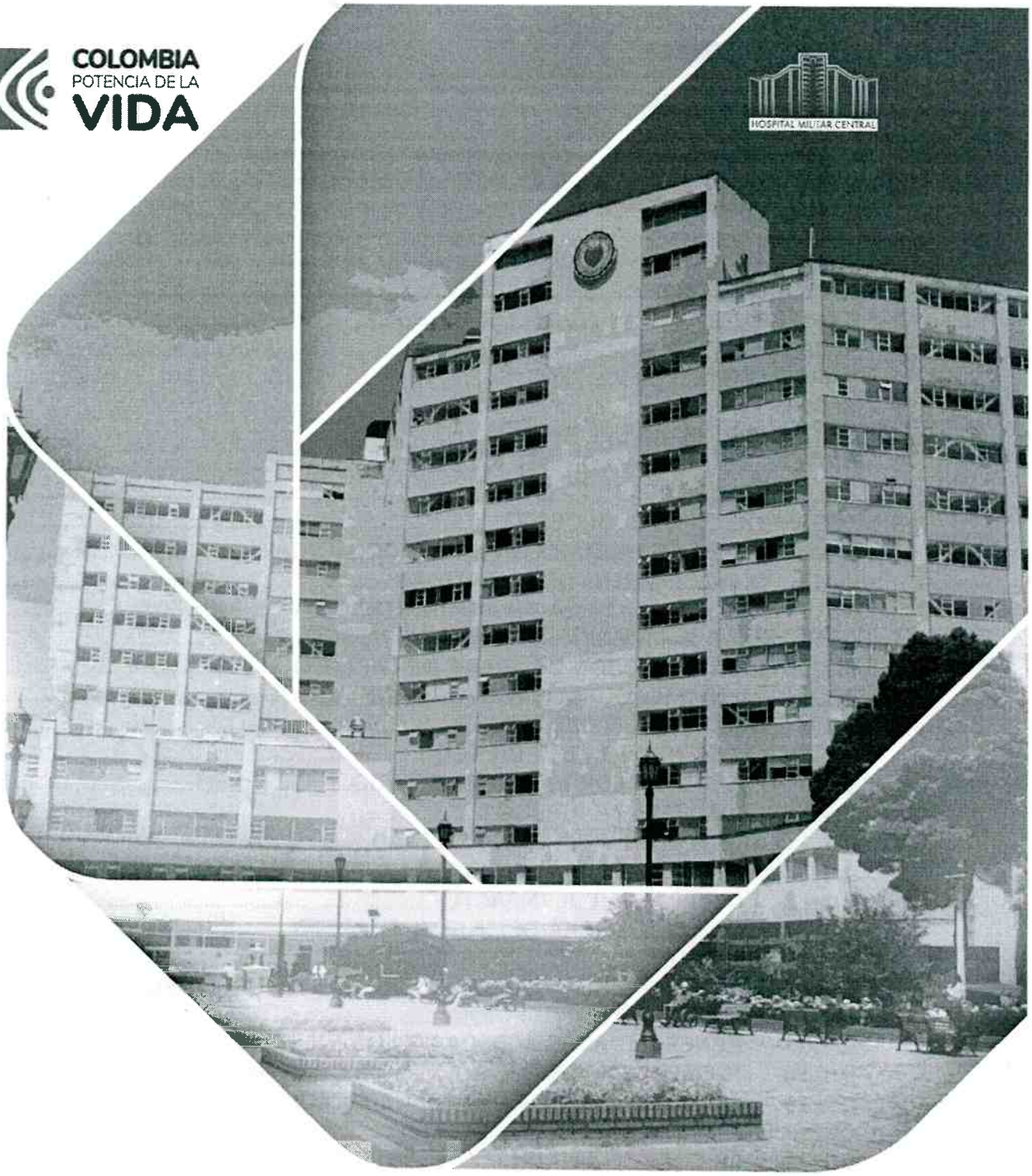
COLOMBIA POTENCIA DE LA VIDA



Oficina Asesora de Planeación
30 de noviembre de 2023 - PL-OAPL-PO-01_V5
HOSPITAL MILITAR CENTRAL - HOMIL

POLÍTICA DE OPERACIÓN PARA LA ADMINISTRACIÓN DEL RIESGO EN EL HOSPITAL MILITAR CENTRAL

TABLA DE CONTENIDO

1 INTRODUCCIÓN

Con base en el Modelo Integrado de Planeación y Gestión - MIPG y de acuerdo con los lineamientos definidos en las dimensiones de Direccionamiento Estratégico y Planeación, Gestión con Valores para Resultados y Control Interno, se dictan directrices para implementar la presente política alineada con los objetivos estratégicos de la entidad, la cual establece la metodología para tratar y manejar los riesgos basados en su valoración, permitiendo la toma adecuada de decisiones por la Alta Dirección.

El **Hospital Militar Central** en concordancia con el proceso de fortalecimiento organizacional determina la Administración del Riesgo como parte integral de la gestión de la entidad con el fin de favorecer el desarrollo, la sostenibilidad, el logro de los objetivos institucionales y dando cumplimiento a las directrices de la circular externa 20211700000004-5 de la Superintendencia Nacional de Salud, del Modelo Integrado de Planeación y Gestión – MIPG, del Plan Anticorrupción y de Atención al Ciudadano - PAAC, del esquema de seguridad de las líneas de defensa; definido en el Modelo Estándar de Control Interno – MECI, de la guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP V.6, al modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital. El presente documento establece lineamientos y parámetros claros y necesarios para la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos que puedan afectar la misión institucional, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales.

2 OBJETIVO

Establecer un marco de referencia general que involucre a todos los servidores públicos y contratistas del **HOSPITAL MILITAR CENTRAL** para la adecuada gestión del riesgo, por medio de la identificación de acciones de control, respuestas oportunas y estrategias institucionales frente a las diferentes situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de los objetivos institucionales.

PROCESOS	OBJETIVO ESTRATÉGICO.	ACTIVIDADES ESTRATÉGICAS	INDICADORES ESTRATÉGICOS
Apoyo Asistencial y farmacéutico. Atención Ambulatoria. Atención Hospitalaria. Comunicaciones y Atención al Usuario. Gerencia y Buen Gobierno.	Asegurar la atención integral para la prestación de servicios de salud.	4	30
Gestión del Conocimiento. Talento Humano.	Formar talento humano en salud y generar conocimiento científico.	2	9
Planeación. Gestión Logística. Gerencia y Buen Gobierno. Planeación. Gestión Jurídica. Comunicaciones y Atención al Usuario. Tecnologías de la Información. Gestión Documental.	Fortalecer la gestión por procesos y cultura de mejoramiento.	1	24
Gestión de Adquisiciones. Gestión Financiera.	Optimizar la gestión Financiera.	1	8

Nota*: Las tareas e indicadores estratégicos contienen en su formulación los atributos de las características SMART (Específico, medible, alcanzable, relevante y proyectados en el tiempo), los cuales se encuentran detallados en el Plan de Acción Institucional.

Desglose características SMART

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: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

3 ALCANCE

La política de operación para la administración del riesgo es aplicable a todas las dependencias, procesos, proyectos y planes institucionales, con el fin de identificar, analizar, valorar, monitorear y dar tratamiento a los riesgos identificados durante el desarrollo de la gestión planificada y a todos los servidores públicos y contratistas en el ejercicio de sus funciones y obligaciones.

4 MARCO LEGAL

A continuación, se relaciona la normativa interna y externa la cual regirá el documento, de acuerdo a la siguiente tabla:

TIPO	No.	FECHA EXPEDICIÓN	ORIGEN	EMISOR	DESCRIPCIÓN
Ley	87	1993	Externo	Congreso de la República.	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
Ley	1474	2011	Externo	Congreso de la República.	Artículo 73. Cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos... Parágrafo. En aquellas entidades donde se tenga implementado un sistema integral de administración de riesgos, se podrá validar la metodología de este sistema con la definida por el Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción."
Decreto	1083	2015	Externo	Departamento Administrativo de la Función Pública.	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Decreto	124	2016	Externo	Departamento Administrativo de la Presidencia de la República.	Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".
Decreto	1499	2017	Externo	Departamento Administrativo de la Función Pública.	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
NTC - ISO	31000	2018	Externo	Icontec.	Gestión del Riesgo

TIPO	No.	FECHA EXPEDICIÓN	ORIGEN	EMISOR	DESCRIPCIÓN
Guía	V. 4	2018	Externo	Departamento Administrativo de la Función Pública.	Guía para la administración del riesgo y el diseño de controles en entidades públicas,
Guía	V.5	2020	Externo	Departamento Administrativo de la Función Pública.	Guía para la administración del riesgo y el diseño de controles en entidades públicas.
Circular Externa	20211700000004-5	2021	Externo	Superintendencia Nacional de Salud	Por la cual se imparten instrucciones generales relativas al código de conducta y de buen gobierno organizacional, el sistema integrado de gestión de riesgos y a sus subsistemas de administración de riesgos.
Guía	V.6	2022	Externo	Departamento Administrativo de la Función Pública.	Guía para la administración del riesgo y el diseño de controles en entidades públicas. Se incluye capítulo específico sobre riesgo fiscal.
Plan Nacional de Desarrollo	2022 - 2026	2023	Externo	Departamento Nacional de Planeación.	Sentar las bases para que el país se convierta en un líder de la protección de la vida, a partir de la construcción de un nuevo contrato social que propicie la superación de injusticias y exclusiones históricas, la no repetición del conflicto, el cambio de nuestra forma de relacionarnos con el ambiente, y una transformación productiva sustentada en el conocimiento y en armonía con la naturaleza.

5 GLOSARIO

CONCEPTOS BÁSICOS RELACIONADOS CON LA GESTIÓN DEL RIESGO.

A continuación, se relacionan una serie de conceptos necesarios para la comprensión de la metodología que se desarrolla a partir del paso 1 política de administración del riesgo, hasta el paso 3 valoración del riesgo.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.	**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 o 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 diligencia. Sus actuaciones se cumplirán en interés de la sociedad, teniendo en cuenta los intereses de sus asociados, y en el cumplimiento de su función, deben realizar como mínimo las expresadas en el artículo 23 de la mencionada Ley.	**Administración del riesgo:** Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos institucionales.	**Análisis de Riesgos:** Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.
Atención en salud: Servicios o tecnologías en salud suministrados a los individuos y a la comunidad para promover, mantener, monitorizar o restaurar el estado de salud.	**Apetito del 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	**Categorías de riesgos prioritarios:** Agrupadores de distintos tipos de riesgos en torno a un elemento común, prioritarios para fines de supervisión definidos por la SNS.	**Causas:** Medios, circunstancias, situaciones o agentes generadores del evento.

	del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.	Cabe resaltar que (el HOSPITAL MILITAR CENTRAL) debe gestionar todos los riesgos que se presenten dentro de su operación, y dependerá de la discrecionalidad y organización que cada entidad les quiera dar para su tratamiento. Sin embargo, deberán contemplar como mínimo, los siguientes riesgos: Riesgo en Salud, Riesgo Actuarial; Riesgo de Crédito, Riesgo de Liquidez, Riesgo de Mercado de Capitales, Riesgo Operacional, Riesgo de Grupo y Riesgo de Lavado de Activos y Financiación del Terrorismo.	
Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.	**Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.	**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.	**CICCI:** Comité Institucional de Coordinación de Control Interno.
CGDI: Comité de Gestión y Desempeño Institucional.	**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,	**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. **Nota:** Tratándose de riesgo fiscal, el impacto siempre será económico	**Contingencia:** Posible evento futuro, condición o eventualidad.

	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.	y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.	
Controles: Medidas prudenciales, preventivas y correctivas que ayudan a contrarrestar la exposición a los diferentes riesgos. Entre estas se encuentra la implementación de políticas, procesos, prácticas u otras estrategias de gestión.	**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 re procesos.	**Corrupción:** Uso del poder para desviar la gestión de lo público hacia el beneficio privado.
Crisis (Emergencia): Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.	**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	**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.	**Establecimiento del Contexto:** Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.

	contar con una estructura, unas políticas y unos procedimientos ejercidos por toda la organización (desde la Junta Directiva y la Alta Gerencia, hasta los propios empleados), los cuales pueden proveer una seguridad razonable en relación con el logro de los objetivos de la entidad.		
Evento: Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas, las actividades de ruta crítica de los proyectos de inversión y las actividades críticas de control de los procesos.	**Evento de pérdida:** Son las situaciones que generan pérdidas a las entidades al exponerse a cualquier riesgo.	**Factibilidad:** Presencia de factores internos y externos que pueden propiciar el riesgo.	**Factibilidad:** Presencia de factores internos y externos que pueden propiciar el riesgo.
Frecuencia: Periodicidad con que ha ocurrido un evento.	**Gestión del riesgo:** Proceso efectuado para proporcionar un aseguramiento razonable con respecto al logro de los objetivos institucionales. 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 la entidad.	**Gestión del Riesgo Fiscal:** Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).	**Gestión Integral del Riesgo en Salud – GIRS:** Es una estrategia transversal de la Política de Operación para la Administración del Riesgo en el Hospital Militar Central, que se establece en la articulación e interacción de los agentes del sistema de salud para identificar, evaluar, medir, intervenir y llevar a cabo el seguimiento y monitoreo de los riesgos para la salud de las personas, familias y comunidades.

Identificación del Riesgo: Descripción de la situación no deseada.	**Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.	**Líneas de Defensa:** Proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.	**Mapa de Riesgos:** Documento que resume los resultados de las actividades de gestión del riesgo.
MIPG: Modelo Integrado de Planeación y Gestión.	**MECI:** Modelo Estándar de Control Interno. Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.	**OCIN:** Oficina de Control Interno.	**Pérdidas:** Cuantificación económica que representa la materialización de un evento de riesgo, donde se incluyen los gastos derivados de su atención.
Perfil de Riesgo: Resultado consolidado de la medición de los riesgos a los que se ve expuesta la entidad.	**Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.	**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, influyendo su volumen de negocios, y su situación general. Esta puede variar por factores tales como el desempeño, escándalos, menciones en prensa, entre otros.	**Riesgo:** Efecto que se causa sobre los objetivos de la entidad, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.	**Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).	**Riesgo en salud:** Probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo, que puede ser también el empeoramiento de una condición previa o la necesidad de requerir más consumo de bienes y servicios que hubiera podido evitarse.	**Riesgo Fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta política, el evento potencial es equivalente a la causa raíz.
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.	**Seguridad del paciente:** Es el conjunto de elementos estructurales, procesos, instrumentos y metodologías basadas en evidencia científicamente probadas que propenden por minimizar el riesgo de sufrir un evento adverso en el proceso de atención de salud, o de mitigar sus consecuencias.	**SVE:** Suite Visión Empresarial, aplicativo para la gestión de planeación, indicadores y riesgos.
TIC: Tecnologías de la Información y las Comunicaciones.	**Tratamiento:** Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.	**Valoración:** Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.	**Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6 GESTIÓN GENERAL DEL RIESGO

La gestión general del riesgo se define como el proceso de identificar, analizar y cuantificar las probabilidades de ocurrencia de eventos no deseados, pérdidas y efectos secundarios que se puedan presentar en la entidad, afectando la misionalidad y el cumplimiento de los objetivos estratégicos.

El sistema general de gestión de riesgos del Hospital Militar Central está compuesto por los siguientes componentes:

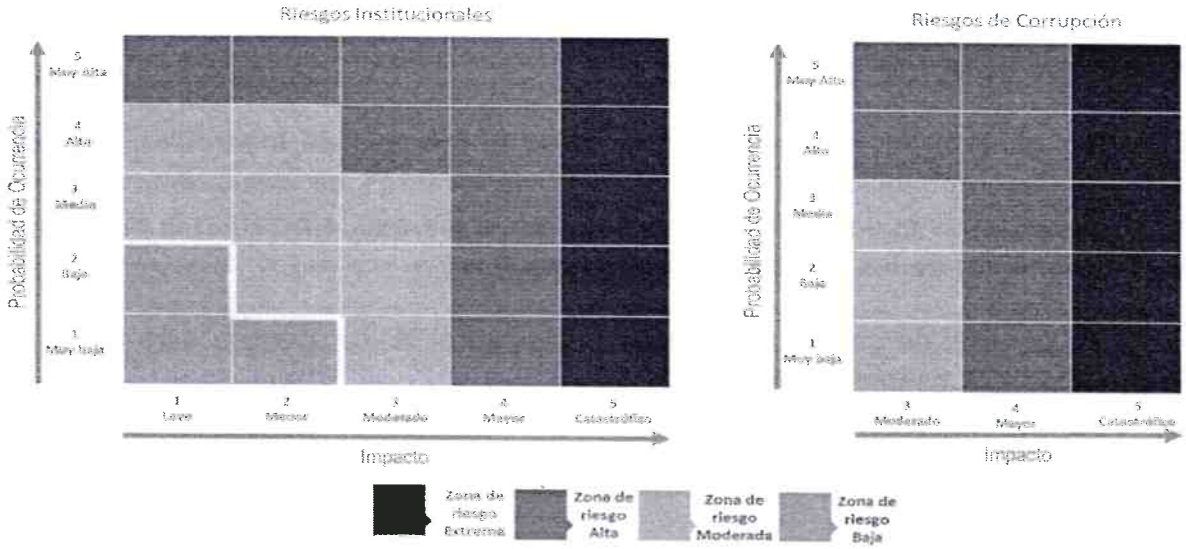
- Riesgos de Gestión – Operacional.
  - Riesgo Fiscal.
  - Riesgo Actuarial.
  - Riesgo de Crédito.
  - Riesgo de Liquidez.
  - Riesgo Reputacional.
  - Riesgos de Seguridad de la Información.
  - Riesgos asociados a trámites del HOMIL.
- Riesgos de Corrupción – Fraude Interno.
- Riesgos de seguridad del paciente.
- Riesgos relacionados con Lavado de Activos y Financiación del Terrorismo.

7 NIVELES DE ACEPTACIÓN DEL RIESGO

Acorde con los riesgos residuales definidos por los líderes de procesos y socializados en el Comité Institucional de Gestión y Desempeño y Comité de Coordinación de Control Interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

El **Hospital Militar Central** determina que para los riesgos residuales de gestión y seguridad digital que se encuentren en zona de riesgo baja y media, está dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

8 ROLES Y RESPONSABILIDADES

Las responsabilidades están definidas mediante el esquema de líneas de defensa y en el Hospital Militar Central se acogen de acuerdo a la siguiente tabla:

LÍNEA DE DEFENSA	RESPONSABLES	RESPONSABILIDAD FRENTEAL RIESGO
	Staff Directivo. Comité de Gestión y Desempeño Institucional.	• Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Recomendar mejoras a la política de operación para la administración del riesgo. • Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.
Línea Estratégica	Comité institucional de coordinación de control interno.	• Aprobar la política de administración del riesgo previamente estructurada por parte de la Oficina Asesora de Planeación, como segunda línea de defensa en la entidad; revisar y 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. • Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Analizar los riesgos, vulnerabilidades y amenazas 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 institucionales de la entidad.
Primera Línea	A cargo de los gerentes públicos – Subdirectores y Jefes de Oficina. Líderes de los procesos, programas y proyectos de la entidad. Jefes de Unidad.	• Asegurar que al interior de sus grupos de trabajo se reconozca el concepto de "Administración de Riesgo" la política, metodología y marco de referencia de Función Pública aprobado por la línea estratégica. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar el cumplimiento de los objetivos estratégicos, objetivos del proceso, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgos del proceso a cargo. • Identificar cuando se requiera, nuevos riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, objetivos del proceso, programas, proyectos y planes asociados a su proceso. • Informar a la Oficina Asesora de Planeación (segunda línea) sobre la identificación de nuevos riesgos, con el objetivo de dar continuidad a la metodología establecida en la entidad y posterior aprobación por parte del Comité Institucional de Gestión y Desempeño. • Elaborar y enviar propuesta de los nuevos riesgos identificados por el área y proceso responsable, a la Oficina Asesora de Planeación para revisión y análisis metodológico, dando cumplimiento a los lineamientos definidos por la entidad en materia de administración de riesgos. • Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, gestión, reporte de acciones de autocontrol, reporte del monitoreo y socialización de los riesgos al interior de los grupos de trabajo. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Revisar el adecuado diseño y 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 seleccionados para el tratamiento de los riesgos identificados. • Registrar en el formato **CÓDIGO: PL-OAPL-PR-05-FT-01** las acciones de autocontrol realizadas frente a cada

		riesgo en el periodo de reporte, de acuerdo a los controles y periodicidades definidas en el mapa de riesgos por proceso. • Señalar en la matriz del monitoreo al mapa de riesgos, si el riesgo se materializó o no se materializó. **MATERIALIZACIÓN DE RIESGOS** • Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados que puedan afectar el cumplimiento de los objetivos, programas, proyectos y planes de los procesos a cargo, de acuerdo a las periodicidades definidas por la entidad. (Monitoreo al mapa de riesgos). • Frente a cada riesgo materializado, se deberán diligenciar las celdas correspondientes al "Plan de manejo y/o mitigación del riesgo en el formato CÓDIGO: PL-OAPL-PO-FT-01 - SEGUIMIENTOS Y MONITOREO MAPA DE RIESGOS. • Diligenciar el ***"plan de manejo y/o mitigación del riesgo"*** en el formato **CÓDIGO: PL-OAPL-PO-FT-01 - SEGUIMIENTOS Y MONITOREO MAPA DE RIESGOS,** para cada uno de los riesgos materializados. • "Si se materializó el riesgo, describa brevemente el hecho y especifique el área y/o servicio en donde tuvo lugar" • "Descripción numérica ¿Cuántos hechos se presentaron?" • Realizó análisis "Causa –Raíz". ¿Si – No? • Descripción del Análisis. • Acciones desarrolladas para mitigar el riesgo materializado. • Responsable de la ejecución y cumplimiento del plan. • Registrar la fecha y plazo de ejecución del plan de manejo y/o mitigación del riesgo. • Registros / Evidencias. • Una vez diligenciado el monitoreo al mapa de riesgos en el formato definido por la entidad, este deberá ser reportado y cargado en la plataforma SVE, e indicar si algún riesgo tuvo materialización; de ser así, se procederá a realizar el registro de materialización del evento en la misma plataforma. • Revisar y hacer seguimiento a las acciones establecidas en el plan de manejo y/o mitigación del riesgo establecido para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces. • En caso de la materialización de un riesgo no identificado, gestionarlo, con el acompañamiento de la Oficina Asesora de Planeación, e incluirlo en el mapa de riesgo institucional.

		• Revisar el monitoreo al mapa de riesgos antes del cargue en el aplicativo, garantizando la veracidad de la información reportada dentro de los plazos establecidos. • Cargar el reporte del monitoreo al mapa de riesgos en la SVE dentro de los plazos establecidos. • Garantizar el repositorio, custodia y disposición permanente de las evidencias de la ejecución de los controles establecidos en el mapa de riesgos. • Considerar y tener en cuenta las recomendaciones plasmadas en los informes de las auditorías realizadas por la Oficina de Control Interno.
Segunda Línea	Jefe Oficina Asesora de Planeación. Área Gestión de Calidad.	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del CICCI. • Capacitar al grupo de trabajo de cada dependencia en la herramienta SVE para la gestión del riesgo. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa, realizar recomendaciones y seguimiento para el fortalecimiento de estos. • Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. • Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad. • Hacer seguimiento al plan de acción de tratamiento del riesgo, esto dependerá del tratamiento establecido, si es Aceptar no se requieren acciones adicionales, en caso de escoger Reducir (mitigar) se deben diligenciar las acciones que se adelantarán como complemento a los controles establecidos, no necesariamente son controles adicionales. Para Reducir (compartir), es viable diligenciar la acción que deriva de esta (ejemplo póliza seguros, tercerización), indicando información relevante. • Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para aprobación y seguimiento ante el CGDI. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Acompañar y orientar metodológicamente a los líderes de proceso en la identificación de nuevos riesgos que puedan

		afectar el cumplimiento de los objetivos estratégicos y del proceso. • Coordinar con los líderes de proceso la designación del responsable de realizar el reporte de seguimiento a los riesgos, controles, acciones de autocontrol y planes de acción en el aplicativo SVE. • Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. • Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos. • Socializar y publicar en la página web e intranet el mapa de riesgos institucional y sus actualizaciones. • La Oficina Asesora de Planeación o quien haga sus veces, deberá dar a conocer a los servidores públicos y contratistas de la entidad el mapa de riesgos de gestión y de corrupción antes de su publicación. Para lograr este propósito se deberán diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de gestión y de corrupción. Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos gestión y de corrupción. • Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Revisar las acciones y planes de mejora y/o mitigación del riesgo establecido para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y logar el cumplimiento a los objetivos. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe, plasme acciones de autocontrol y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.

		• Socializar el informe de monitoreo de riesgos los miembros del Comité Institucional de Coordinación de Control Interno. • Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean gestionados por la primera línea de defensa. • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos en el CICCI. • Revisar metodológicamente el diligenciamiento del monitoreo al mapa de riesgos reportado por los jefes de unidad o líderes de proceso en el aplicativo – SVE dentro de los plazos establecidos, y dar continuidad al flujo de aprobación. *La verificación de evidencias de la ejecución de los controles está a cargo de la Oficina de Control Interno)
Segunda Línea	Jefes de Oficina. Jefes de Unidad. Jefes de Servicios. Supervisores de Contrato.	• Presentar el mapa de riesgos del proceso desarrollado en las mesas de trabajo a la primera línea para la aprobación y visto bueno. • Socializar y comunicar, al interior de sus procesos, la política de operación para la administración del riesgo, el mapa de riesgos y los resultados del seguimiento. • Monitorear los riesgos identificados y aplicar los controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Registrar las acciones de autocontrol realizadas de acuerdo a la periodicidad establecida en la metodología, con el objetivo de mitigar la materialización de los riesgos. • Realizar el seguimiento al mapa de riesgos de su proceso en los plazos definidos. • Reportar en el módulo de riesgos del aplicativo SVE el registro de los avances en la gestión del riesgo. • Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Implementar las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • La Oficina Asesora Jurídica - OFAJ, tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. • Considerar y tener en cuenta las recomendaciones plasmadas en los informes de las auditorías realizadas por la Oficina de Control Interno.

		• Comunicar oportunamente a la Oficina Asesora de Planeación sobre la materialización de riesgos en cumplimiento del artículo 4º de la Ley 1150 de 2007 "De la distribución de riesgos en los contratos estatales. Los pliegos de condiciones o sus equivalentes deberán incluir la estimación, tipificación y asignación de los riesgos previsibles involucrados en la contratación.- supervisores de contrato.
Tercera línea	Oficina de Control Interno	• Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. • Asesorar a las áreas y dependencias en la identificación y prevención de riesgos. (Tomado de matriz de responsabilidad y autoridad del DAPF). • 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. • Incluir el seguimiento al mapa de riesgos en el Plan Anual de Auditoria y reportar los resultados al CICCI. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Realizar el seguimiento a los riesgos de gestión, seguridad digital y corrupción y la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en las áreas en los diferentes niveles de operación de la entidad. • Supervisar en coordinación con los demás responsables de la segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones de autocontrol pertinentes para reducir la probabilidad o impacto de los riesgos. • Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser gestionado con el acompañamiento de la Oficina Asesora de Planeación y ser incluido en el mapa de riesgo institucional. • Realizar seguimiento y verificación de las evidencias de la ejecución de los controles definidos en el mapa de riesgos institucional. • Hacer seguimiento a los controles establecidos por la primera línea de defensa, acorde con la información suministrada por los líderes de procesos.

		• Hacer seguimiento al monitoreo del mapa de riesgos en la Suite Visión Empresarial – SVE y evidencias de la ejecución de los controles definidos, dentro de los plazos establecidos. • Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de manejo y/o mitigación del riesgo y realizará el seguimiento de acuerdo a lo establecido en la Política de Riesgos. • Presentar al Comité Institucional de Coordinación de Control Interno el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en las áreas en los diferentes niveles de operación de la entidad. • Recomendar mejoras a la política de operación para la administración del riesgo.

De igual manera, la ***Oficina Asesora de Planeación*** lleva a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Comunicar a la entidad la política y el mapa de riesgos institucional y realizar las gestiones para su publicación en la página web e intranet de la entidad.
- Socializar a líderes de proceso 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 para el reporte y cargue del mapa de riesgos en la herramienta Suite Visión Empresarial –SVE.
- Liderar las mesas de trabajo de identificación del riesgo.
- Verificar que los controles estén definidos conforme a los requerimientos de la metodología.
- Consolidar el mapa de riesgos institucional con la información presentada por los líderes de proceso, construida en las mesas de trabajo.
- Revisar que el cargue de información en la SVE esté acorde con lo aprobado.

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

- Verificar las acciones preventivas de acuerdo con la periodicidad definida.
- Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación.

- Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir.
- Comunicar al equipo de trabajo los resultados de la gestión del riesgo.
- Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento.
- Garantizar la generación, repositorio, custodia y disposición permanente de las evidencias de la ejecución de los controles establecidos en el mapa de riesgos.

Los **servidores en general** deben:

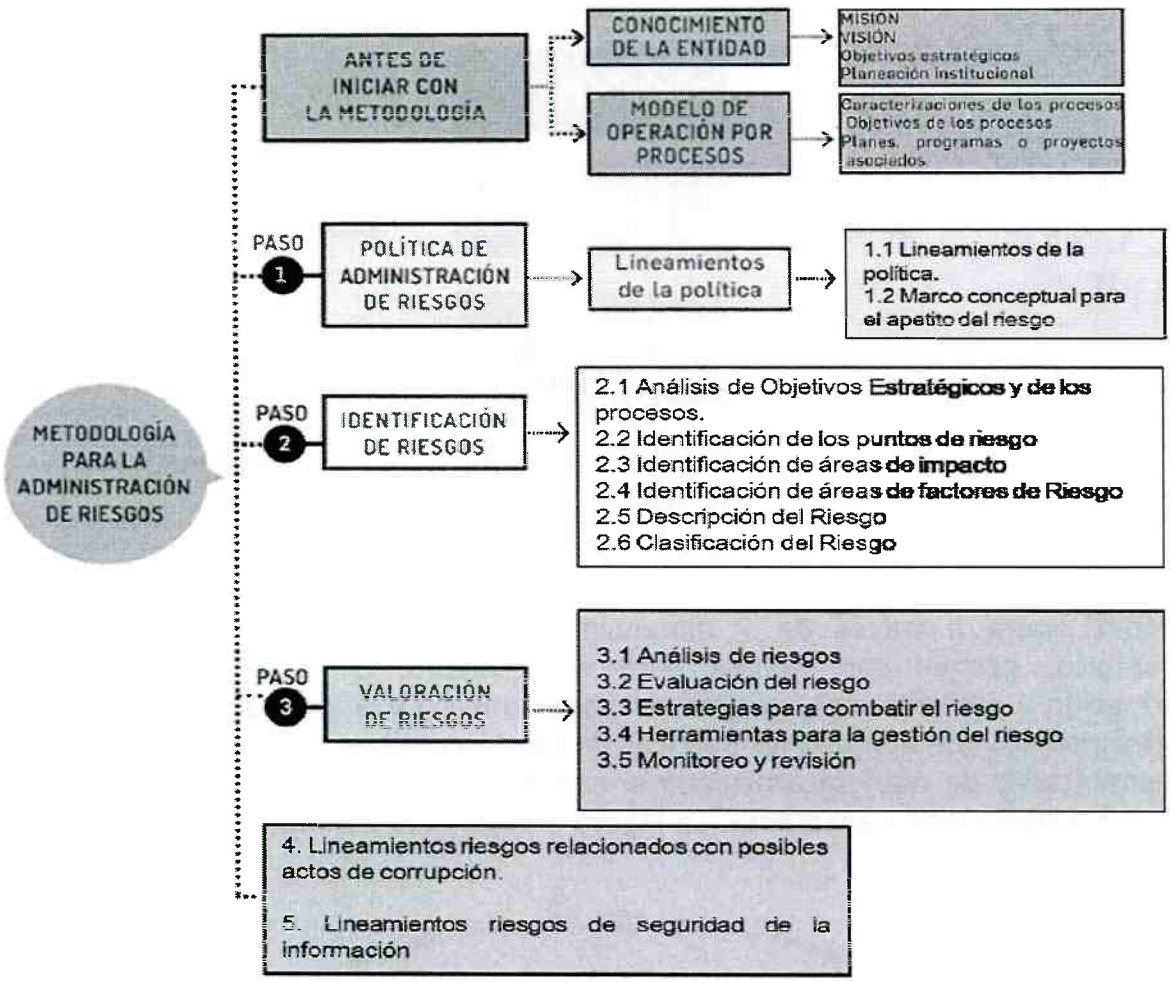
- Participar en el diseño de los controles que tienen a cargo.
- Ejecutar el control de la forma como está diseñado.
- Proponer mejoras a los controles existentes.

9 DESARROLLO METODOLÓGICO.

La metodología se fundamenta en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V. 6, emitida por el Departamento Administrativo de la Función Pública y algunos elementos se adaptan de acuerdo con la estructura y características del **Hospital Militar Central.** Dicha metodología del DAFP establece seis (6) pasos básicos, los cuales son:

Política de Administración del Riesgo, Identificación del Riesgo, Valoración del Riesgo, Riesgos de Corrupción y Riesgos de Seguridad de la Información y Riesgos de Seguridad del Paciente.

La gestión del riesgo facilita la toma de decisiones al interior de la entidad, impulsando así el crecimiento y la sostenibilidad de las acciones adelantadas, por tal razón, a continuación, se presenta la estructuración de la metodología de gestión del riesgo:



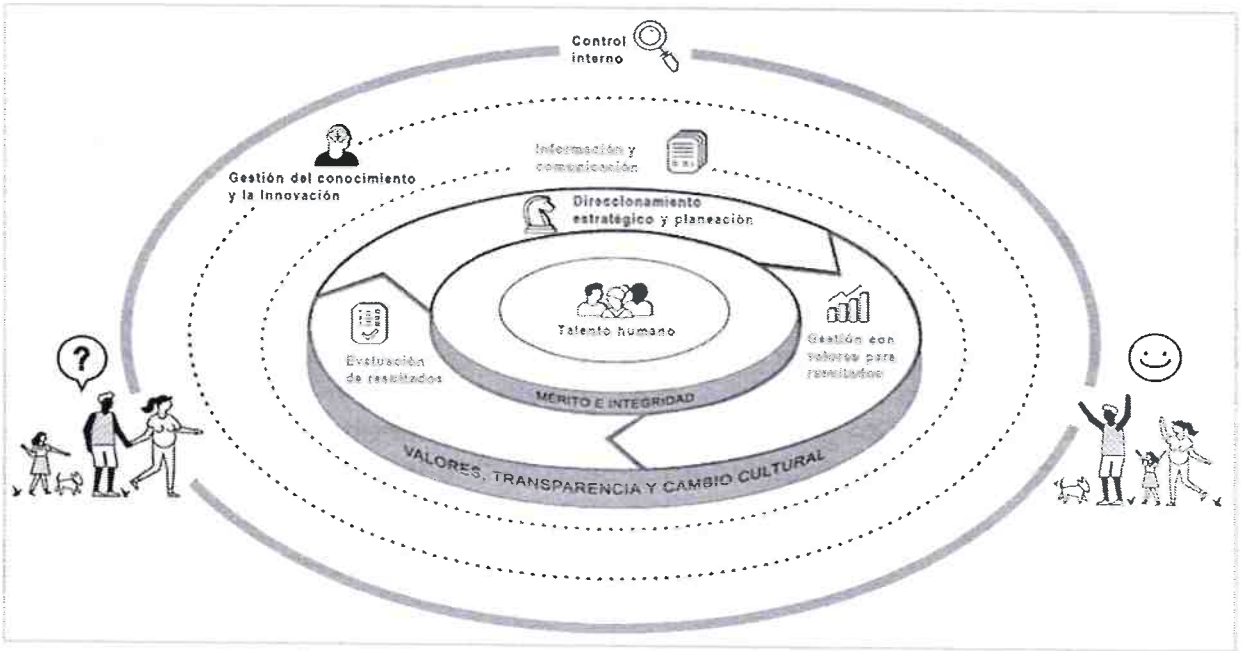
Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

9.1.1 ANTES DE INICIAR CON LA METODOLOGÍA.

El modelo integrado de planeación y gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, este modelo tiene el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio (Manual operativo MIPG, 2019, p. 6).

Fuente: Función Pública, 2017

El MIPG opera a través de 7 dimensiones (talento humano, direccionamiento estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y, finalmente, control interno) que agrupan las políticas de gestión y desempeño institucional y que, implementadas de manera articulada e interrelacionada, permitirán que el modelo funcione y opere adecuadamente. La Figura 1 ilustra las 7 dimensiones del modelo:



Fuente: Función Pública, 2017

9.1.2 CONOCIMIENTO DE LA ENTIDAD

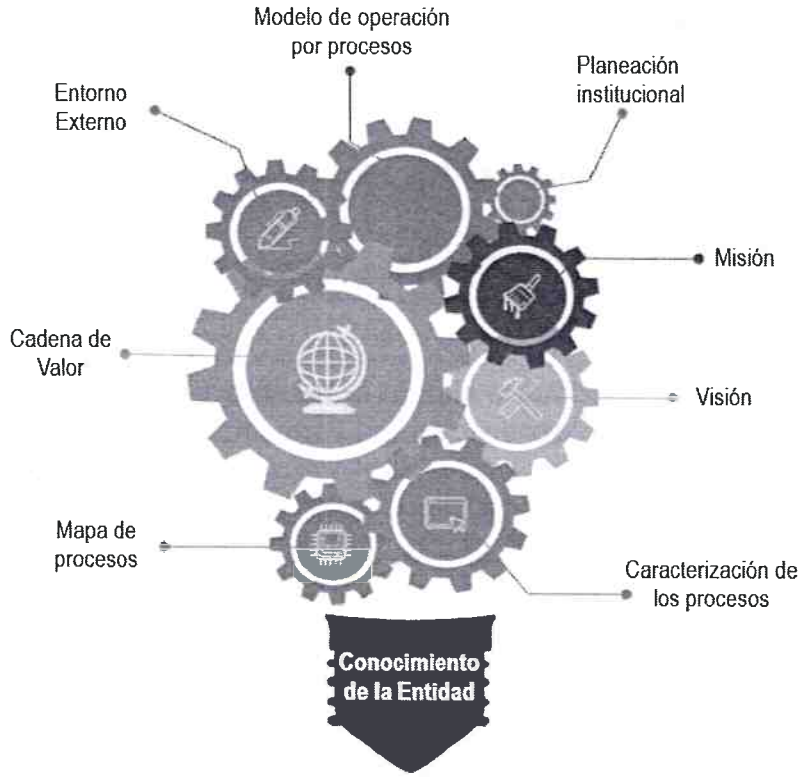
MISIÓN

Prestar servicios integrales especializados a los usuarios del Subsistema de Salud de las Fuerzas Militares centrados en el paciente y su familia y gestionar conocimiento a través de la academia y la investigación.

VISIÓN

El Hospital Militar Central continuará siendo la reserva estratégica de la nación en servicios integrales de salud y generación del conocimiento.

9.1.2.1 MODELO DE OPERACIÓN



Es preciso analizar el contexto general de la entidad, para establecer su complejidad, procesos, planeación institucional, permitiendo conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la Metodología en general.

9.1.2.2 MAPA DE PROCESOS

Mapa de Procesos
Resolución N° 588 del 8 de junio de 2018

En relación al mapa de procesos de la entidad, por cada uno de los quince (15) procesos del HOMIL, de deberán identificar riesgos que afecten el cumplimiento de los objetivos estratégicos y adicional elaborar el mapa de riesgos para cada vigencia, basado en los distintos sistemas de información, que pretenden identificar las actividades o procesos sujetos y expuestos a riesgos, cuantificar la probabilidad de estos eventos y medir el daño potencial asociado a su ocurrencia.

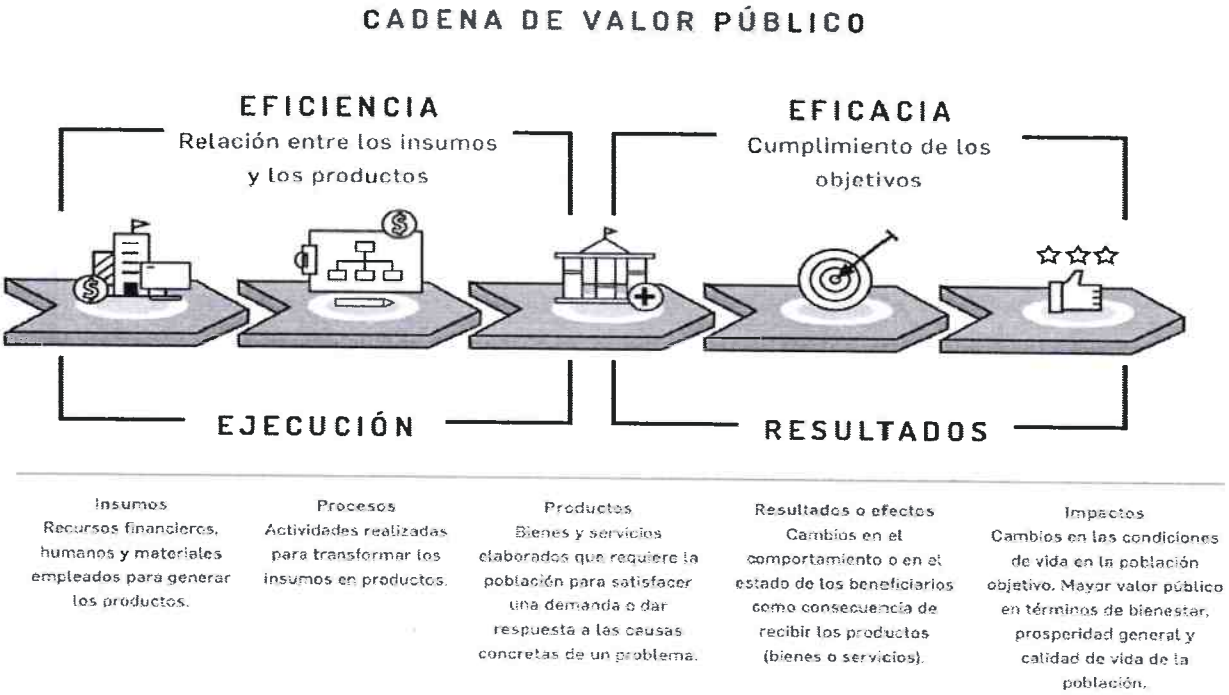
9.1.3 PASO 1 - POLÍTICA DE ADMINISTRACIÓN
9.1.4 DE RIESGOS

El **Hospital Militar Central** en ejercicio de su labor misional, se encuentra comprometido con la adecuada administración de los riesgos, a través de la definición del contexto de la entidad donde se desarrollan los procesos estratégicos, misionales, de apoyo y de evaluación, para lo cual adelantará acciones de identificación, análisis, valoración, monitoreo, tratamiento y seguimiento de los riesgos que puedan afectar el logro de los objetivos institucionales.

9.1.5 PASO 2 – IDENTIFICACIÓN DEL RIESGO

IDENTIFICACIÓN DE PUNTOS DE RIESGO

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

9.1.6 IDENTIFICACIÓN DE ÁREAS DE IMPACTO

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

9.1.7 IDENTIFICACIÓN DE FACTORES DE RIESGO

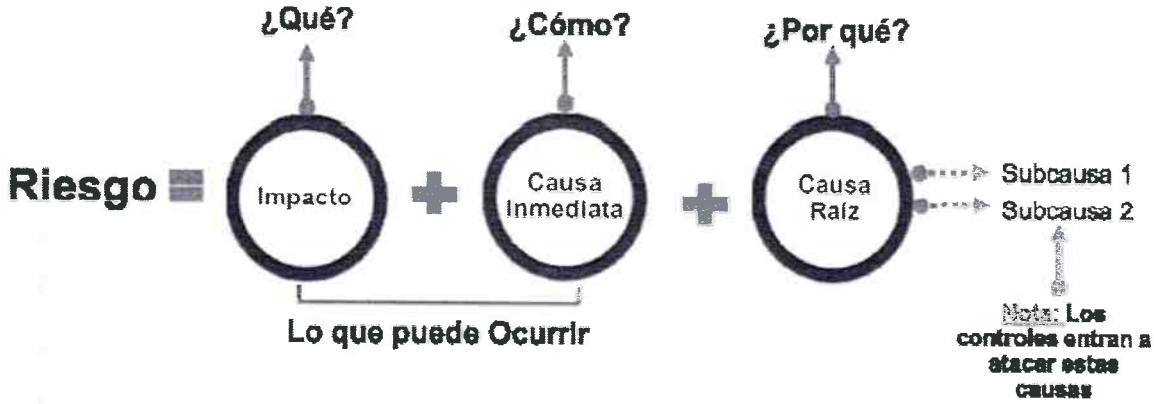
Son las fuentes generadoras de riesgos.

FACTOR	DEFINICIÓN		DESCRIPCIÓN
PROCESOS OPERACIONAL	Eventos relacionados con errores en las actividades que deben realizar los servidores de la entidad.		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 de activos.
			Posibles comportamientos no éticos de los funcionarios y contratistas.
			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.
EVENTOS EXTERNOS	Situaciones externas que afectan la entidad		Suplantación de Identidad.
			Asalto a oficina.
			Atentados, vandalismo, orden público.
SALUD	Eventos relacionados con la ocurrencia de un evento no deseado, evitable y negativo para la salud de un individuo, puede ser el empeoramiento de una condición previa.		Enfermedad.
			Traumatismos, eventos adversos, seguridad del paciente.
			Evolución negativa, desfavorable o complicaciones.
FISCAL	Eventos relacionados con pérdidas económicas por efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.		Daño que se genera sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir un evento potencial.
			Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

FACTOR	DEFINICIÓN		DESCRIPCIÓN
ACTUARIAL	Eventos relacionados con pérdidas económicas debido a no estimar adecuadamente el valor de los contratos por venta de servicios.		Desconocimiento de la demanda efectiva de servicios que van a atender, de la situación de salud de la población y de la frecuencia de uso.
			Concentración poblacional, con un enfoque diferencial de género, étnico, grupos etarios, regiones, grupo de riesgo, curso de vida, entre otros.
			Atención en zonas de difícil acceso y alta dispersión de la población.
			Hechos catastróficos o situaciones similares que afecten un número elevado de la población incluida en los contratos.
			Variaciones en las condiciones de morbi-mortalidad.
			Incrementos inesperados en los costos de proveedores.
			Incorporación de tecnología nueva que requiera recursos de inversión considerables.
CRÉDITO	Eventos relacionados con pérdidas como consecuencia del incumplimiento de obligaciones por parte de sus deudores.		Variación de los términos acordados (montos, plazos y condiciones técnicas del contrato).
			Glosas.
LIQUIDEZ	Eventos relacionados con la posibilidad que la entidad no cuente con recursos líquidos para cumplir sus obligaciones de pago en el corte, mediano y largo plazo.		Limitaciones al programa anual mensualizado de caja
			Modificaciones (plazo de pagos a proveedores).

9.1.8 DESCRIPCIÓN DEL RIESGO

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso, como para personas ajenas al proceso.



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

9.1.9 CLASIFICACIÓN DEL RIESGO

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

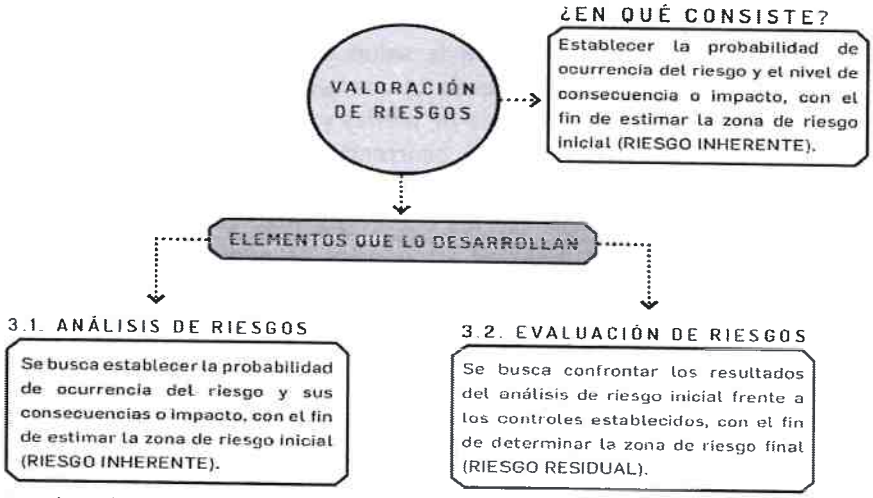
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales están involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
Salud	Probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo, que puede ser también el empeoramiento de una condición previa o la necesidad de requerir más consumo de bienes y servicios que hubiera podido evitarse. El evento, es la ocurrencia de la enfermedad, traumatismos o su evolución negativa, desfavorable o complicaciones de esta; y las causas, son los diferentes factores asociados a los eventos.
Fiscal	Son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.
Actuarial	Posibilidad de incurrir en pérdidas económicas debido a no estimar adecuadamente el valor de los contratos según los diferentes tipos de contratos (cápita, evento, Grupo Relacionado de Diagnóstico, Pago Global Prospectivo entre otros) por venta de servicios, de tal manera que estos resulten insuficientes para cubrir las obligaciones futuras que se acordaron.

Crédito	Posibilidad que la entidad incurra en pérdidas como consecuencia del incumplimiento de las obligaciones por parte de sus deudores en los términos acordados, como, por ejemplo, monto, plazo y demás condiciones.
Liquidez	Posibilidad que una entidad no cuente con recursos líquidos para cumplir con sus obligaciones de pago tanto en el corto (riesgo inminente) como en el mediano y largo plazo (riesgo latente).
Sarlaft	El Sistema de Administración del Riesgo de Lavado de Activos y Financiación al Terrorismo –SARLAFT–, es el mecanismo que permite a las entidades prevenir la pérdida o daño que pueden sufrir por su propensión a ser utilizadas como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, por sus clientes o usuarios.

Nota 1: Para la identificación de riesgos y peligros asociados a "Seguridad y Salud en el trabajo", el Hospital Militar Central deberá aplicar el procedimiento Código: GH-SSTR-PR-05 - IDENTIFICACIÓN DE PELIGROS, EVALUACIÓN Y VALORACIÓN DE LOS RIESGOS o documento que lo actualice y/o modifique, liderado por el área de seguridad y salud en el trabajo.

Nota 2: Todo lo relacionado con el Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo, se gestionará bajo la metodología y responsabilidad definida por el funcionario que desempeñe las funciones del Oficial de Cumplimiento titular o suplente.

9.1.10 PASO 3 - VALORACIÓN DEL RIESGO



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

9.1.11 ANÁLISIS DE RIESGOS

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

9.1.12 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.

Como referente, a continuación, se muestra un ejemplo en una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

ACTIVIDAD	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD FRENTE AL RIESGO
Planeación estratégica.	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa.	Mensual	Media
Contabilidad, cartera.	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería. ***Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probab*ilidad, 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 siguiente tabla se establecen los criterios para definir el nivel de probabilidad.

9.1.13 CRITERIOS PARA CALIFICAR LA PROBABILIDAD

La calificación de la probabilidad de que un riesgo se llegue a materializar debe partir de datos históricos, con lo cual se determina la frecuencia. En caso de que estos datos no existan, se realiza una ponderación de la factibilidad de ocurrencia que consideren diferentes funcionarios o contratistas conocedores del proceso. Los niveles para calificar la probabilidad, en términos de frecuencia y factibilidad, se definen en la siguiente tabla.

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 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%

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

9.1.14 DETERMINAR EL IMPACTO

Para la construcción de la tabla de criterios, se definen los impactos económicos y reputacionales como las variables principales.

En la guía de administración del riesgo del DAFP se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

Ejemplo: Para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

9.1.15 CRITERIOS PARA DEFINIR EL IMPACTO

Para determinar la magnitud del impacto de los riesgos, se tienen en cuenta los siguientes parámetros dependiendo del tipo de impacto, tal y como se relaciona a continuación:

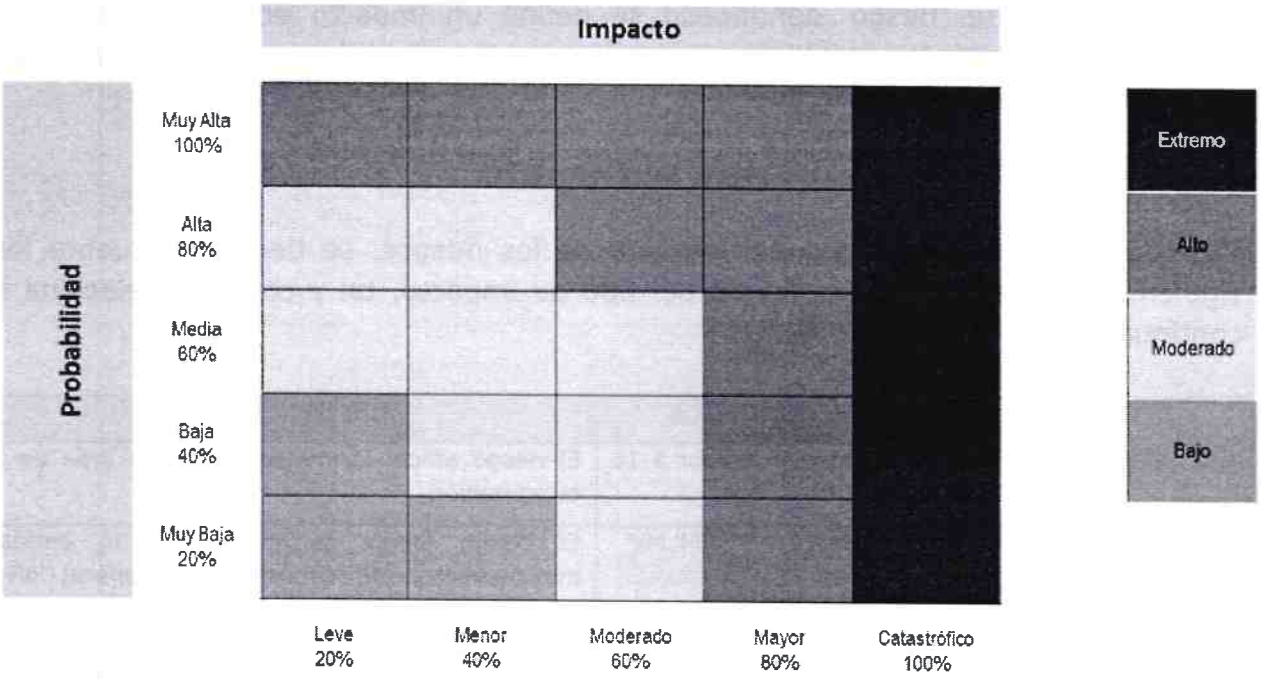
NIVEL	%	ECONÓMICA	REPUTACIONAL
Leve	20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor	40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
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.

Fuente: *Guía para la administración del riesgo y el diseño de controles èn entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

9.1.16 EVALUACIÓN DEL RIESGO

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

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.



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

9.1.17 PASO 4 - LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

DISPOSICIONES GENERALES

En el marco del Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: gestión del riesgo de corrupción. Es importante recordar que el desarrollo de este componente se articula con los demás establecidos para el desarrollo del plan, ya que se trata de una acción integral en la lucha contra la corrupción.

COMPONENTES PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

En materia de riesgos asociados a posibles actos de corrupción, para la presente política se consideran los siguientes aspectos:

El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Los riesgos de corrupción se establecen sobre procesos.
El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

9.1.18 GENERALIDADES ACERCA DE LOS RIESGOS DE CORRUPCIÓN

- **Se elabora** anualmente por cada responsable de los procesos al interior de la entidad, junto con su equipo de trabajo.
- **Ajustes y modificaciones:** después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción. En este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

- **Socialización:** Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, o la de gestión del riesgo deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción. Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.
- **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 gestión, seguridad digital y corrupción.
- **Seguimiento:** el jefe de control interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de gestión, seguridad digital y corrupción. En este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

9.1.19 IDENTIFICACIÓN DEL RIESGO DE CORRUPCIÓN.

A continuación, se señalan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la entidad podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos:

Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

Direccionamiento estratégico (alta dirección)	Concentración de autoridad o exceso de poder. Extralimitación de funciones. Ausencia de canales de comunicación. Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto)	Inclusión de gastos no autorizados. Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.

	Inexistencia de archivos contables. Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	Estudios previos o de factibilidad deficientes. Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). Pliegos de condiciones hechos a la medida de una firma en particular. Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. Urgencia manifiesta inexistente. Concentrar las labores de supervisión en poco personal. Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	Ausencia o debilidad de medidas y/o políticas de conflictos de interés. Concentración de información de determinadas actividades o procesos en una persona. Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. Ocultar la información considerada pública para los usuarios. Ausencia o debilidad de canales de comunicación.
De investigación y Sanción	Inexistencia de canales de denuncia interna o externa. Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. Exceder las facultades legales en los fallos.
De trámites y/o servicios internos y externos	Cobros asociados al trámite. Influencia de tramitadores. Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos)	Falta de procedimientos claros para el trámite. Imposibilitar el otorgamiento de una licencia o permiso. Tráfico de influencias: (amiguismo, persona influyente).

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

9.1.20 LINEAMIENTOS PARA LA IDENTIFICACIÓN DEL RIESGO DE CORRUPCIÓN

Las preguntas clave para la identificación del riesgo son:

- ¿Qué puede suceder?
- ¿Cómo puede suceder?
- ¿Cuándo puede suceder?
- ¿Qué consecuencias tendría su materialización?

RIESGO DE CORRUPCIÓN
Definición de riesgo de corrupción: **Riesgo de corrupción:** Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. "Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Compes No. 167 de 2013) Es necesario que en la descripción del riesgo concurran los componentes de su definición, así: **ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + BENEFICIO DE UN PRIVADO**

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se establece la utilización de la matriz de definición de riesgo de corrupción que incorpora cada uno de los componentes de su definición.

Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

MATRIZ DE DEFINICIÓN RIESGOS DE CORRUPCIÓN				
DESCRIPCIÓN DEL RIESGO	ACCIÓN U OMISIÓN	USO DEL PODER	DESVIAR LA GESTIÓN DE LO PÚBLICO	BENEFICIO PRIVADO
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

En materia de riesgos asociados a posibles actos de corrupción, se consideran los siguientes aspectos:

El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Los riesgos de corrupción se establecen sobre procesos.
El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

9.1.21 LA CORRUPCIÓN EN LOS TRÁMITES ADMINISTRATIVOS

Los riesgos de corrupción en trámites se pueden presentar en dos momentos:

- En el momento de efectuar el trámite propiamente dicho, cuando interactúan el ciudadano y el servidor (es decir de la ventanilla hacia afuera de la entidad por ejemplo cuando el ciudadano presenta un documento o efectúa un pago).
- En el momento en que se ejecutan los procedimientos al interior de la entidad para dar cumplimiento al trámite (de la ventanilla hacia adentro. La entidad tiene procedimientos internos, como por ejemplo distribuir la documentación recibida entre las áreas internas cambiando el turno).

A continuación, las definiciones de cada uno de los factores que determinan la presión:

- Internos: son factores de la trayectoria socioeconómica, ética y educativa del servidor que inciden en las decisiones afectando los recursos públicos y la imagen institucional.

- Externos: son factores del contexto del mercado y de variables culturales que se manifiestan en ofrecimiento de dádivas por acción u omisión de los servidores públicos provenientes de carteles de contratistas o grupos legales e ilegales.

9.1.22 IDENTIFICACIÓN DE RIESGOS DE CORRUPCIÓN ASOCIADOS A TRÁMITES

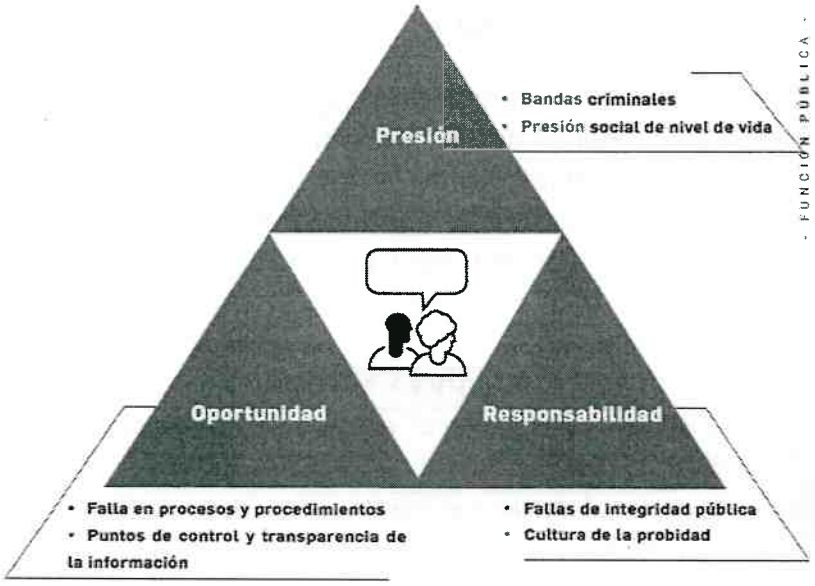
La identificación de riesgos de corrupción asociados a trámites inicia con el análisis de los objetivos de los procesos misionales que incluyan procedimientos que deben atender los usuarios para cumplir los requerimientos de un trámite.

El punto de partida para la identificación de riesgos de corrupción asociados a trámites es el análisis del contexto que considere factores internos y externos a la gestión del trámite.

En el contexto interno se deben determinar las debilidades que generan riesgos de corrupción. Algunos de ellos son: espacios de discrecionalidad (toma de decisiones con cierta autonomía), fallas en el diseño de los procesos, normatividad compleja, excesivos costos administrativos, débiles sistemas de información, inadecuada selección de personal, ausencia de manuales, tecnología obsoleta o carente de controles, entre otros.

Por otra parte, en el contexto externo se deben considerar las amenazas del entorno que pueden incidir en el uso del poder para beneficio de un privado: la intervención de carteles de contratistas, organizaciones delictivas, grupos armados, participación y control social débiles, fragilidad en el control externo, recursos públicos no regulados efectivamente, entre otros.

En los posibles factores externos para el análisis del entorno se pueden tener en cuenta los componentes del triángulo de la corrupción (Figura 1.), y deben ser analizados en cada una de las etapas de los trámites.



El Hospital Militar Central cuenta con 10 trámites administrativos, los cuales se encuentran inscritos en el sistema único de información de trámites – SUIT.

Trámites Administrativos Hospital Militar Central:

- Certificado de nacido vivo.
- Atención inicial de urgencia.
- Certificado de defunción.
- Historia clínica.
- Asignación de cita médica para la prestación de servicios en salud.
- Dispensación de medicamentos y dispositivos médicos.
- Admisión del paciente a los servicios de salud ambulatorios y hospitalarios.
- Exámenes de laboratorio clínico.
- Estudios anatomopatológicos, de inmunofenotipo y biomoleculares en tejidos humanos.
- Donación Voluntaria de Sangre

Para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios, se adopta el anexo No. 3 "Protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios" del Departamento Administrativo de la Función Pública – DAFP.

9.1.23 VALORACIÓN DE RIESGOS DE CORRUPCIÓN

La determinación de la probabilidad.

La calificación de la probabilidad de que un riesgo se llegue a materializar debe partir de datos históricos, con lo cual se determina la frecuencia. En caso de que estos datos no existan, se realiza una ponderación de la factibilidad de ocurrencia que consideren diferentes funcionarios o contratistas conocedores del proceso. Los niveles para calificar la probabilidad, en términos de frecuencia y factibilidad, se definen en la siguiente tabla.

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 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%

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

La determinación del Impacto.

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos.

Ahora bien, para establecer estos niveles de impacto se deberán aplicar las siguientes preguntas frente al riesgo identificado:

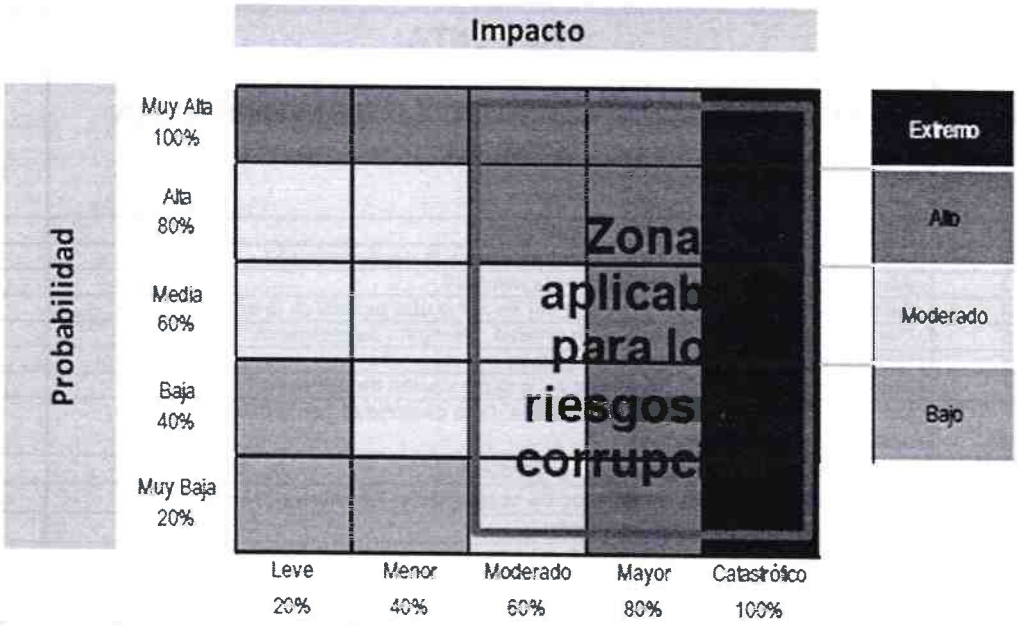
CRITERIOS PARA CALIFICAR EL IMPACTO EN RIESGOS DE CORRUPCIÓN			
No.	**PREGUNTA:** **SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...**	**RESPUESTA**	
		SI	**NO**
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos		
7	¿Afectar la generación de los productos o la prestación de serivicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida 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 pérdida 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?		
Responder afirmativamente de **UNA** a **CINCO** pregunta(s) genera un impacto moderado Responder afirmativamente se **SEIS** a **ONCE** preguntas genera un impacto mayor. Responder afirmativamente de **DOCE** a **DIECINUEVE** preguntas genera un impacto catastrófico		0	0
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

Análisis preliminar (riesgo inherente):

En esta etapa se define el nivel de severidad para el riesgo de corrupción identificado, para lo cual se aplica la matriz de calor, teniendo en cuenta el ajuste frente a los niveles de impacto insignificante y menor mencionados en la determinación del

impacto, lo que implica que las zonas de severidad para este tipo de riesgos se delimita como se muestra a continuación:



9.1.24 PASO 5 - LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El Hospital Militar Central – HOMIL conforme lo establecido en la directiva permanente N° 002 del 15 de junio de 2021 - LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE GOBIERNO DIGITAL EN EL HOSPITAL MILITAR CENTRAL en el numeral 2. Seguridad de la Información gestiona la seguridad de la información dando aplicabilidad al Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas V5.

Por lo anterior y en el marco del cumplimiento a lo establecido en Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas V6, el Hospital Militar Central gestionará los riesgos de seguridad de la información conforme lo establecido en el numeral 5 de la mencionada guía, así:

Identificar los activos de seguridad de la información.
Identificar los riesgos inherentes de seguridad de la información (Pérdida de la confidencialidad, Pérdida de la integridad, Pérdida de la disponibilidad)

Valorar los riesgos de seguridad de la información
Identificar los controles asociados a la seguridad de la información

9.1.25 PASO 6 - LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON LA SEGURIDAD DEL PACIENTE.

Gestión Integral del Riesgo en Salud

La Gestión Integral del riesgo en Salud –GIRS, es una estrategia transversal de la Política de Operación para la Administración del Riesgo en el Hospital Militar Central, que se establece en la articulación e interacción de los agentes del sistema de salud para identificar, evaluar, medir, intervenir y llevar a cabo el seguimiento y monitoreo de los riesgos para la salud de las personas, familias y comunidades, orientada al logro de resultados en salud y al bienestar de la población atendida por el HOMIL, articulado con la Política de Seguridad del Paciente. La GIRS se anticipa a las enfermedades y los traumatismos para que éstos no se presenten o se detecten y traten precozmente para impedir, acortar o paliar su evolución y consecuencias.

Riesgo de Seguridad del Paciente.

El Plan Decenal de Salud Pública concibe el riesgo de seguridad del paciente – riesgo en salud como "la probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo, que puede ser también el empeoramiento de una condición previa o la necesidad de requerir más consumo de bienes y servicios que hubiera podido evitarse" (MSPS, 2013, p. 51). El evento es la ocurrencia de la enfermedad o su evolución desfavorable y sus causas son los diferentes factores asociados. El riesgo en salud a su vez puede clasificarse como primario si se refiere a la probabilidad de aparición de nueva morbilidad o su severidad o como técnico si alude a la probabilidad de "ocurrencia de eventos derivados de fallas de atención en los servicios de salud y de la mayor carga de enfermedad por mortalidad evitable y discapacidad" (MSPS, 2013, p. 147).

El objetivo de la estrategia es el logro de un mejor nivel de salud de la población, una mejor experiencia de los usuarios durante el proceso de atención y unos costos acordes a los resultados obtenidos (MSPS, 2016a).

Frente a la identificación, análisis, valoración, manejo, reporte y monitoreo de los riesgos de seguridad del paciente, se aplicará la metodología definida por el Departamento Administrativo de la Función Pública en su versión No. 6 y esta será aplicada por el HOSPITAL MILITAR CENTRAL.

De igual manera, el **Área de Gestión de Calidad** lleva a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Asegurar que al interior de sus grupos de trabajo se reconozca el concepto de "Administración de Riesgo" la política, metodología y marco de referencia de Función Pública aprobado por la línea estratégica.
- Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos de seguridad del paciente que pueden afectar el cumplimiento de los objetivos estratégicos, objetivos del proceso, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgos del proceso a cargo.
- Identificar cuando se requiera, nuevos riesgos de seguridad del paciente que puedan afectar el cumplimiento de los objetivos estratégicos, objetivos del proceso, programas, proyectos y planes asociados a su proceso.
- Informar a la Oficina Asesora de Planeación (segunda línea) sobre la identificación de nuevos riesgos de seguridad del paciente, con el objetivo de dar continuidad a la metodología establecida en la entidad y posterior aprobación por parte del Comité Institucional de Gestión y Desempeño.
- Elaborar y enviar propuesta de los nuevos riesgos de seguridad del paciente identificados por el área y proceso responsable, a la Oficina Asesora de Planeación para revisión y análisis metodológico, dando cumplimiento a los lineamientos definidos por la entidad en materia de administración de riesgos.
- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, gestión, reporte de acciones de autocontrol, reporte del monitoreo y socialización de los riesgos de seguridad del paciente al interior de los grupos de trabajo.
- Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos de seguridad del paciente identificados y proponer mejoras para su gestión.
- Revisar el adecuado diseño y 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.
- Registrar y consolidar en el formato establecido por la entidad, las acciones de autocontrol realizadas frente a cada riesgo en salud en el periodo de reporte, de acuerdo a los controles y periodicidades definidas en el mapa de riesgos por proceso.
- Señalar en la matriz del monitoreo al mapa de riesgos, si el riesgo se materializó o no se materializó.

MATERIALIZACIÓN DE RIESGOS

- Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos de seguridad del paciente materializados que puedan afectar el cumplimiento de los objetivos, programas, proyectos y planes de los procesos a cargo, de acuerdo a las periodicidades definidas por la entidad. (Monitoreo al mapa de riesgos).
- Frente a cada riesgo materializado, se deberán diligenciar las celdas correspondientes al "Plan de manejo y/o mitigación del riesgo en el formato establecido por la entidad.
    - "Si se materializó el riesgo, describa brevemente el hecho y especifique el área y/o servicio en donde tuvo lugar"
    - "Descripción numérica ¿Cuántos hechos se presentaron?"
    - Realizó análisis "Causa –Raíz". ¿Si – No?
    - Descripción del Análisis.
    - Acciones desarrolladas para mitigar el riesgo materializado.
    - Responsable de la ejecución y cumplimiento del plan.
    - Registrar la fecha y plazo de ejecución del plan de manejo y/o mitigación del riesgo.
    - Registros / Evidencias.
- Revisar y hacer seguimiento a las acciones establecidas en el plan de manejo y/o mitigación del riesgo establecido para cada uno de los riesgos de seguridad del paciente materializados, con el fin de que se tomen medidas oportunas y eficaces.
- En caso de la materialización de un riesgo en salud no identificado, este deberá ser gestionado, con el acompañamiento de la Oficina Asesora de Planeación, e incluirlo en el mapa de riesgo institucional. el repositorio
- Garantizar, custodia y disposición permanente de las evidencias de la ejecución de los controles establecidos en el mapa de riesgos.
- Considerar y tener en cuenta las recomendaciones plasmadas en los informes de las auditorías realizadas por la Oficina de Control Interno.

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

- Verificar las acciones preventivas de acuerdo con la periodicidad definida.
- Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación.

- Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo en salud, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir.
- Comunicar al equipo de trabajo los resultados de la gestión de los riesgos de seguridad del paciente.
- Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento.
- Garantizar la generación, repositorio, custodia y disposición permanente de las evidencias de la ejecución de los controles establecidos en el mapa de riesgos.

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.

10 VALORACIÓN DE CONTROLES:

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.

10.1.1 ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL

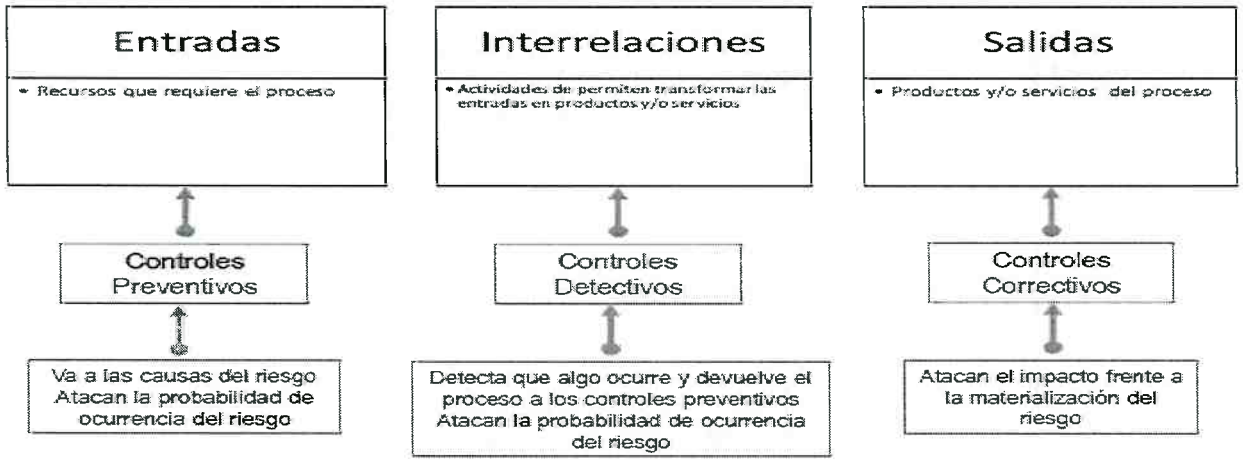
Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **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.
- **Periodicidad:** Plazos de ejecución de las acciones de control.

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

10.1.2 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 se consideran 3 fases globales del ciclo de un proceso así:



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

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 re-procesos.
- **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 se tiene:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

Análisis y evaluación de los controles – Atributos:

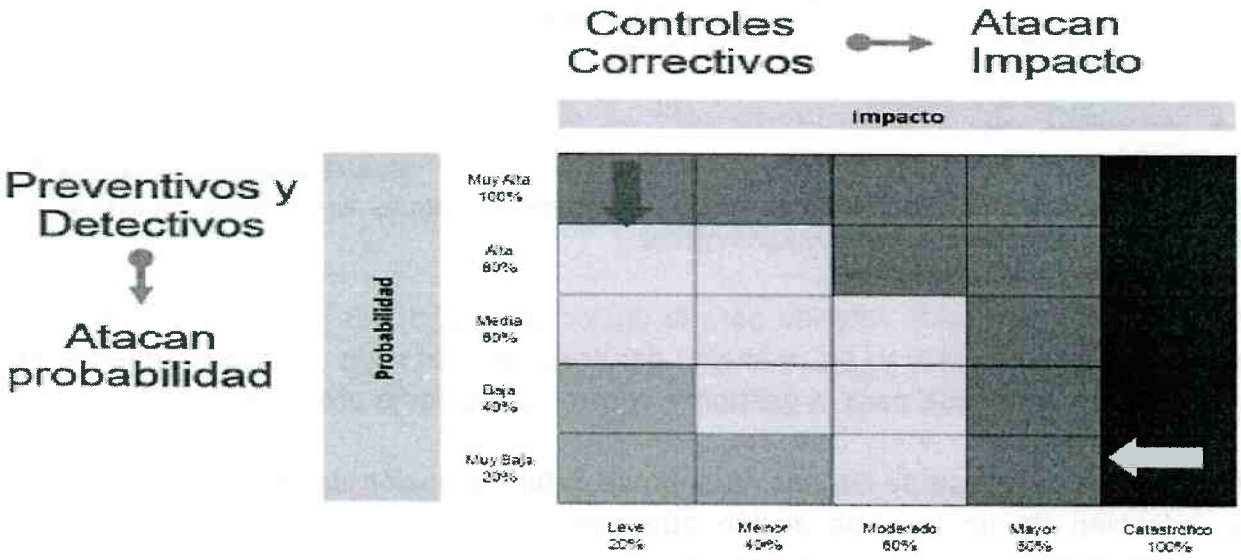
A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

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 intervención de personas para su realización.	25%
		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.	-

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

***Nota:** 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 muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

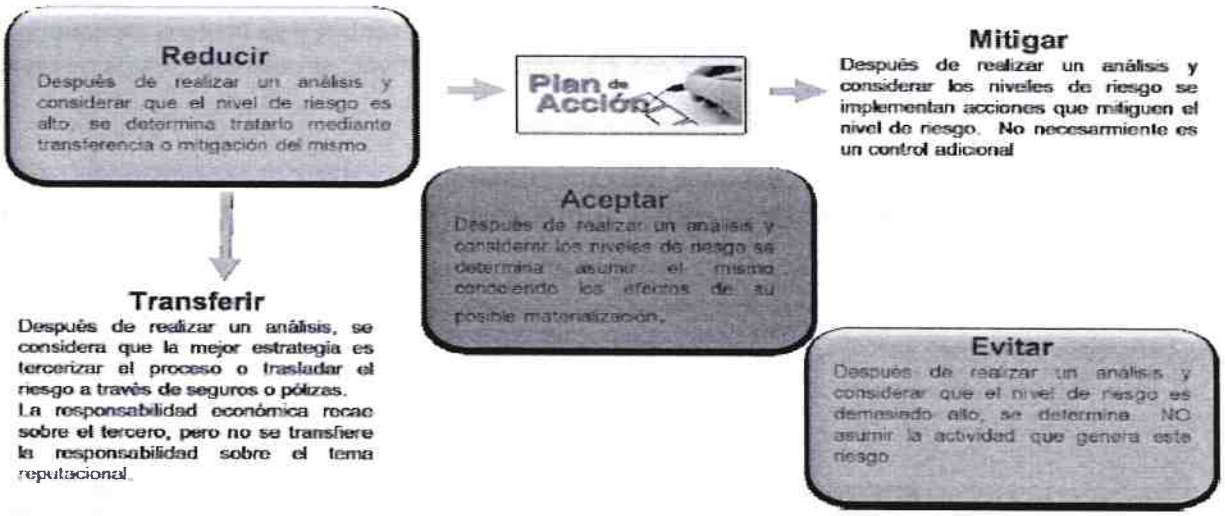


***Fuente:** Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

11 ESTRATEGIAS PARA COMBATIR EL RIESGO

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

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: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.*

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

NIVEL DE ACEPTACIÓN		
ZONA DE RIESGO	**RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL**	**RIESGOS DE CORRUPCIÓN/TRÁMITE**
Bajo	**ACEPTAR** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado.	**NINGÚN** riesgo de corrupción podrá ser aceptado.
Moderado	Se establecen acciones de Control Preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo.	
Alto	Se debe incluir el riesgo tanto en el Mapa de Riesgos del Proceso como en el Mapa de Riegos Institucional y se establecen acciones de control Preventivas que permitan **EVITAR** la materialización del riesgo.	Se adoptan medidas para **REDUCIR** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. **Evitar** - Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
Extremo	Se incluye el riesgo en el Mapa de riesgo del Proceso y en el Mapa de	

	Riesgo Institucional, se establecen acciones de Control Preventivas y correctivas que permitan **EVITAR** la materialización del riesgo.	Se reduce la probabilidad o el impacto del riesgo, **TRANSFIRIENDO O COMPARTIENDO** una parte del riesgo.

***Nota**: Frente a los riesgos de corrupción en trámites, el HOSPITAL MILITAR CENTRAL adopta el anexo No. 3 de la guía de administración del riego "protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios", del Departamento Administrativo de la Función Pública.*

11.1.1 HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO:

Como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

Gestión de eventos: un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de ayuda.
- Las PQRD (peticiones, quejas, reclamos, denuncias).
- Oficina jurídica.
- Líneas internas de denuncia.

Esta herramienta genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

Desempeño del control= # eventos / frecuencia del riesgo (# veces que se hace la actividad)

Gestión Indicadores clave de riesgo: Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

DISEÑO, ACTUALIZACIÓN, MONITOREO Y SEGUIMIENTO AL MAPA DE RIESGOS

12 DISEÑO DE LOS MAPAS DE RIESGOS

Los líderes de proceso deben identificar los riesgos de acuerdo a la metodología expresada anteriormente con el acompañamiento de la **Oficina Asesora de Planeación** y la **Oficina de Control Interno**. Una vez identificados y validados los riesgos, estos se deben consignar en el formato Mapa de riesgos por Proceso**,** y cumplir con los criterios establecidos en el mismo con respecto al flujo de aprobación.

Los líderes de proceso (Subdirectores, jefes de oficina y/o unidad) presentarán ante el Comité Institucional de Gestión y Desempeño el mapa de riesgos correspondiente para su aprobación.

13 PROCESO DE ACTUALIZACIÓN Y MONITOREO

El mapa de riesgos institucional deberá ser actualizado como mínimo una vez al año o cada vez que los líderes de proceso así lo determinen, teniendo en cuenta el conocimiento sobre la evolución de la gestión o como resultado de recomendaciones provenientes de ejercicios de auditorías, o cambios en la normatividad.

Así mismo, es necesario realizar el monitoreo periódico de los riesgos, teniendo en cuenta que esta actividad es de gran importancia y está a cargo de los líderes de los procesos en conjunto con sus equipos, permitiendo así asegurar la eficiencia en la administración de los riesgos del Hospital Militar Central.

Para realizar el monitoreo a los riesgos, se cuenta con el formato Mapa de Riesgos **PL-OAPL-PO-01-FT-02**, en el cual se deben describir las acciones de "autocontrol" realizadas para mitigar la materialización de los riesgos, seleccionar si el riesgo se materializó, la eficacia del control e igualmente se reportan las acciones adelantadas en el plan de manejo y/o mitigación del riesgo, en caso de materializarse.

Con el fin de consolidar los monitoreos de los riesgos se parametrizarán las actividades de reporte en la plataforma Suite Visión, en la cual los líderes de proceso reportarán el comportamiento de los riesgos.

Adicionalmente, cada líder de proceso deberá garantizar la custodia y disposición permanente de las evidencias de ejecución de los controles definidos en cada proceso.

13.1.1 FECHAS DE REPORTE, MONITOREO Y SEGUIMIENTO.

Los líderes de proceso deben realizar reporte de los mapas de riesgos por proceso en las siguientes fechas:

Riesgos de Gestión – Seguridad Digital

LÍNEA DE DEFENSA	FECHAS DE REPORTE (TRIMESTRAL)												
	EN	FE	MA	AB	MA	JU	JU	AG	SE	OC	NO	DI	EN
CORTE	1		31	1		30	1		30	1		31	
1er línea *(Líder de proceso)*				3			3			3			3
2da línea (Planeación)				5			5			5			5
3er línea *(Control Interno)*					10				10				10

Responsabilidad de las líneas de defensa frente a las fechas de reporte:
1er línea: Realizar el reporte y cargue del monitoreo en la Suite Visión Empresarial, en el formato PL-OAPL-PO-01-FT-02 en las siguientes fechas:

- 3er día hábil de abril.
- 3er día hábil de julio.
- 3er día hábil de octubre.
- 3er día hábil de enero.

2da línea: Realizar análisis del monitoreo y posterior informe con la información reportada por los líderes de proceso, en las siguientes fechas, así:

- 5to día hábil de abril.
- 5to día hábil de julio.
- 5to día hábil de octubre.
- 5to día hábil de enero

3er línea: Realizar seguimiento a los mapas de riesgos de gestión y corrupción, verificando la efectividad de los controles establecidos, en las siguientes fechas, así:

- 10 de mayo.
- 10 de septiembre.
- 10 de enero

Riesgos de Corrupción

LÍNEA DE DEFENSA	FECHAS DE REPORTE (MENSUAL)												
	EN	FE	MA	AB	MA	JU	JU	AG	SE	OC	NO	DI	EN
CORTE	1-31	1-28	1-31	1-30	1-31	1-30	1-31	1-31	1-30	1-31	1-30	1-31	1-31
1er línea *(Líder de proceso)*		3	3	3	3	3	3	3	3	3	3	3	3
2da línea (Planeación)				5			5			5			5
3er línea *(Control Interno)*					10				10				10

1er línea: Realizar el reporte y cargue del monitoreo en la Suite Visión Empresarial, en el formato PL-OAPL-PO-01-FT-02 en las siguientes fechas:

- 3er día hábil de enero.
- 3er día hábil de febrero.
- 3er día hábil de abril.
- 3er día hábil de mayo.
- 3er día hábil de junio.
- 3er día hábil de julio.
- 3er día hábil de agosto.
- 3er día hábil de septiembre.
- 3er día hábil de octubre.
- 3er día hábil de noviembre.
- 3er día hábil de diciembre.
- 3er día hábil de enero

2da línea: Realizar análisis del monitoreo y posterior informe con la información reportada por los líderes de proceso, así:

- 5to día hábil de abril.
- 5to día hábil de julio.
- 5to día hábil de octubre.
- 5to día hábil de enero.

3er línea: Realizar seguimiento a los mapas de riesgos corrupción, verificando la efectividad de los controles establecidos, así:

- 10 de mayo.
- 10 de septiembre.
- 10 de enero
-

3er línea: Realizar seguimiento a los mapas de riesgos de gestión, verificando la efectividad de los controles establecidos, así:

- 10 de mayo.
- 10 de agosto.
- 10 de noviembre.
- 10 de febrero.

14 ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

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

ACCIONES DE RESPUESTA A RIESGOS MATERIALIZADOS		
Tipo de Riesgo	**Responsable**	**Acción**
Riesgo de Corrupción	Líder de proceso	El servidor público, contratista o tercero debe informar a su superior inmediato, jefe de unidad, jefe de oficina, subdirector y a la Oficina de Control Interno Disciplinario, sobre los delitos, contravenciones y fallas disciplinarias de las cuales tenga conocimiento. Toda persona servidos público, contratista o tercero) debe denunciar a la autoridad competente los delitos de cuya comisión tenga conocimiento y que deban investigarse. El servidor público, contratista o tercero que conozca de la comisión de un delito que deba investigarse de oficio, iniciará sin tardanza la investigación si tuviere competencia para ello; en caso contrario, pondrá inmediatamente el hecho en conocimiento ante la autoridad competente". Bajo esas orientaciones de tipo normativo, corresponde al servidor público que identifica la irregularidad, informar a la dependencia, o autoridad respectiva para que de acuerdo con sus competencias de curso a la investigación a que haya lugar. Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. Efectuar el análisis de causas y determinar acciones preventivas y de mejora. Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario.

		Informar a discreción los posibles actos de corrupción al ente de control.
Riesgos de Gestión y Seguridad digital		Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo. Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. Dar cumplimiento al plan de manejo y/o mitigación del riesgo.
	Control Interno	Informar al líder del proceso sobre el hecho encontrado. Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de manejo y/o mitigación del riesgo y realizará el seguimiento de acuerdo a lo establecido en la Política de Riesgos.

Nota: Todo lo relacionado con el Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo - SARLAFT, se gestionará bajo la metodología y responsabilidad definida por el funcionario que desempeñe las funciones del Oficial de Cumplimiento titular o suplente.

15 SEGUIMIENTO

La Oficina de Control Interno realizará seguimiento del mapa de riesgos de gestión, seguridad digital y corrupción institucional y revisará de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, de acuerdo con los siguientes aspectos:

- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
- Implementar en el proceso de auditoría interna se analicen los riesgos de gestión, seguridad digital y corrupción y la efectividad de los controles incorporados en el mapa de riesgos institucional.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- Para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.
- Realizar seguimiento y verificación de las evidencias de la ejecución de los controles definidos en el mapa de riesgos institucional.
- Hacer seguimiento a los controles establecidos por la primera línea de defensa, acorde con la información suministrada por los líderes de procesos.
- Hacer seguimiento al monitoreo del mapa de riesgos en la Suite Visión Empresarial – SVE y evidencias de la ejecución de los controles definidos, dentro de los plazos establecidos.
- Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de manejo y/o mitigación del riesgo y realizará el seguimiento de acuerdo a lo establecido en la Política de Riesgos.

Nota: La Oficina de Control Interno, realizará seguimiento al Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo, la metodología definida por el funcionario que desempeñe las funciones del Oficial de Cumplimiento titular o suplente.

Nota: Para consultas adicionales sobre la metodología implementada en el Hospital Militar Central, podrá consultar la guía para la administración del riesgo y el diseño de controles en entidades públicas V. 6 – Departamento Administrativo de la Función Pública.

https://www.funcionpublica.gov.co/web/eva/detalle-publicacion?entryId=34316499

16 COMUNICACIÓN Y SOCIALIZACIÓN DE LA POLITICA DE ADMINISTRACIÓN DEL RIESGO

Una vez aprobada la Política de administración del riesgo por parte del Comité Institucional de Coordinación de Control Interno, se deberá comunicar y socializar con los servidores públicos y contratistas de la entidad, con el fin de generar apropiación sobre la gestión del riesgo institucional.

17 RIESGOS OPERATIVOS ASOCIADOS A PROCEDIMIENTOS.

Para los riesgos operativos asociados a procedimientos, estos serán responsabilidad de cada área en toda la fase de desarrollo de identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos que puedan afectar la misionalidad del área.

18 SISTEMA DE ADMINISTRACIÓN DEL RIESGO DE LAVADO DE ACTIVOS Y DE LA FINANCIACIÓN DEL TERRORISMO (SARLAFT).

El Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo (SARLAFT) es el sistema de prevención y control que deben implementar los vigilados por la Superintendencia Nacional de Salud en Colombia, de acuerdo con

la circular externa No. 009 del 21 de abril de 2016 y 20211700000005-5 de 2021, a través de las cuales, se presentan las normas o estándares y definición de los lineamientos para que el sector salud pueda realizar una implementación correcta y ajustada a las necesidades del sector y de la empresa en particular.

Para la correcta implementación, gestión y actualización del Riesgos Lavado de Activos y Financiación del Terrorismo (LA/FT), el Hospital Militar Central aplicará lo dispuesto en los siguientes documentos:

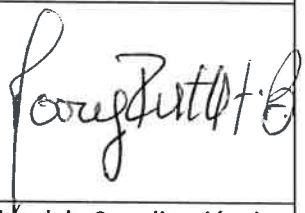
- Manual - Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo, código: GB-DIGE-MN-01.
- Manual - Subsistema de Administración de Riesgos de Corrupción, Opacidad y Fraude SICOF, código: GB-DIGE-MN-02.
- Matriz de Riesgos de Lavado de Activos y Financiación del Terrorismo, código: GB-DIGE-MN-01-FT-02.
- Política - Antisoborno y Soborno Transaccional, código: CA-CORE-PR-01-FT-05.
- Procedimiento – Medición del Riesgo de Corrupción, Opacidad, Fraude y Soborno en el HOSPITAL MILITAR CENTRAL, código: GB-DIGE-PR-10
- Procedimiento – Metodología de Gestión de Operaciones Inusuales y Sospechosas, código: GB-DIGE-PR-07.
- Formato – Reporte de Operaciones Inusuales, código: GB-DIGE-PR-07-FT-01.
- Formato – Seguimiento a Fuentes Informativas Externas, Código: GB-DIGE-PR-08-ft-02.
- Procedimiento: Monitoreo al Sistema de Administración y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo, código: GB-DIGE-PR.08
- Programa de Transparencia y Ética Empresarial, código: PL-OAPL-PR.10.FT.01

Lo anterior, está bajo la responsabilidad del funcionario que desempeñe las funciones del Oficial de Cumplimiento titular o suplente.

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
ACTIVIDADES QUE SUFRIERON CAMBIOS		OBSERVACIONES DEL CAMBIO	MOTIVOS DEL CAMBIO	FECHA DEL CAMBIO
ID	ACTIVIDAD			
1	Primeraversión del Documento	N.A.	N.A.	18 de Diciembre de 2018_V1
		Documento ajustado al formato institucional vigente.	Cambio código	25 de

CONTROL DE CAMBIOS				
ACTIVIDADES QUE SUFRIERON CAMBIOS		OBSERVACIONES DEL CAMBIO	MOTIVOS DEL CAMBIO	FECHA DEL CAMBIO
ID	ACTIVIDAD			
2	Actualización Política Operativa para la Administración del Riesgo.	Inclusión marco legal. Definición de roles y responsabilidades de las líneas dedefensa. Identificación de riesgos de seguridad digital. Análisis y evaluación del diseño del control. - Fechas de reporte.	versión anterior: PL-OAPL-PR-05-DI-01	noviembre de2020
3	Actualización y precisión de algunos elementos metodológicos.	Estructura para la redacción adecuada del riesgo. Factores de riesgo y la relación con las tipologías de riesgos (se precisan los factores de riesgo y su relación con las tipologías de riesgo). Criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de Severidad	Cambio código formatos.	07 de Septiembre de 2021
4	Actualización	Actualización de roles y responsabilidades del esquema de líneas de defensa. Identificación de nuevos riesgos por parte de los líderes de proceso. Acciones ante los riesgos materializados. Acciones de autocontrol por parte de los líderes de proceso. Criterios para calificar el impacto en riesgos de corrupción. Lineamientos frente a riesgos de seguridad digital. Cambio en las fechas de reporte, monitoreo y seguimiento.	Actualización metodológica.	Julio de 2022
	Actualización lineamientos política para la operación de riesgos	Actualización lineamientos a partir del cumplimiento para la plataforma estratégica, alineado a las necesidades de la institución para la definición, valoración y seguimiento de los riesgos	Actualización metodológica	30 de noviembre de 2023

APROBACIÓN				
	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
ACTUALIZÓ	Nicolás Corredor Ramírez	Contratista Oficina Asesora de Planeación	Noviembre de 2023	
REVISÓ	**Dra.** Mary Ruth Fonseca	Jefe de Oficina Asesora del Sector Defensa – Oficina Asesora de Planeación	Noviembre de 2023	
APROBÓ	**La presente política se encuentra aprobado por el Comité Institucional de Coordinación de Control Interno (Acta de aprobación del día 30 de noviembre de 2023)**			
PLANEACIÓN –CALIDAD **Revisión Metodológica**	**SMSM.** Pilar Adriana Duarte Torres	Servidor Misional en Sanidad Militar – Área Gestión de Calidad	Noviembre de 2023