra el deber de los órganos de administración y de control, del Oficial de Cumplimiento, así como de todos los funcionarios, de asegurar el cumplimiento de los reglamentos internos y demás disposiciones relacionadas en Subsistema de Administración del Riesgo de Corrupción, la Opacidad y Fraude - SICOF.
- ✓ Los colaboradores de la ESE Hospital César Uribe Piedrahita deben informar de manera inmediata cualquier conflicto de intereses que vaya en contravía de los valores y principios corporativos, a fin de evitar daños y perjuicios a la organización; así mismo, informar la existencia de relaciones entre la entidad y terceras partes, empleados u otros individuos o grupos relacionados con la organización cuyos intereses puedan coincidir en la realización de alguna actividad conjunta (dualidad de interés y no conflicto).

- ✓ Los criterios de evaluación del riesgo de Corrupción, Opacidad y Fraude se definen de acuerdo con los controles existentes en el proceso al momento de la evaluación de los factores de riesgo. Para poder calificarlos y clasificarlos, se debe contemplar los ámbitos de riesgo, sus consecuencias, la probabilidad de que puedan ocurrir esas consecuencias y el impacto que le acarrearía al proceso y/o a la ESE en el evento de materializarse el riesgo.
- ✓ Todos los colaboradores de la ESE que omitan denunciar situaciones que impliquen un posible riesgo de corrupción, opacidad y fraude, configura un incumplimiento de la presente política y constituye una falta grave, sujeto a acción disciplinaria por parte de la ESE o la correspondiente empresa responsable de proveer el recurso humano.
- ✓ La ESE No establecerá ningún tipo de relación contractual con empleados, clientes y contrapartes que aparezcan relacionados en las listas de verificación vinculantes con procesos de investigación y señales de alerta asociados a riesgo de Corrupción, Opacidad y Fraude.
- ✓ La ESE Hospital César Uribe Piedrahita, garantiza la reserva y confidencialidad frente a los hechos que sean denunciados; así mismo, los denunciantes que realicen los reportes de conductas indebidas y faciliten información o participen en una investigación, estarán cubiertos por medidas de protección a represalias cuando así lo consideren. En tal caso, la ESE verificará la pertinencia de implementar medidas que permitan salvaguardar la integridad del denunciante (forma anónima).
- ✓ No ofrecemos, aceptamos o solicitamos regalos o atenciones, si se entiende o parece entenderse, como una obligación o un soborno (Política de regalos).
- ✓ Todos los terceros y de más partes interesadas, que se vinculen contractualmente con la ESE, serán responsables de proteger la

información a la cual acceden y procesen, para evitar su perdida, alteración, destrucción o uso indebido, mediante acuerdos de confidencialidad.

Adicionalmente se establece el procedimiento PR-01-01-003 PROCEDIMIENTO DE DENUNCIAS de corrupción, Opacidad o Fraude en la ESE Hospital César Uribe Piedrahita, donde se detalla claramente los canales para proceder ante cualquier caso de corrupción.

En cuanto a cualquier **Conflicto de Interés** que se presente por una acción u omisión, un interés financiero, político o personal, o una relación sentimental con otro empleado o un tercero, podría impedir directa o indirectamente, juicios y valoraciones independientes y objetivas, o podrían a llegar a motivar la toma de decisiones incorrectas en el ámbito profesional (Establecido en el Código de conducta, Buen Gobierno e integridad).

Entre los hechos que se suponen un conflicto de intereses se encuentra:

- ✓ Utilizar indebidamente información privilegiada o confidencial para obtener provecho de intereses individuales, propios o de terceros.
- ✓ No guardar y desproteger la reserva comercial e industrial de la entidad.
- ✓ Utilizar su posición en la ESE o su nombre para obtener para sí o para un tercero, tratamientos especiales en negocios particulares, con cualquier persona natural o jurídica que tenga alguna relación con la entidad.
- ✓ Demás hechos estipulados en el código de Conducta, Buen Gobierno e Integridad de la ESE.

Para garantizar cualquier irregularidad por conflicto de intereses el formato FO-01-01-019 DECLARACIÓN DE SITUACIONES DE CONFLICTO DE INTERESES, debe ser diligenciado por el funcionario o colaborador que realiza las acciones o actividades que pueden verse afectadas.

Es importante tener claros los siguientes conceptos en SICOF

Conflicto de intereses:

La omisión de reportar situaciones que impliquen un posible conflicto de intereses, así como omisión de la declaración si presenta o no conflicto de intereses mediante los canales establecidos por la ESE, configura un incumplimiento de la presente política y constituye una falta grave a las obligaciones reglamentarias del colaborador y quedará sujeto a acción disciplinaria por parte de la ESE.

Fraude:

Cualquier acto ilegal caracterizado por engaño o violación de confianza, los cuales no requieren la aplicación de amenaza de violencia o de fuerza física, es considerado un fraude.

Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes y servicios, para evitar pagos o para asegurarse ventajas personales o de negocio.

Corrupción:

Es la voluntad de actuar deshonestamente abusando del poder encomendado por la ESE Hospital César Uribe Piedrahita, a cambio de beneficios personales, ya sea de manera directa o indirecta y favorecimiento injustamente a terceros en contra de los intereses de la entidad; a su vez, la corrupción es el ofrecimiento, promesa u otorgamiento de un incentivo para influenciar una decisión u obtener una ventaja indebida para el beneficio propio, de la Compañía o de un tercero, con la que la ESE tenga relación contractual o comercial.

Opacidad

La opacidad es la carencia de prácticas claras, precisas, fácilmente discernibles y aceptadas. El entendimiento de este concepto se facilita en la medida en que se reconoce su opuesto, el ideal en el marco de la buena gobernanza, esto es, la transparencia.

La falta de transparencia no permite contar con información fiable, procesos y normas claras por parte de los funcionarios o entidades relacionadas.

Factores de Opacidad que pueden presentarse en la ESE:

- ✓ Concentración del Poder
- ✓ Desconocimiento de procesos y Procedimientos
- ✓ Excesiva discrecionalidad

Serán considerados como hechos de Corrupción y/o Soborno:

- ✓ Pago de un soborno a un funcionario para obtener una ventaja ilegítima frente a la competencia, con el fin de ganar un permiso o derecho de operación en un territorio, mercado o viabilizar un negocio.
- ✓ Pagos entregados a funcionarios para obtener certificados, agilizar pagos de terceros, trámites y otros tipos de servicios públicos y privados.
- ✓ Pagos por ocultar cualquier sobrecosto en la venta u ofrecimiento de medicamentos e insumos.
- ✓ Pagos por ocultar la falsificación de medicamentos e insumos y el suministro de medicamentos vencidos, sin perjuicio de las denuncias penales correspondientes

La corrupción es un fenómeno social que involucra tres elementos fundamentales:

A estos elementos pueden asociarse otros, que darían lugar a diferentes clases de corrupción.

A continuación, se presentan las principales categorías que se han desarrollado:

- ✓ Según la naturaleza del actor, la corrupción puede ser pública o privada. Si el poder o la confianza proviene del sector público, la corrupción es pública, así alguna de las partes involucradas pertenezca al sector privado; en cambio, cuando la corrupción se da exclusivamente en el sector privado es privada.
- ✓ Según la cantidad de actores involucrados y cuando el desvío se da por un ofrecimiento o exigencia del beneficio, la corrupción puede ser pluripersonal (al menos de dos) o de una sola persona, o unipersonal.

Acciones que Constituyen Actos de Corrupción

Con el fin de garantizar una gestión ética y transparente se prohíben las siguientes conductas:

Obtención de Ventajas Ilegitimas: Pago de un soborno a un funcionario para obtener una ventaja ilegítima frente a la competencia, con el fin de ganar un permiso o derecho de operación en un territorio, mercado o viabilizar un negocio.

Aceptar Dádivas, Regalos u Otro beneficio: Son beneficios entregados a funcionarios para obtener certificados, agilizar pagos de terceros, trámites y otros tipos de servicios públicos y privados. Los pagos de facilitación son sobornos que para la Organización están prohibidos, por cuanto va en contra de las políticas y normas estipuladas en el código de Conducta y Buen Gobierno y Política de regalos y atenciones.

En cuanto al Uso Indebido de la Información orientada a opacidad, es importante tener claro que los colaboradores de la ESE, deben salvaguardar la información confidencial de forma oral o escrita, independientemente del medio (teléfono, plataformas de comunicación como Teams, Zoom, correo electrónico, mensajes de texto, etc...), así mismo, deben considerar si el receptor tiene las funciones, atribuciones y/o autorizaciones requeridas para su uso y/o tratamiento. El uso inapropiado de todos los activos tangibles e intangibles del hospital, de acuerdo con las funciones y responsabilidades de cada uno de los empleados y/o directivos, así como propender por la protección de los activos contra pérdida, robo, abuso o uso no autorizado.

Se considera uso indebido de la información:

- ✓ Obtener información de uso exclusivo de la ESE Hospital César Uribe Piedrahita, por el medio que fuere sin la autorización respectiva, violando las medidas y niveles de seguridad de la información.
- ✓ Comercializar, y ofrecer inapropiadamente la información confidencial, de reserva, de propiedad intelectual que hacen parte del patrimonio de la ESE Hospital César Uribe Piedrahita.
- ✓ Modificar, eliminar o inutilizar programas de computador y software de propiedad de la ESE Hospital César Uribe Piedrahita.
- ✓ Duplicar, reproducir o comercializar programas de computador o software de propiedad y uso exclusivo de la ESE Hospital César Uribe Piedrahita (Ver Políticas de confidencialidad y de Seguridad de la Información).

Mecanismo para evitar el uso indebido de información

Los mecanismos para evitar el uso de información privilegiada o reservada se encuentran en las Políticas de Seguridad y confidencialidad de la Información donde se determina entre otros:

- ✓ Transmisión segura de la información
- ✓ Accesos seguros
- ✓ Firmas digitales
- ✓ Control de Acceso físico
- ✓ Ubicación y protección de los equipos
- ✓ Retiro y seguridad de equipos y medios de información fuera de las instalaciones

Malversación de Activos:

La ESE Hospital César Uribe Piedrahita debe asegurar el uso apropiado de todos sus activos tangibles e intangibles, de acuerdo con las funciones y responsabilidades de cada uno de los empleados, así como propender por la

protección de los activos contra pérdida, robo, abuso o uso no autorizado. La directriz de seguridad de la información debe establecer que la información solo puede ser accedida por los empleados, contratistas y vinculados con la ESE.

Así mismo, la información debe estar protegida contra alteraciones no autorizadas, realizadas con o sin intención, y debe estar disponible cuando sea requerida en los términos de calidad establecidos por la ESE. Durante el ciclo de vida de la información, la interacción con la misma debe dejar rastro de eventos relevantes como la creación, modificación, eliminación y acceso de acuerdo con los niveles de protección definidos.

Tipos de Malversación de Activos:

- ✓ Tomar dinero o activos de forma indebida, sin autorización.
- ✓ Uso inadecuado de los fondos de caja menor.
- ✓ Falsificar o alterar algún tipo de documento o registro, con el fin de obtener un beneficio individual o para un tercero.
- ✓ Realizar pagos no autorizados o incurrir en gastos que no estén debidamente soportados con documentos legales.

5.5.1. Generalidades acerca de los riesgos de corrupción

La gestión del riesgo la deben adelantar todas las entidades del orden nacional, departamental y municipal, anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.

Consolidación: La oficina de planeación, quien haga sus veces, o a la de dependencia encargada le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

Publicación: El mapa de riesgo de corrupción se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública

que establece el artículo 2. 1. 1. 2. 1. 4 del Decreto o 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación, además la entidad adelantara acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el mapa de riesgos de corrupción. Se dejará la evidencia del proceso de socialización y publicarse sus resultados.

Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

5.5.2. Valoración de riesgos de corrupción, opacidad y Fraude

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

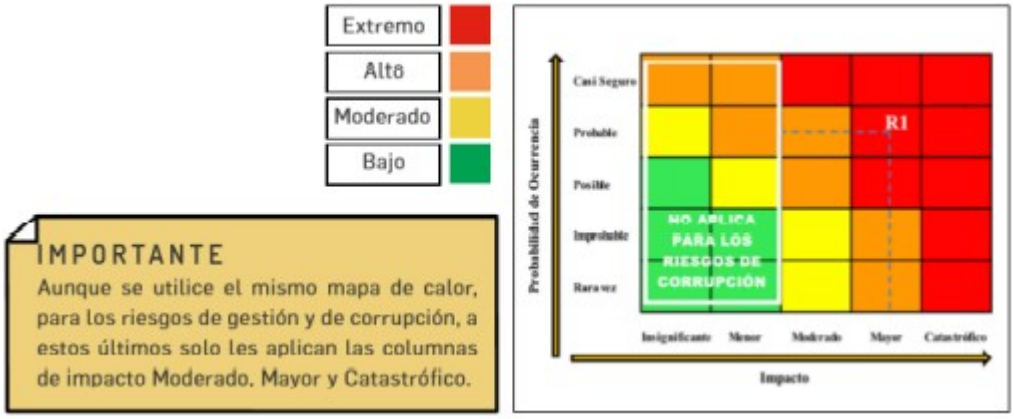
	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Criterios para calificar el impacto en riesgos de corrupción:

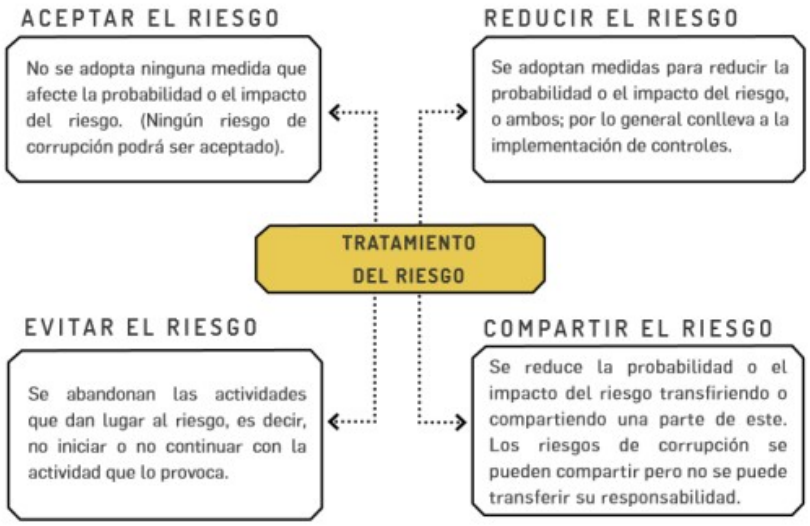
Nº	Pregunta Si el riesgo se materializa podría?	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad ?		
4	¿Afectar el cumplimiento de misión del sector al cual pertenece la Entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectados u reputación?		
6	¿Generar perdí da de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios ?		
8	¿Dar lugar al detrimento de cal i dad de vi da de la comunidad por la perdí da del bien o servicios o los recursos públicos?		
9	¿Generar perdí da de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios ?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales ?		
14	¿Dar lugar a procesos penales ?		
15	¿Generar perdí da de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional ?		
18	¿Afectar la imagen nacional ?		
19	¿Generar daño ambiental ?		

Para los riesgos de corrupción, Opacidad y Fraude, 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 insignificante y menor, que sí aplican para los demás riesgos. Por último ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.



Fuente: Secretaria de transparencia

En cuanto al tratamiento de los riesgso de corrupcion, opacidad o fraude se debe tener en cuenta lo siguiente:



ACEPTAR EL RIESGO: NUNCA PUEDEN SER ACEPATDOS

EVITAR EL RIESGO: Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades. 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: 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.

REDUCIR EL RIESGO: 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.

5.5.3. Tratamiento del riesgo – rol de la primera línea de defensa

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente su efectividad depende, de qué tanto se está logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control

5.5.4. Monitoreo de riesgos de corrupción, opacidad y fraude

Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para

este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, 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 de este documento.

5.5.5. Reporte de la gestión del riesgo de corrupción, opacidad y fraude

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 adecuado.

5.5.6. Seguimiento de riesgos de corrupción, opacidad y fraude

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

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 de los diez (10) primeros días del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

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.

En especial deberá adelantar las siguientes actividades:

- ✓ Garantizar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- ✓ Realizar seguimiento a la gestión del riesgo.
- ✓ Realizar 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 por parte del Oficial de cumplimiento de la ESE

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

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4) 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.

5.5.6.1. Estructura Organizacional y Responsabilidades dentro del subsistema de Riesgos de corrupción, Opacidad y fraude:

Las ESE establece y asignar funciones en relación con las distintas etapas y elementos del Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF. Así mismo, establece como mínimo las siguientes funciones a cargo de los órganos de dirección, administración y demás áreas de la entidad:

5.5.6.1.1. Junta Directiva

Sin perjuicio de las funciones asignadas en otras disposiciones, el Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF, de la ESE, contempla como mínimo las siguientes funciones a cargo de la Junta Directiva u órgano que haga sus veces:

a. Definir y aprobar las estrategias y políticas generales relacionadas con el SICOF, con fundamento en las recomendaciones del Oficial de Cumplimiento o persona encargada por la entidad para la ejecución del SICOF.

b. Adoptar las medidas necesarias para garantizar la independencia del Oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF y hacer seguimiento a su cumplimiento.

c. Aprobar el Manual de prevención de la Corrupción, la Opacidad y el Fraude y sus actualizaciones.

d. Hacer seguimiento y pronunciarse sobre el perfil de Corrupción, Opacidad y Fraude de la entidad.

e. Pronunciarse sobre la evaluación periódica del SICOF, que realicen los órganos de control.

f. Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SICOF.

g. Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el Oficial de Cumplimiento o persona encargada por la entidad para la ejecución del SICOF.

h. Conocer los informes relevantes respecto del SICOF, e impartir las órdenes necesarias para que se adopten las recomendaciones y correctivos a que haya lugar.

i. Efectuar seguimiento en sus reuniones ordinarias a través de informes periódicos que presente el oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF, sobre la gestión del mismo en la entidad y las medidas adoptadas para el control o mitigación de los riesgos más relevantes, por lo menos cada 6 meses.

j. Evaluar las recomendaciones relevantes sobre el SICOF, que formulen el oficial de cumplimiento o persona encargada por la entidad para la ejecución del mismo y los órganos de control interno, adoptar las medidas pertinentes, y hacer seguimiento a su cumplimiento.
k. Analizar los informes que presente el oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF respecto de las labores realizadas para evitar que la entidad sea utilizada como instrumento para la realización de actividades delictivas, actos de Corrupción, Opacidad o Fraude y evaluar la efectividad de los controles implementados y de las recomendaciones formuladas para su mejoramiento.

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

5.5.6.1.2. Representante legal

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

5.5.6.1.3. Oficial de Cumplimiento

Para el adecuado cumplimiento de la labor que corresponde al Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude – SICOF, así como a su mejoramiento continuo será delegado el oficial de cumplimiento o persona encargada por la entidad, sin que ello implique una sustitución a la responsabilidad que de manera colegiada le corresponde al máximo órgano social u órgano equivalente en la materia, desarrollando funciones de carácter eminentemente de asesoría y apoyo. El oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF, debe cumplir como mínimo con las siguientes condiciones:

a. Diseñar y someter a aprobación de la Junta Directiva u órgano que haga sus veces, el manual de prevención de la Corrupción, la Opacidad y el Fraude y sus actualizaciones.

b. Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva.

c. Diseñar y proponer para aprobación de la Junta Directiva o quien haga sus veces, la estructura, instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente sus Riesgos de prevención y detección de la Corrupción, la Opacidad y el Fraude, en concordancia con los lineamientos, etapas y elementos mínimos previstos en esta Circular.

d. Desarrollar e implementar el sistema de reportes, internos y externos, de prevención y detección de la Corrupción, la Opacidad y el Fraude de la entidad.

e. Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los Riesgos de Corrupción, Opacidad y Fraude medidos.

f. Establecer y monitorear el perfil de riesgo de la entidad e informarlo al órgano correspondiente, en los términos de la presente Circular.

g. Desarrollar los modelos de medición del riesgo de Corrupción, Opacidad y Fraude.

h. Desarrollar los programas de capacitación de la entidad relacionados con el SICOF.

i. Presentar un informe periódico, como mínimo semestral, a la Junta Directiva y al representante legal, sobre la evolución y aspectos relevantes del SICOF, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.

j. Establecer mecanismos para la recepción de denuncias (líneas telefónicas, buzones especiales en el sitio web, entre otros) que faciliten, a quienes detecten eventuales irregularidades, ponerlas en conocimiento de los órganos competentes de la entidad.

k. Informar al máximo órgano social u órgano equivalente sobre el no cumplimiento de la obligación de los administradores de suministrar la información requerida para la realización de sus funciones.

l. Estudiar los posibles casos de Corrupción, Opacidad y Fraude, dentro del ámbito de su competencia, para lo cual debe contar con la colaboración de expertos en aquellos temas en que se requiera y elaborar el informe correspondiente para someterlo a consideración del máximo órgano social.
m. Informar a la Superintendencia Nacional de Salud los posibles casos de Corrupción, Opacidad y Fraude que se lleguen a presentar a través de los canales dispuestos para tal fin.
n. Proponer al máximo órgano social programas y controles para prevenir, detectar y responder adecuadamente a los Riesgos de Corrupción, Opacidad y Fraude, y evaluar la efectividad de dichos programas y controles.
o. Poner en funcionamiento la estructura, procedimientos y metodologías inherentes al SICOF, en desarrollo de las directrices impartidas por el máximo órgano social, garantizando una adecuada segregación de funciones y asignación de responsabilidades.
p. Elaborar el plan anual de acción del SICOF y darle estricto cumplimiento.
q. Recomendar a la Junta directiva medidas preventivas y/o acciones ante organismos competentes (Judiciales y/o disciplinarlos) para fortalecer el SICOF.

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

El Oficial de cumplimiento o persona encargada por la entidad para la ejecución del SICOF, debe dejar constancia documental de sus actuaciones en esta materia, mediante memorandos, cartas, actas de reuniones o los documentos que resulten pertinentes para el efecto. Adicionalmente, debe mantener a disposición del auditor interno, el revisor fiscal y demás órganos de supervisión o control los soportes necesarios para acreditar la correcta implementación del SICOF, en sus diferentes elementos, procesos y procedimientos.

5.5.6.1.4. Revisoría Fiscal

Sin perjuicio de las funciones asignadas en otras disposiciones al Revisor Fiscal, éste debe elaborar un reporte al cierre de cada ejercicio contable, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude - SICOF.
A su vez, debe poner en conocimiento del Representante Legal los incumplimientos del SICOF, sin perjuicio de la obligación de informar sobre ellos a la Junta Directiva u órgano que haga sus veces.

5.5.6.1.5. Control Interno

Sin perjuicio de las funciones asignadas en otras disposiciones a la Auditoría Interna, o quien ejerza el control interno, ésta debe evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SICOF, con el fin de determinar las deficiencias y sus posibles soluciones. Así mismo, deberá informar los resultados de la evaluación al representante legal o Junta Directiva.

5.5.6.2. Capacitación:

La ESE Hospital César Uribe Piedrahita, contará con un plan de capacitación del Programa de Corrupción, Opacidad, y Fraude, que harán parte del Plan Integral de capacitaciones, liderado por Gestión del Talento Humano Humana, con una Periodicidad Anual.
Todos los empleados vinculados directamente y por empresas contratadas, recibirán capacitación anualmente sobre los temas relacionados con Corrupción, Opacidad, y Fraude, para los nuevos empleados, se capacitarán en la inducción.

El área de formación informará mensualmente el cumplimiento de las capacitaciones, resultado de evaluaciones, planillas de asistencia en Corrupción, Opacidad, y Fraude, con el fin que el Oficial de Cumplimiento, pueda ajustar el plan de capacitación; de igual forma el área de formación dará resguardo a los soportes de capacitación referente a Corrupción, Opacidad, y Fraude.
De toda capacitación quedará soporte escrito en el que se relacionen como mínimo, el (los) tema (s) tratado (s) y quede identificado el empleado que recibió tal capacitación (nombre, apellidos, número del documento de identificación, cargo, gerencia, dirección o área y firma).

Dadas las condiciones de salud pública y/o disposiciones del Gobierno Colombiano que impida la realización de eventos presenciales, se dará uso de herramientas tecnologías que permitan la divulgación, socialización y capacitación relacionada con Corrupción, Opacidad, y Fraude. Para dejar constancia, se diligenciará de manera digital la asistencia a la conferencia y se guardará como evidencia de la participación de colaboradores y/o terceros.

La ESE capacitará y entrenará a sus empleados en los procesos de inducción, programas de refuerzo y actualización, de acuerdo con los resultados de las evaluaciones reportados por el área de Gestión Humana. Las capacitaciones están enfocadas pedagógicamente a los empleados en forma detallada, en qué

consiste la Corrupción, Opacidad, y Fraude, políticas, la normatividad vigente, las señales de alerta, cómo detectar este tipo de actividades. Adicionalmente permite dar a conocer las obligaciones y responsabilidades que tienen los empleados frente a la Corrupción, Opacidad, y Fraude. En caso de ser necesarias, se realizarán visitas de seguimiento y retroalimentación sobre aquellas oficinas y/o procesos que presentaron incumplimientos representativos sobre asuntos relacionados con Corrupción, Opacidad, y Fraude, validando con cada empleado responsable, el cumplimiento de los controles establecidos.

5.5.6.3. Colaboración con la Justicia y Autoridades Administrativas

La información requerida por las autoridades judiciales y administrativas en temas relacionados con el SICOF, serán analizadas por el Oficial de Cumplimiento para ser asignadas con las áreas competentes y será la encargada de compilar y proyectar la respuesta para ser enviada al área jurídica, quien hará la revisión previa él envió.

5.6. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI) , el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

5.6.1 Identificación de los activos de seguridad de la información:

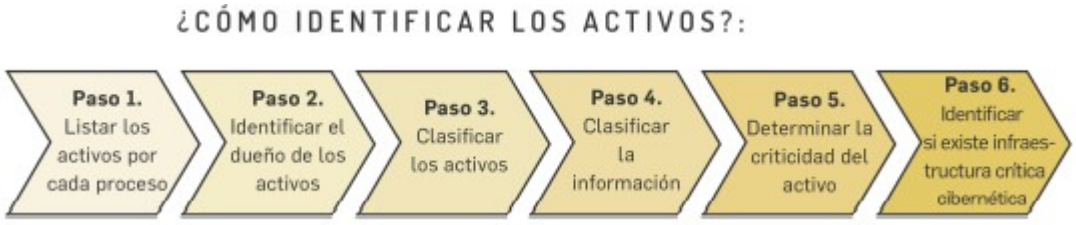
Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	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).

-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

Pasos para identificación de activos de información:



Para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas”.

A continuación se muestra un ejemplo de activos:

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el *front office* de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

5.6.2 Identificación del riesgo de seguridad de la información:

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- ✓ Pérdida de la confidencialidad
- ✓ Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el *Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:*

Tabla de amenazas y vulnerabilidad ce acuerdo con el tipo de activo:

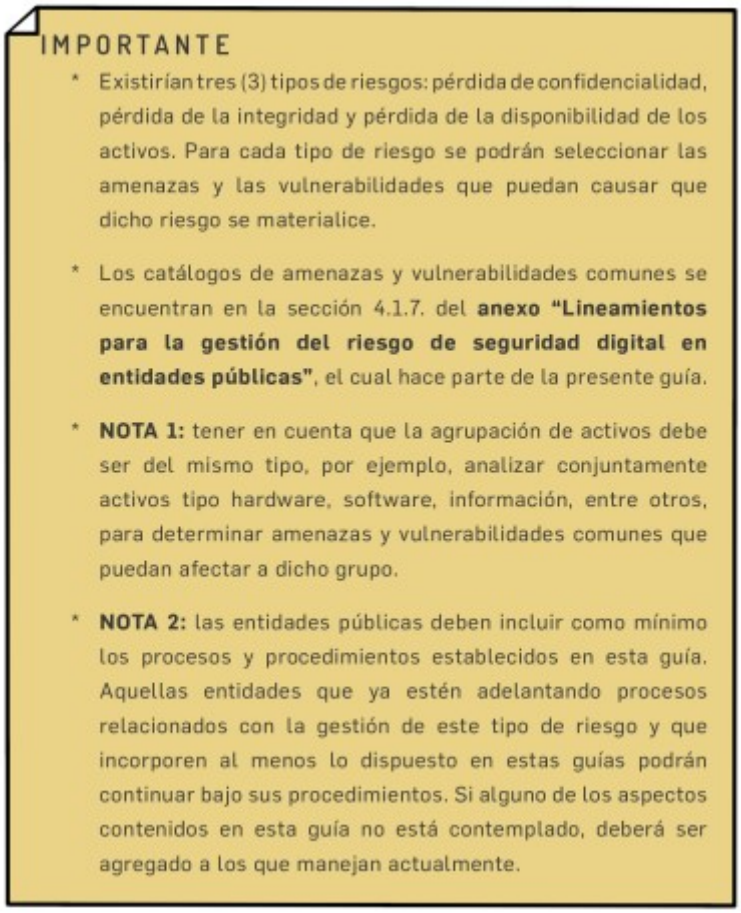
Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min T IC, 2018.

A continuación se observa un ejemplo de identificación del riesgo sobre un activo como es la base de datos de nómina.

Seleccionar las vulnerabilidades asociadas a la amenaza identificada

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018

5.6.3. Valoración del riesgo

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas anteriormente, la cual se retoma a continuación:

Probabilidad:

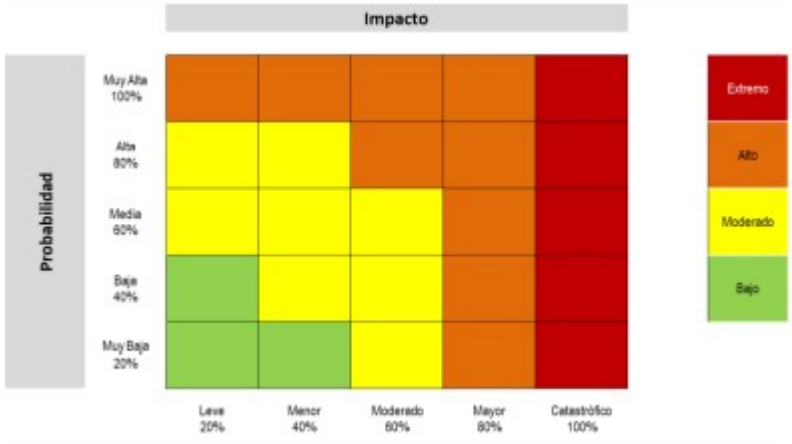
	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Impacto:

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor establecida, que se retoma a continuación:

La matriz de calor es la misma definida para los demás subsistemas:



La Valoración del riesgo en seguridad de la información:

IMPORTANTE

Cada entidad deberá adaptar los criterios a su realidad.
El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

RIESGO	ACTIVO	AMENAZA	VULNERABILI-DAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confiden-cialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

IMPORTANTE:
La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

5.6.4. Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos. Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Controles para riesgos de seguridad de la información:

Procedimientos operacionales y responsabilidades	**Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información**
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

A continuación se brinda un ejemplo de un Formato mapa riesgos seguridad de la información:

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Pérdida de la integridad**	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	**Probable**	**Menor**	**Moderado**	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

En este ejemplo el responsable de control fue la oficina de TI, sin embargo existen actividades para el área de personal, recursos fisicos o cada oficina en particular. El análisis de riesgo determinará los controles y los responsables en cada caso.

6. DOCUMENTOS DE REFERENCIA

1. Circular externa 009 de abril de 2016 de la superintendencia Nacional
2. Circular externa 4-5 de septiembre de 2021 de la superintendencia Nacional
3. Circular externa 5-5 de septiembre de 2021 de la superintendencia Nacional.
4. ICONTEC Internacional. (2018). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).
5. PO-01-01-001 POLÍTICA DE ADMINISTRACIÓNDEL RIESGOS

7. CONTROL DE CAMBIOS

VERSION	FECHA	DESCRIPCION DEL CAMBIO	RESPONSABLE
01	29/08/2022	Elaboración del documento	Evelin Ruth Morales Osorio – Oficial de cumplimiento.