

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
		<b>FECHA: 08/01/2021</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>TRD:</b> <b>PÁGINA: 1 de 62</b>

## Contenido

1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO.....	3
1.1. Objetivo General.....	3
1.2. Objetivos Específicos .....	3
1.3 Alcance .....	3
1.4 Contexto Entidad .....	4
1.5 Términos y definiciones .....	4
1.6 Características básicas de los proveedores de insumos y medicamentos .....	6
1.7 Política general de administración del riesgo.....	7
1.8 Revisión de la política.....	7
1.9 Estructura para la gestión del Riesgo .....	7
1.10 Marco conceptual para el apetito del riesgo .....	10
2. IDENTIFICACIÓN DEL RIESGO .....	12
2.1 Análisis y Definición de Objetivos .....	12
2.2 Identificación de los puntos de riesgo .....	12
2.3 Identificación de áreas de impacto.....	13
2.4 Identificación de áreas de factores de riesgo .....	13
2.5 Descripción del riesgo .....	15
2.6 Clasificación del riesgo .....	17
3. VALORACIÓN DEL RIESGO .....	19
3.1 Análisis de riesgos.....	19
<b>3.1.1 Determinar la probabilidad.....</b>	<b>19</b>
<b>3.1.2 Determinar el impacto .....</b>	<b>21</b>
3.2 Evaluación de riesgos.....	22
<b>3.2.1 Análisis preliminar (riesgo inherente).....</b>	<b>23</b>
<b>3.2.2 Evaluación de los riesgos para medir la exposición de la ESE a los impactos del riesgo</b>	<b>23</b>
<b>3.2.3 Valoración de controles .....</b>	<b>24</b>
<b>3.2.4 Nivel de riesgo (riesgo residual).....</b>	<b>27</b>
3.3 Estrategias para combatir el riesgo.....	30
3.4 Herramientas para la gestión del riesgo.....	31
<b>3.4.1 Gestión de eventos .....</b>	<b>31</b>
<b>3.4.2 Indicadores clave de riesgo.....</b>	<b>31</b>
4. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN .....	35

4.1. Disposiciones generales .....	35
4.2. Generalidades acerca de los riesgos de corrupción .....	36
4.3. Identificación del riesgo de corrupción. ....	38
<b>4.3.1 Procesos, procedimientos o actividades susceptibles de riesgos de corrupción.....</b>	<b>38</b>
<b>4.3.2 Lineamientos para la identificación del riesgo de corrupción .....</b>	<b>40</b>
4.4. Valoración del riesgo .....	41
<b>4.4.1. La determinación de la probabilidad .....</b>	<b>41</b>
<b>4.4.2. La determinación del impacto .....</b>	<b>42</b>
<b>4.4.3. Análisis preliminar (riesgo inherente).....</b>	<b>43</b>
<b>4.4.4. Valoración de controles .....</b>	<b>44</b>
5. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN .....	48
5.1. Identificación de los activos de seguridad de la información .....	48
5.2. Identificación del riesgo .....	50
5.3. Valoración del riesgo .....	53
5.4. Controles asociados a la seguridad de la información .....	57
6. ESTRUCTURA ORGANIZACIONAL: ROLES Y RESPONSABILIDADES .....	60
6.1 Representante Legal .....	60
6.2 Oficial de Cumplimiento o Persona Encargada.....	60
6.3 Comité de Riesgos .....	61
6.4 Área de Gestión de Riesgos o Área Encargada .....	61
6.5 Líderes de Procesos.....	62
7. SUBSISTEMAS DE RIESGOS .....	63
8. MONITOREO Y REVISIÓN .....	63
8.1. RESPONSABLES DE LOS PROCESOS .....	63
8.2. REPORTE PLAN DE TRATAMIENTO DE RIESGOS CONSOLIDAR INFORMACIÓN PARA LA GESTIÓN DEL RIESGO.....	64
8.3. INDICADORES - GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL .....	65
8.4. SEGUIMIENTO RIESGOS DE CORRUPCIÓN .....	66
9. COMUNICACIÓN Y CONSULTA.....	67

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 3 de 62</b>

## 1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Teniendo en cuenta que el Decreto 1083 de 2015 en su artículo 4 establece que la Administración del riesgo es parte integral del fortalecimiento de los Sistemas de Control Interno en las entidades públicas y determina que las autoridades correspondientes deberán establecer y aplicar políticas para su gestión, el Hospital Departamental San Rafael de Zarzal Valle a continuación establece los lineamientos para la gestión del riesgo aplicable en todos los niveles de la entidad.

Dicha política se asienta sobre las siguientes bases:

### 1.1. Objetivo General

Generar una cultura de conocimiento y manejo de los riesgos que prevengan la ocurrencia de situaciones o eventos que tengan un impacto o consecuencia sobre el cumplimiento de la misión y objetivos estratégicos, generando un ambiente de control al interior de la E.S.E. Hospital Departamental San Rafael de Zarzal.

### 1.2. Objetivos Específicos

- Desplegar a todos los niveles de la organización, los lineamientos institucionales frente a la gestión del riesgo, fortaleciendo el compromiso de los colaboradores y la cultura de prevención y autocontrol.
- Gestionar y administrar los riesgos establecidos en los procesos para evitar su materialización.
- Dotar a la institución de una herramienta útil que facilite la administración integral de gestión de riesgos.
- Establecer mecanismos para identificar, valorar, minimizar y monitorear los riesgos a los que constantemente está expuesta la Entidad.
- Garantizar el cumplimiento de los requisitos normativos en cuanto a la administración y gestión de riesgos, protegiendo los recursos públicos a través de acciones que permitan reducir, mitigar o eliminar la materialización de riesgos.

### 1.3 Alcance

La política de riesgos es aplicable a todos los procesos, procedimientos y proyectos de la E.S.E. Hospital Departamental San Rafael de Zarzal y a todas las acciones ejecutadas por los servidores públicos durante el ejercicio de sus funciones.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 4 de 62</b>

## 1.4 Contexto Entidad

El HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL es una Empresa Social del Estado entendida como categoría especial, de entidad pública descentralizada del Orden Departamental, dotada de personería jurídica, patrimonio propio y autonomía administrativa conforme lo establece la Ordenanza 076 del 30 de septiembre de 1996, la cual contribuye al mejoramiento de la calidad de vida de la comunidad Zarzaleña Y Municipios circunvecinos.

La Institución ofrece servicios de I y II Nivel de complejidad a toda la población zarzaleña y los municipios circunvecinos como lo son la Unión, la victoria, Versalles, toro, Obando y Cartago, siendo integrando a la red pública hospitalaria en la zona norte del departamento.

Entre los servicios incorporados al portafolio de servicios de la entidad, se encuentran hospitalización, consulta externa, quirúrgicos, urgencias, transporte asistencial, apoyo diagnóstico, programa específica de detención temprana, consulta médica especializada, imagenología (Rayos x y ecografías) entre otros.

Como Institución Prestadora de Servicios de Salud (I.P.S.) de Nivel Dos (2) de Atención, el Hospital Departamental San Rafael de Zarzal E.S.E., brinda Servicios de Baja y Mediana Complejidad y, a través del mejoramiento continuo mantiene la calidad de los servicios para la satisfacción permanente del usuario, aplicando los principios de equidad, justicia y universalidad. La ética y la humanización rigen las relaciones con la comunidad y con las demás entidades relacionadas con la Institución.

Los servicios prestados se facturan de acuerdo al Manual de Tarifas aprobado por la Junta Directiva de la Empresa y lo establecido en los contratos, convenios o de acuerdo a los mecanismos que haya definido el Gobierno Nacional para este fin. Los recursos se administran con criterios de eficiencia, eficacia y efectividad y los resultados económicos son orientados al mejoramiento de la Empresa en función del cumplimiento y fortalecimiento de su capacidad resolutoria y buscan incrementar la cobertura del servicio optimizando los recursos para el crecimiento institucional.

## 1.5 Términos y definiciones

**Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

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

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 5 de 62</b>

**Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

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

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

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

**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

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

**Control:** Medida que permite reducir o mitigar un riesgo.

**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

**Factores de Riesgo:** Son las fuentes generadoras de riesgos.

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

**Integridad:** Propiedad de exactitud y completitud.

**Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser "Probabilidad \* Impacto", sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

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

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

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 6 de 62</b>

**Riesgo:** Efecto que se causa sobre los objetivos de las entidades, 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 Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

**Riesgo de 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 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.

**Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

**Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

**Usuario:** Es toda persona natural a la que, sin ser cliente y/o contratista y/o proveedor, la entidad le suministra o presta un servicio de salud.

## 1.6 Características básicas de los proveedores de insumos y medicamentos

La E.S.E. Hospital Departamental San Rafael de Zarzal prefiere contar con proveedores con cercanía geográfica, comprometidos con el medio ambiente, que ofrezcan productos de excelente calidad y precios competitivos, con respaldo técnico, respetuosos de las decisiones de compra del Hospital, que otorguen condiciones comerciales y financieras de acuerdo con la oportunidad de pago del Hospital y que cuenten con la capacidad y cumplimiento de las entregas que el Hospital requiere.

Los proveedores deben cumplir los requerimientos, normas y buenas prácticas de identificación, empaque, protección, almacenamiento y transporte de los insumos y medicamentos

Los proveedores deben cumplir con la documentación requerida por el Hospital y los requerimientos del Manual de contratación y los Sistemas de Riesgos

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 7 de 62</b>

## 1.7 Política general de administración del riesgo

El Hospital Departamental San Rafael de Zarzal Valle, declara que en el desarrollo de sus actividades hay una probabilidad de ocurrencia de riesgos que conllevan a un impacto negativo en el cumplimiento de sus objetivos, por lo cual se compromete a adoptar mecanismos y acciones necesarias para la gestión integral de los mismos que prevengan o minimicen su impacto.

Para ello adoptará mecanismos que permitan la identificación, análisis, valoración, seguimiento y control de los riesgos propios de su actividad, acogiendo una autorregulación prudencial. El Hospital Departamental San Rafael determinará su nivel de exposición concreta a los impactos de cada uno de los riesgos para priorizar su tratamiento, y estructurar criterios orientadores en la toma de decisiones respecto de los efectos de los mismos basados en los lineamientos para administración del riesgo dados por el departamento administrativo de la función pública.

El representante del Hospital designa al área de planeación como responsable de la implementación, monitoreo y revisión del Sistemas de Administración Integral de Riesgos

## 1.8 Revisión de la política

Esta Política será revisada al menos 1 vez cada año y cuando se considere necesario por parte de la Junta Directiva, el Representante legal o Jefe de la Oficina de Control Interno, con el fin de determinar si es coherente con la Planeación Estratégica de la ESE, los cambios en la normatividad o políticas estatales, al igual si contempla las opciones de tratamiento del riesgo que permitan tomar decisiones oportunas y adecuadas por la dirección y sea una guía de acción para todos los servidores públicos.

La revisión de la política de riesgos tanto por la Gerencia como por el Comité de riesgos u Oficina de Control Interno busca garantizar que el perfil de riesgos camine alineado a las Políticas Institucionales y Planeación Estratégica.

## 1.9 Estructura para la gestión del Riesgo

La estructura para el análisis de contexto, la identificación y valoración del riesgo que deberá ser aplicada por los procesos está determinada por la metodología para la Administración del Riesgo emitida por el Departamento Administrativo de la Función Pública versión 5.

A partir de dichos lineamientos, específicamente para el análisis de probabilidad e impacto de los riesgos, se establecen tablas o matrices generales tomadas de la Guía Para La Administración del Riesgo versión 5, la cual será la base de trabajo para todo el componente de administración del Riesgo para el Hospital Departamental de Zarzal Valle.

Teniendo en cuenta la institucionalidad del riesgo esta se administra conforme a la siguiente figura:

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – Ext 104, Ext 221, Urgencias 2221011

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)

[gerencia@hospitalsanrafaelzarzal.gov.co](mailto:gerencia@hospitalsanrafaelzarzal.gov.co) – [siau@hospitalsanrafaelzarzal.gov.co](mailto:siau@hospitalsanrafaelzarzal.gov.co)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 8 de 62</b>

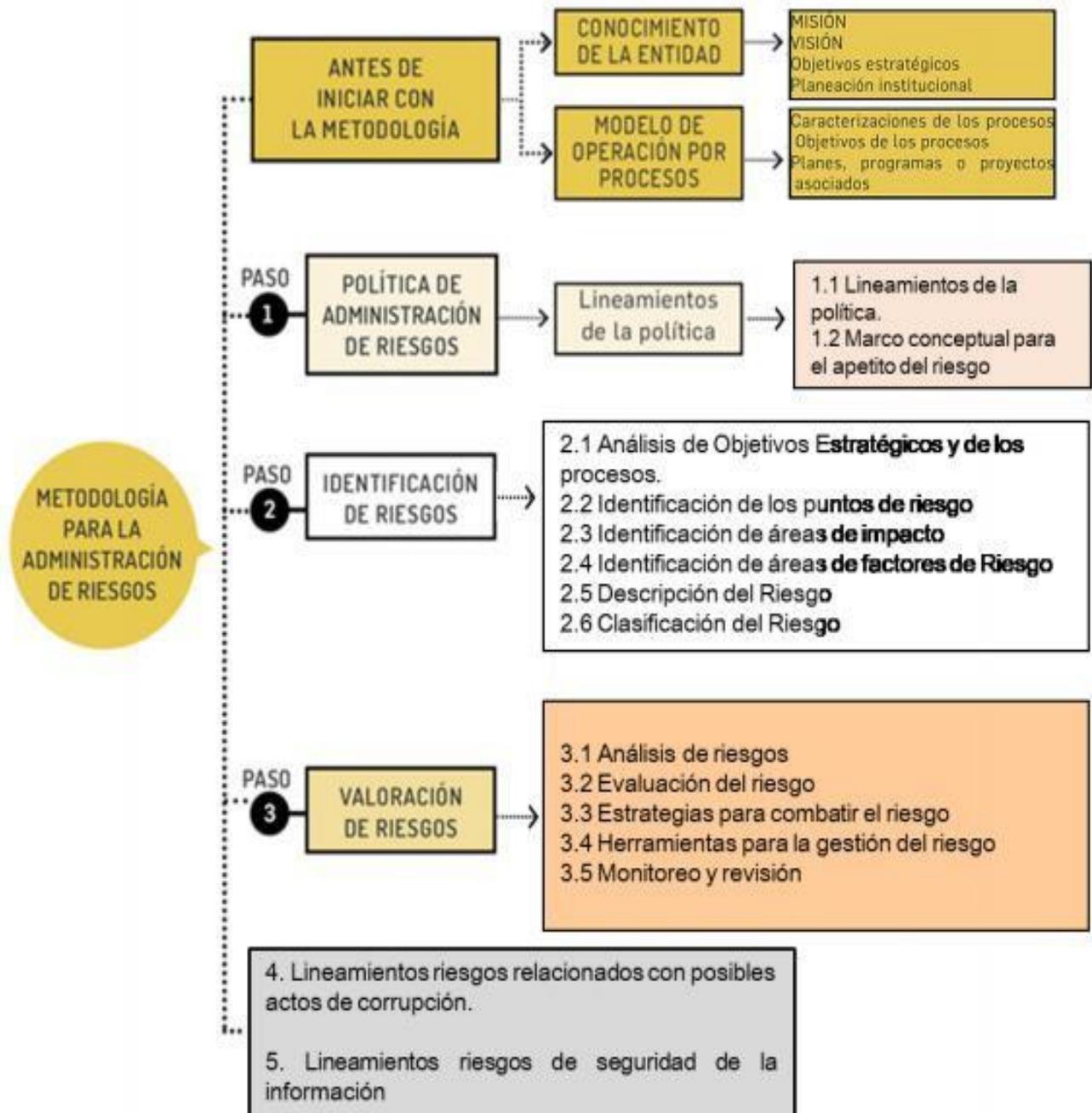
Figura 1. Operatividad Institucionalidad para la Administración del Riesgo



**Fuente:** Dirección de gestión y desempeño institucional de función pública, 2020.

En cuanto a la metodología utilizada se respalda en la proporcionada por la guía de administración del riesgo versión 5 así:

Figura 2. Metodología para la administración del riesgo



**Fuente:** Elaborado y actualizado por la dirección de gestión y desempeño institucional de función pública, 2020.

## 1.10 Marco conceptual para el apetito del riesgo

Teniendo en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación, se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis en cada una de las entidades, iniciando con las siguientes definiciones:

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual las altas direcciones consideran que no sería posible el logro de los objetivos de la entidad.

Gráficamente los anteriores conceptos se relacionan así:

Figura 6. Definiciones de apetito, tolerancia y capacidad de riesgo



**Fuente:** Tomado de la guía de buenas prácticas de gestión de riesgos del instituto de auditores internos (IIA global), junio de 2013.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 11 de 62</b>

## Determinación de la capacidad de riesgo

La entidad debe aplicar los valores de probabilidad e impacto contenidos en esta Guía y con base en esto debe determinar, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

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

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

## Determinación del apetito de riesgo

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

Este valor se denomina “apetito de riesgo”, dado que equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

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

## Tolerancia de riesgo

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

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

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

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

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 12 de 62</b>

## 2. IDENTIFICACIÓN DEL RIESGO

### 2.1 Análisis y Definición de Objetivos

Previo a un análisis y conocimiento de la entidad desde el modelo de operación por procesos, y la planeación institucional, le corresponde a la Segunda Línea de Defensa, el análisis de los objetivos de la entidad tanto del orden estratégico como de procesos.

- Análisis de objetivos estratégicos.** La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.  
 Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).
- Análisis de los objetivos de proceso.** Los objetivos de proceso deben ser analizados con base en las características mínimas, pero, además, se debe revisar que los mismos estén alineados con la misión y la visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.

### 2.2 Identificación de los puntos de riesgo

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

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b> <b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b> <b>TRD:</b> <b>PÁGINA: 13 de 62</b>

Figura 3. Cadena de valor



**Fuente:** Dirección de gestión y desempeño institucional de función pública, 2017.

## 2.3 Identificación de áreas de impacto

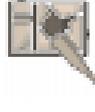
El área de impacto es la consecuencia económica o reputación a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputación.

## 2.4 Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la Tabla 1 encontrará un listado con ejemplos de factores de riesgo que puede tener una entidad.

Tabla 1. Factores de riesgo

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

**Fuente:** Adaptado del curso riesgo operativo de la Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

NOTA: Los factores relacionados son una guía, cada entidad puede analizar los que considere de acuerdo con la complejidad propia de cada entidad y con sector en el que se desenvuelve, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo.

## 2.5 Descripción del riesgo

la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase posibilidad de y se analizan los siguientes aspectos:

Figura 4. Estructura propuesta para la redacción del riesgo



**Fuente:** Adaptado del curso riesgo operativo de la Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 16 de 62</b>

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

*Desglosando la estructura propuesta tenemos:*

- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Es la causa principal o básica, corresponden a las razones por las cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o subcausas que pueden ser analizadas.

## **PREMISAS PARA UNA ADECUADA REDACCIÓN DEL RIESGO**

- No describir como riesgos omisiones ni desviaciones del control.  
Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- No describir causas como riesgos  
Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
- No describir riesgos como la negación de un control.  
Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.
- No existen riesgos transversales, lo que pueden existir son causas transversales.  
Ejemplo: pérdida de expedientes. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

## 2.6 Clasificación del riesgo

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

Tabla 2. Clasificación de riesgos

<b>Ejecución y administración de procesos</b>	Pérdidas derivadas de errores en la ejecución y administración de procesos.
<b>Fraude externo</b>	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
<b>Fraude interno</b>	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 está 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.
<b>Fallas tecnológicas</b>	Errores en <i>hardware</i> , <i>software</i> , telecomunicaciones, interrupción de servicios básicos.
<b>Relaciones laborales</b>	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.
<b>Usuarios, productos y prácticas</b>	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
<b>Daños a activos fijos/ eventos externos</b>	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

Teniendo en cuenta que en la Tabla 2 se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b> <b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b> <b>TRD:</b> <b>PÁGINA: 18 de 62</b>

Figura 05. Relación entre factores de riesgo y clasificación del riesgo

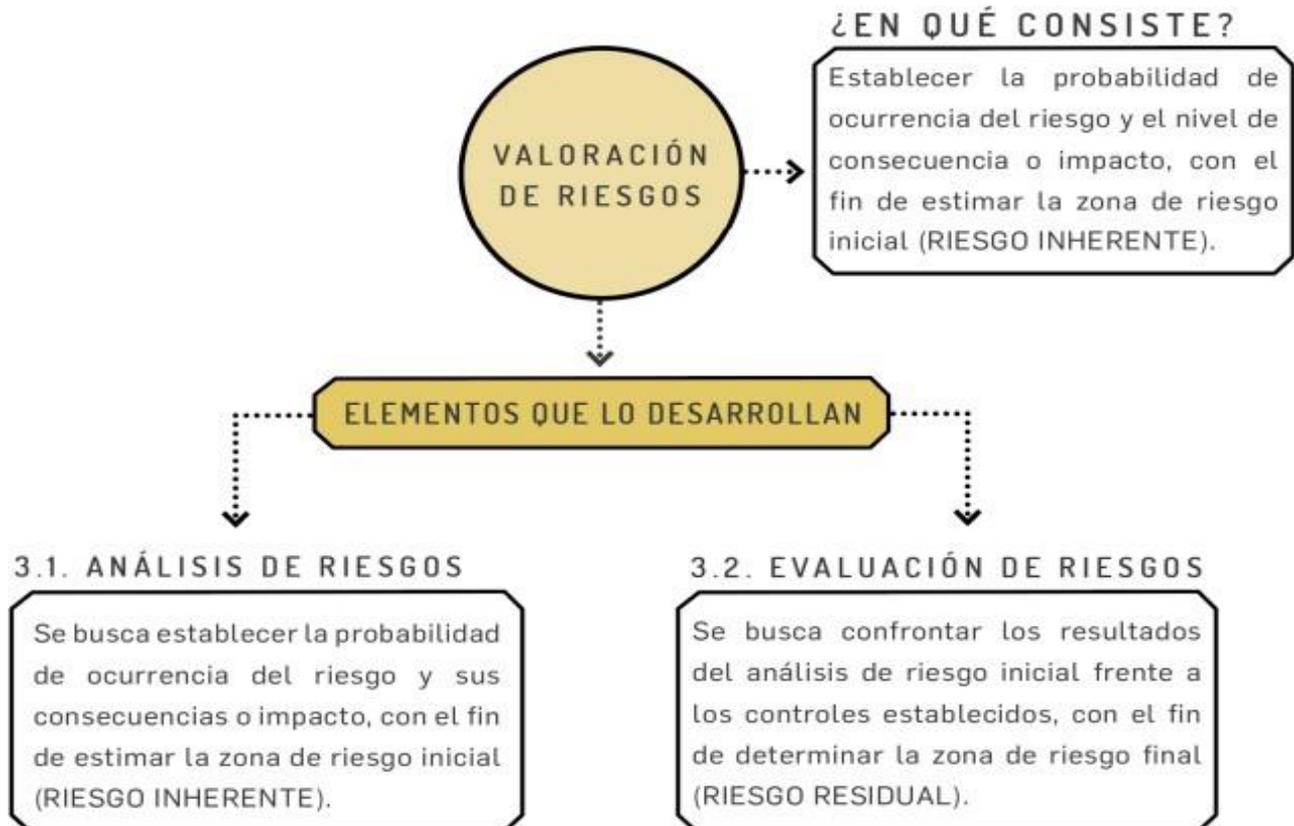


**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 19 de 62</b>

### 3. VALORACIÓN DEL RIESGO

Figura 7. Estructura para el desarrollo de la valoración del riesgo



**Fuente:** Dirección de gestión y desempeño institucional de función pública, 2018.

### 3.1 Análisis de riesgos

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

#### 3.1.1 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.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 20 de 62</b>

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

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

Tabla 3. Actividades relacionadas con la gestión en entidades públicas

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
<p><b>*Tecnología (incluye disponibilidad de aplicativos), tesorería</b></p> <p><b>*Nota:</b> En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.</p> <p>Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.</p>	Diaria	Muy alta

**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 4 se establecen los criterios para definir el nivel de probabilidad.

Tabla 4. Criterios para definir el nivel de probabilidad

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

**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

Nota: Dependiendo del tamaño y complejidad de los procesos de la entidad, la tabla 4 podrá ser ajustada o adaptada a las necesidades de cada entidad.

### 3.1.2 Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputaciones como las variables principales. Cabe señalar que en la versión 2018 de la Guía de administración del riesgo 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 reputaciones en la versión 2020.

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

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

En la tabla 5 se establecen los criterios para definir el nivel de impacto.

Tabla 5. Criterios para definir el nivel de impacto

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

**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

**Nota:** Dependiendo del tamaño y complejidad de los procesos en la entidad, la tabla 5 podrá ser ajustada o adaptada a sus necesidades.

**IMPORTANTE:** Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

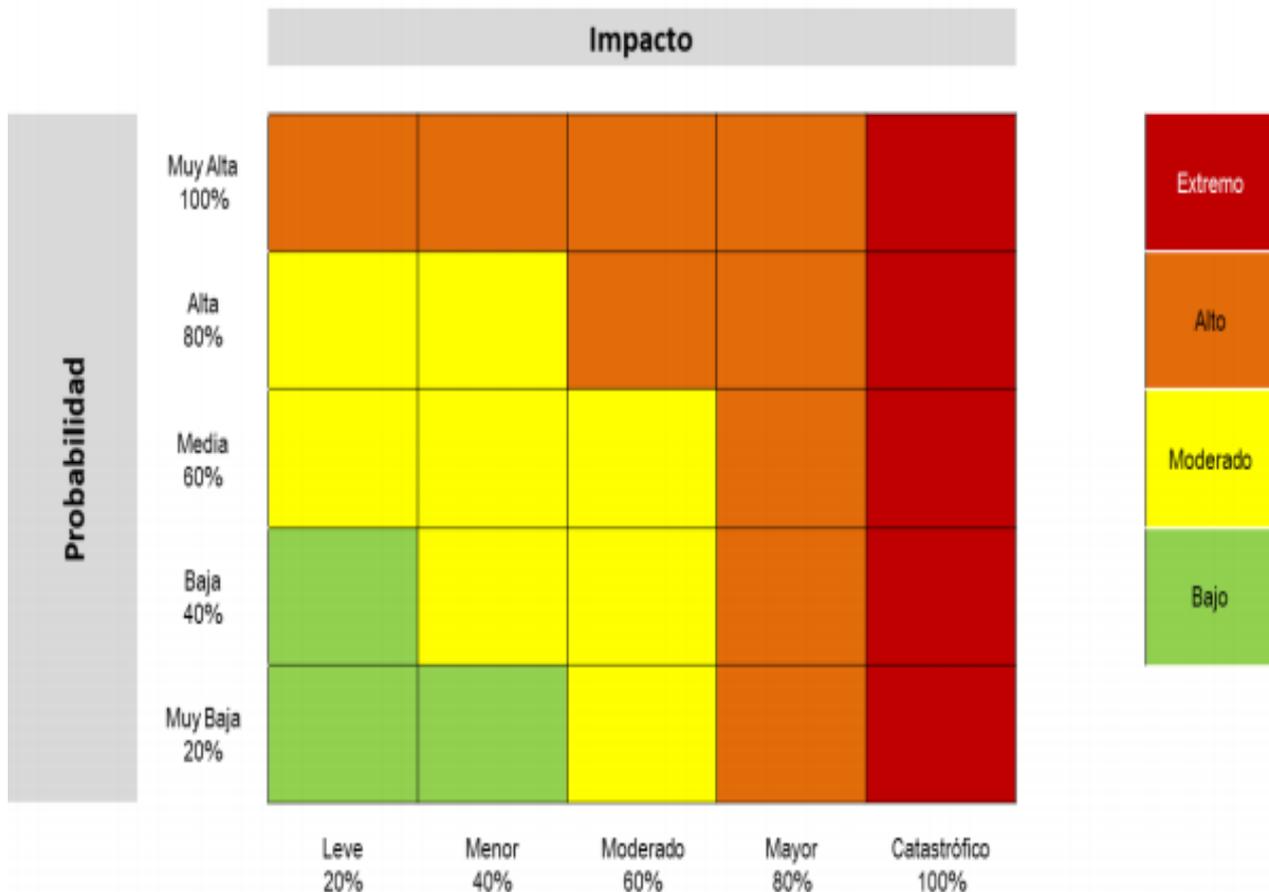
### 3.2 Evaluación de riesgos

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

### 3.2.1 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 (ver figura 8).

Figura 8. Matriz de calor (niveles de severidad del riesgo)



**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

### 3.2.2 Evaluación de los riesgos para medir la exposición de la ESE a los impactos del riesgo

Tratamiento del riesgo consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder establecer mecanismos de administración de los riesgos, así como niveles de tolerancia o aceptación de los riesgos identificados.

- Se determina el apetito de riesgo **MODERADO** como nivel de riesgo aceptable para la institución, por lo tanto, todos los riesgos definidos en la matriz de riesgos deben quedar con riesgo inherente **BAJO** o **MODERADO**.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 24 de 62</b>

b) El Hospital tolera o acepta los riesgos que se encuentren en zona residual **BAJA** y **MODERADA**, los riesgos en estas zonas cumplen con los criterios de aceptación de riesgo, no es necesario, para estos establecer acciones de control preventivas que permitan reducir la probabilidad de ocurrencia del riesgo, más sin embargo si no se presentan riesgos en zona **EXTREMA** se conservará la misma metodología priorizando la zona de más alta a la zona baja de riesgo.

c) Se priorizan los riesgos del Hospital que se consideren en **ALTO** o **EXTREMO** o que sean de CORRUPCIÓN, se deben incluir en la matriz de riesgos y se establecen acciones de control preventivas que permitan mitigar la materialización del riesgo.

d) Riesgos de Corrupción no son aceptables bajo ninguna circunstancia

### 3.2.3 Valoración de controles

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

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

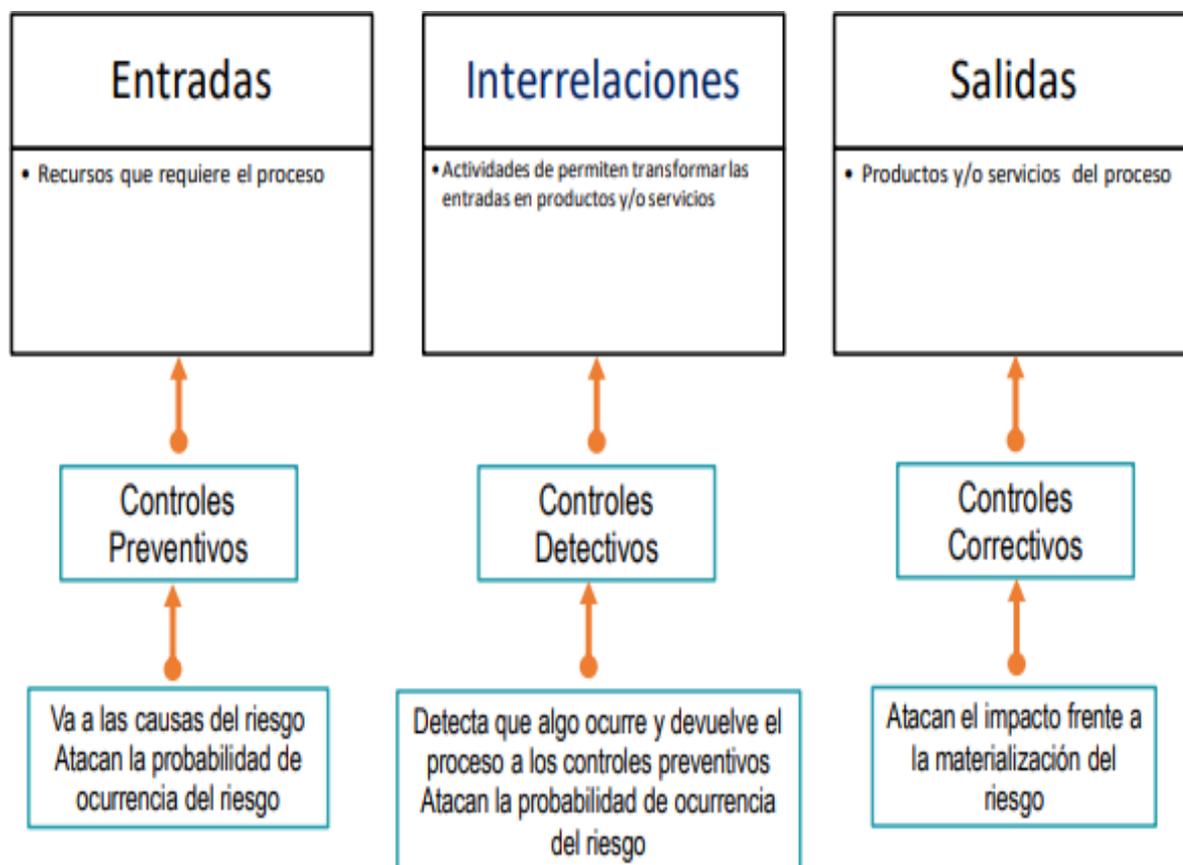
**3.2.3.1 Estructura para la descripción del control:** Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

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

**3.2.3.2 Tipología de controles y 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:

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>		<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 25 de 62</b>

Figura 9. Ciclo del proceso y las tipologías de controles



**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

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

- Control preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- Control detectivo: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- Control correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- Control manual: Controles que son ejecutados por personas.
- Control automático: Son ejecutados por un sistema.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 26 de 62</b>

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

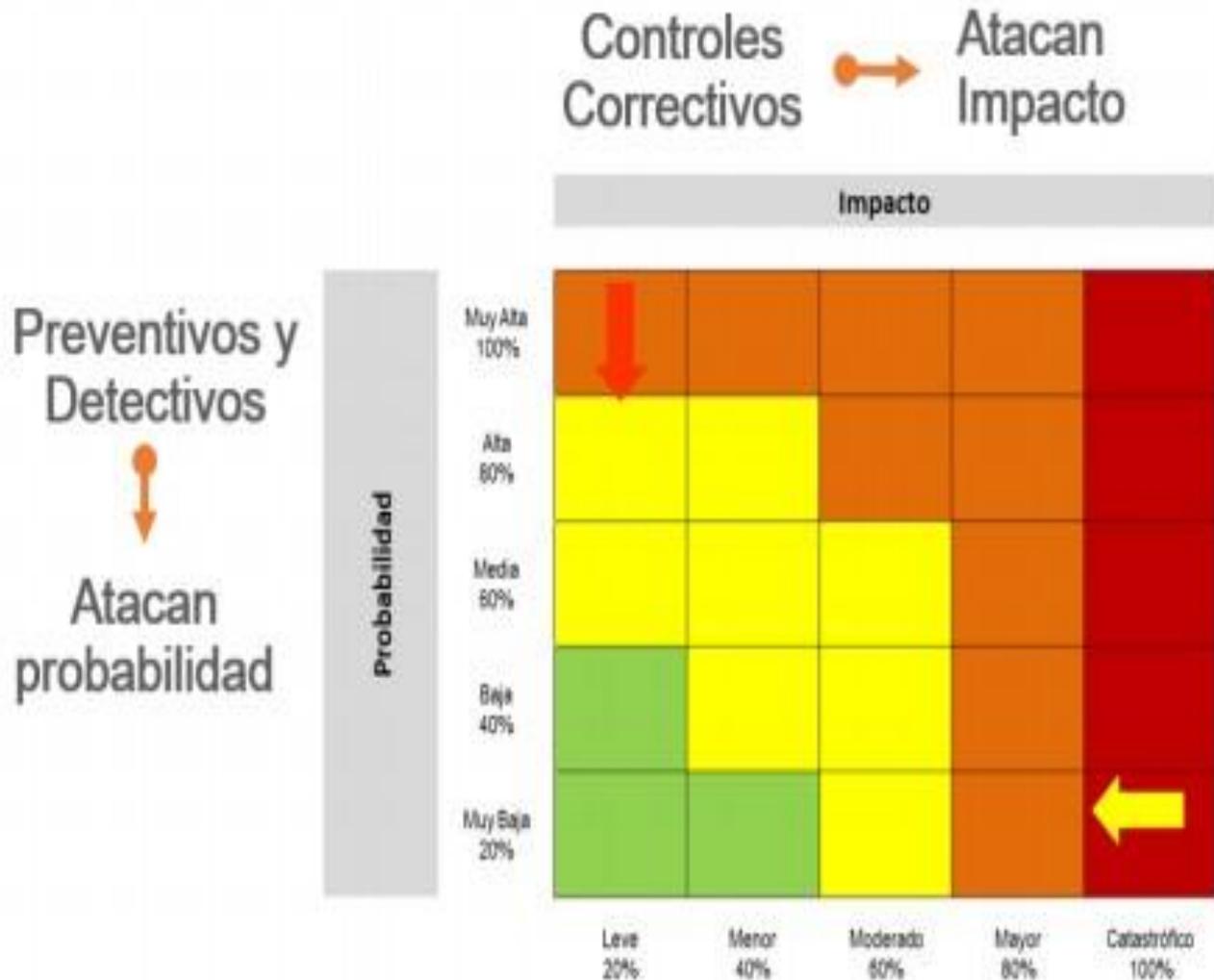
Tabla 6. Atributos para el diseño del control

Características		Descripción	Peso	
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la	25%
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

**Fuente:** Adaptado del curso riesgo Operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

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.

Figura 10. Movimiento en la matriz de calor acorde con el tipo de control



**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

### 3.2.4 Nivel de riesgo (riesgo residual)

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

## FORMATO MAPA DE RIESGOS

Parte 1. Identificación del riesgo:

Proceso:											
Objetivo:											
Alcance:											
Referencia	Impacto	Causa inmediata	Causa raíz	Descripción del riesgo	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente
1											

Parte 2. Valoración del riesgo:

No. control	Descripción del control	Afectación		Atributos					Probabilidad residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia							
1															

Parte 3. Planes de acción (Para la opción de tratamiento reducir):

Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado

**Fuente:** Adaptado del curso riesgo operativo Universidad del Rosario por la dirección de gestión y desempeño institucional de función pública, 2020.

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – Ext 104, Ext 221, Urgencias 2221011

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)  
[gerencia@hospitalsanrafaelzarzal.gov.co](mailto:gerencia@hospitalsanrafaelzarzal.gov.co) – [siau@hospitalsanrafaelzarzal.gov.co](mailto:siau@hospitalsanrafaelzarzal.gov.co)

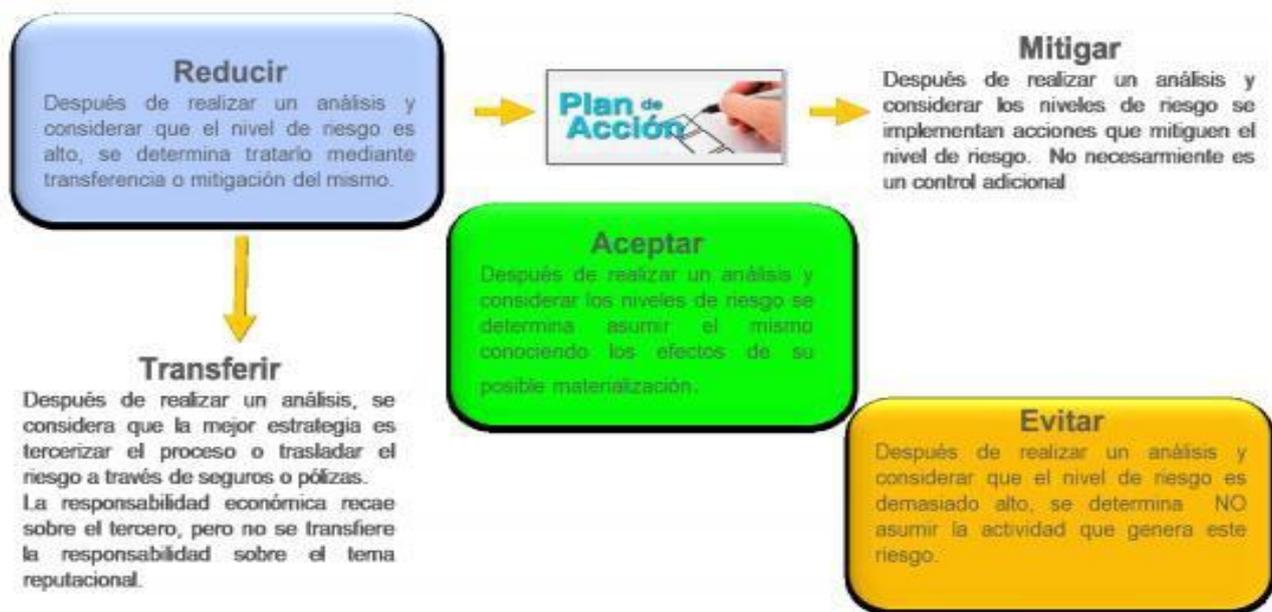
	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>		<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 30 de 62</b>

### 3.3 Estrategias para combatir el riesgo

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

En la figura 11 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Figura 11. Estrategias para combatir el riesgo



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

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

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

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca dentro del Plan de Continuidad de Negocio <sup>1</sup> y se consideraría un control correctivo.

<sup>1</sup> De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 31 de 62</b>

### 3.4 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:

#### 3.4.1 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

Este mecanismo 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)

#### 3.4.2 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. En la tabla 7 se muestran algunos ejemplos de estos indicadores.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 32 de 62</b>

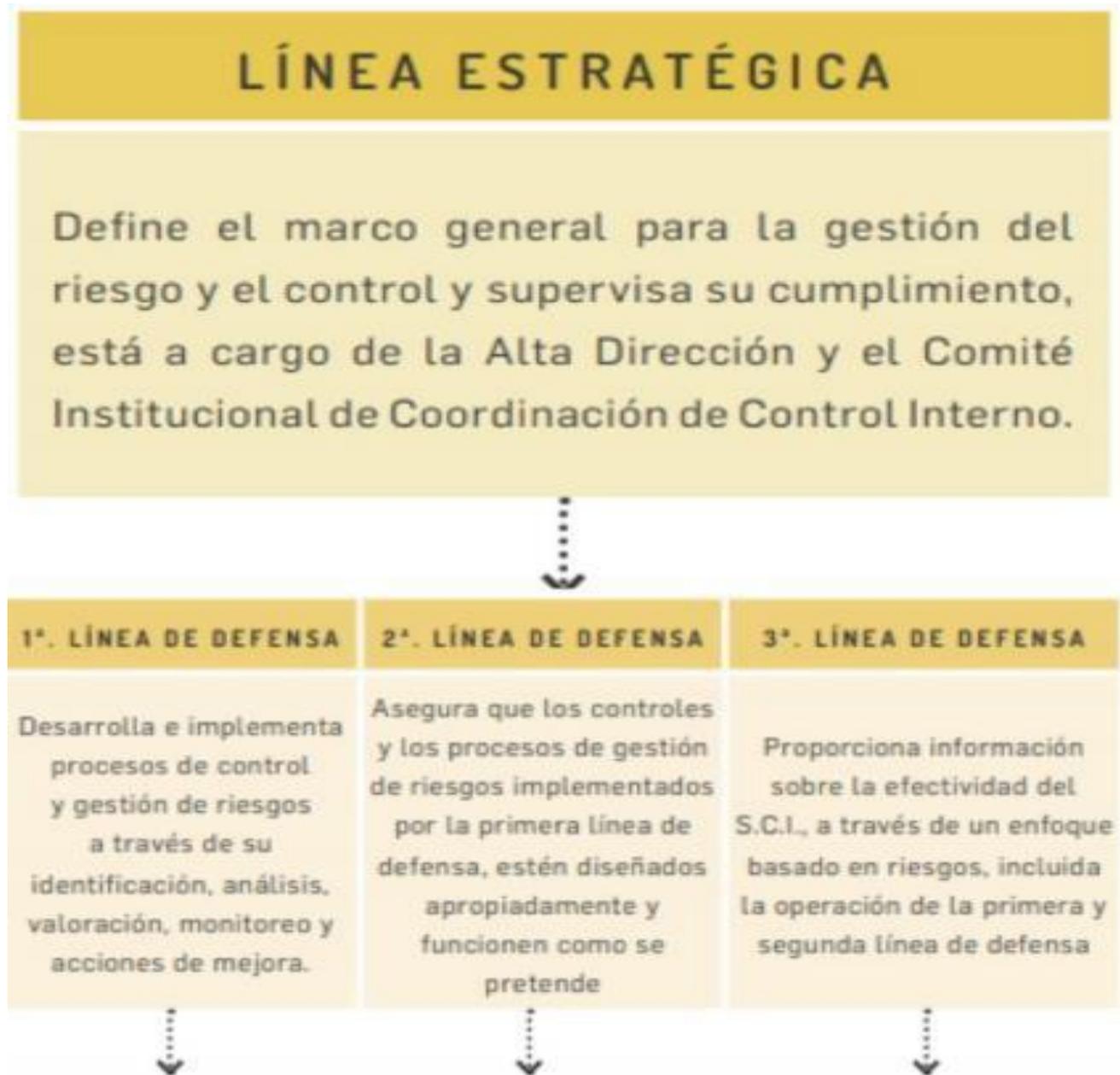
Tabla 7 Ejemplos indicadores clave de riesgo

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

**Fuente:** Adaptado del listado de indicadores y métricas ([www.riesgoscero.com](http://www.riesgoscero.com)) por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

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

Tabla 8. Esquema de líneas de defensa



A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.  
Rol principal: diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.

Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.

Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

A cargo de la oficina de control interno, auditoría interna o quien haga sus veces.

El rol principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I.

El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

**Fuente:** Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

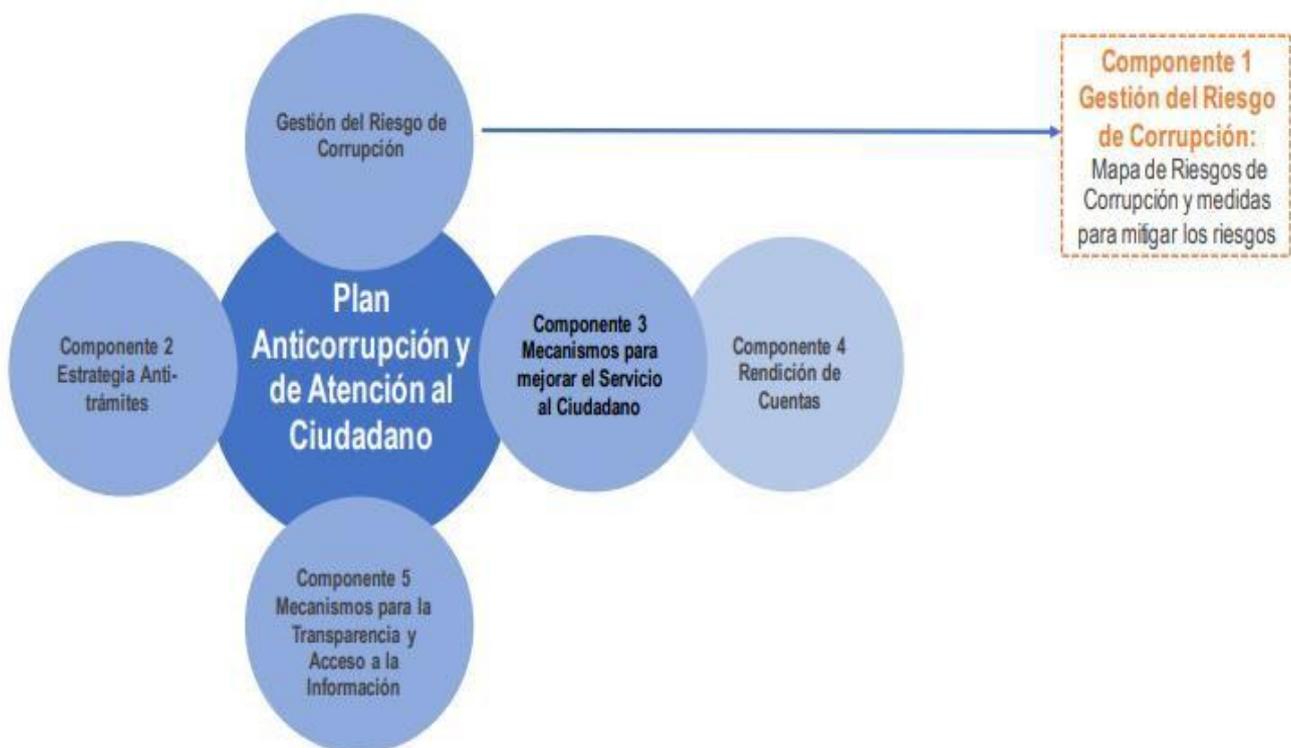
	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 35 de 62</b>

## 4. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

### 4.1. 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.

Figura 12. Componentes plan anticorrupción y de atención al ciudadano



**Fuente:** Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y la Secretaría de Transparencia, 2020.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 36 de 62</b>

En materia de riesgos asociados a posibles actos de corrupción, para la presente guía 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.

#### **4.2. Generalidades acerca de los riesgos de corrupción**

- Entidades encargadas de gestionar el riesgo: Lo deben adelantar las entidades del orden nacional, departamental y municipal.
- Se elabora anualmente por cada responsable de los procesos al interior de las entidades, junto con su equipo.
- 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.
- Monitoreo: En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- Seguimiento: El jefe de control interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

Teniendo en cuenta la criticidad del tema y que se requiere su publicación en página web, las entidades podrán anonimizar la información relacionada con los controles establecidos que pueden tener relación con información clasificada o reservada, como se muestra en el siguiente ejemplo:

Tabla 9. Ejemplo Información anonimizada

N.º	Riesgo	Clasificación	Causa	Probabilidad	Impacto	Riesgo Residual	Opción de Manejo	Actividad de Control
1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o para terceros...	Corrupción	Falta de...	Probable	Catastrófico	Catastrófico	Evitar	[Redacted]

**Información anonimizada**

**IMPORTANTE:**

Tenga en cuenta que la información clasificada o reservada la señala la ley, un decreto con fuerza de ley o convenio internacional ratificado por el Congreso o en la Constitución.

Una resolución no puede calificar la información como clasificada o reservada.

**Fuente:** Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y la Secretaría de Transparencia, 2018.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 38 de 62</b>

### 4.3. Identificación del riesgo de corrupción.

#### 4.3.1 Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

A manera de ilustración 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:

Tabla 10. Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

<b>Direccionamiento estratégico (alta dirección)</b>	<ul style="list-style-type: none"> <li>● Concentración de autoridad o exceso de poder. Extralimitación de funciones.</li> <li>● Ausencia de canales de comunicación.</li> <li>● Amiguismo y clientelismo.</li> </ul>
<b>Financiero (está relacionado con áreas de planeación y presupuesto)</b>	<ul style="list-style-type: none"> <li>● Inclusión de gastos no autorizados.</li> <li>● Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración.</li> <li>● Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.</li> <li>● Inexistencia de archivos contables.</li> <li>● Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.</li> </ul>

<p><b>De contratación (como proceso o bien los procedimientos ligados a este)</b></p>	<ul style="list-style-type: none"> <li>● Estudios previos o de factibilidad deficientes.</li> <li>● 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).</li> <li>● Pliegos de condiciones hechos a la medida de una firma en particular.</li> <li>● Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica).</li> <li>● Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación.</li> <li>● Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.</li> <li>● Urgencia manifiesta inexistente.</li> <li>● Concentrar las labores de supervisión en poco personal.</li> <li>● Contratar con compañías de papel que no cuentan con experiencia.</li> </ul>
<p><b>De información y documentación</b></p>	<ul style="list-style-type: none"> <li>● Ausencia o debilidad de medidas y/o políticas de conflictos de interés.</li> <li>● Concentración de información de determinadas actividades o procesos en una persona.</li> <li>● Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración.</li> <li>● Ocultar la información considerada pública para los usuarios.</li> <li>● Ausencia o debilidad de canales de comunicación</li> </ul>
<p><b>De Investigación y Sanción</b></p>	<ul style="list-style-type: none"> <li>● Inexistencia de canales de denuncia interna o externa.</li> <li>● Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este.</li> <li>● Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.</li> <li>● Exceder las facultades legales en los fallos.</li> </ul>
<p><b>De trámites y/o servicios internos y externos</b></p>	<ul style="list-style-type: none"> <li>● Cobros asociados al trámite.</li> <li>● Influencia de tramitadores.</li> <li>● Tráfico de influencias: (amiguismo, persona influyente).</li> </ul>
<p><b>De reconocimiento de un derecho (expedición de licencias y/o permisos)</b></p>	<ul style="list-style-type: none"> <li>● Falta de procedimientos claros para el trámite</li> <li>● Imposibilitar el otorgamiento de una licencia o permiso.</li> <li>● Tráfico de influencias: (amiguismo, persona influyente).</li> </ul>

Fuente: Secretaría de Transparencia, 2018.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 40 de 62</b>

### 4.3.2 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?

**Definición 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”.*  
(Conpes N° 167 de 2013)

Es necesario que en la descripción del riesgo concurren los componentes de su definición, así:

**Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.**

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción porque 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:

Tabla 11. Matriz para la definición del riesgo de corrupción

<b>MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN</b>				
<b>Descripción del riesgo</b>	<b>Acción u omisión</b>	<b>Uso del poder</b>	<b>Desviar la gestión de lo público</b>	<b>Beneficio privado</b>
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: Secretaría de Transparencia de la Presidencia de la República.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 41 de 62</b>

Tabla 12 Ejemplo riesgo de corrupción

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
"Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad"	La combinación de factores como insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación, pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad, repercutiendo en la continuidad de su operación.	Operativo	Carencia de controles en el procedimiento de contratación  Insuficiente capacitación del personal de contratos  Desconocimiento de los cambios en la regulación contractual  Inadecuadas políticas de operación	1. Parálisis en los procesos 2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor 3. Demandas y demás acciones jurídicas 4. Detrimiento de la imagen de la entidad ante sus grupos de valor 5. Investigaciones disciplinarias

## 4.4 Valoración del riesgo

### 4.4.1. La determinación de la probabilidad

La determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.1. Es importante resaltar que la frecuencia a la que se hace referencia en 3.1.1 se relaciona con la ejecución de la actividad de la cual proviene el riesgo de corrupción. Es decir, se debe considerar desde el objetivo del proceso y su exposición al riesgo, en este sentido, y para este análisis, se retoma la tabla 4 definida en el aparte 3.1.1:

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

#### 4.4.2. 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 (ver tabla 13):

Tabla 13. Criterios para calificar el impacto en riesgos de corrupción

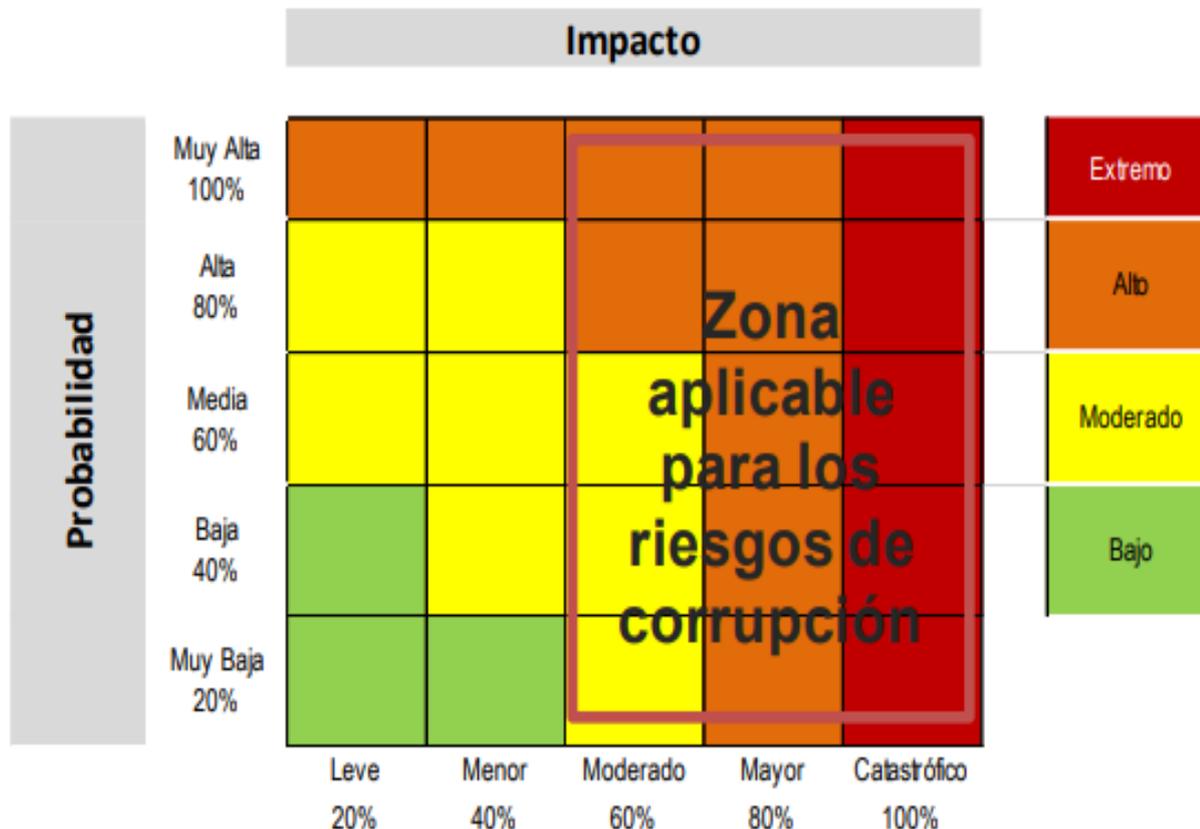
N.º	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		<b>10</b>	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Fuente: Secretaría de Transparencia de la Presidencia de la República.

#### 4.4.3. 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 establecida en el numeral 3.2.1 de la presente guía, 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 delimitan como se muestra a continuación:

Figura 13. Matriz de calor para riesgos de corrupción



**Fuente:** Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y la Secretaría de Transparencia, 2018.

#### 4.4.4. Valoración de controles

La valoración de los controles existentes establecido en el numeral 3.2.2, así como las demás disposiciones contenidas en el capítulo 3 de esta guía, son aplicables a la gestión del riesgo de corrupción.

A continuación, se desarrolla un ejemplo aplicando la metodología, atendiendo la siguiente información:

- Proceso: gestión de la contratación.
- Objetivo: ejecutar las etapas precontractual y contractual en las diferentes modalidades en esta materia, acorde con el plan anual de adquisiciones aprobado para cada vigencia.
- Alcance: inicia con el análisis de las contrataciones aprobadas en el plan anual de adquisiciones y termina con las compras y contrataciones requeridas y la asignación de supervisores o interventores (según aplique).

- Riesgo identificado: posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin celebrar un contrato.
- Número de veces que se ejecuta la actividad: las actividades de contratos implican 20 en el mes = 240 contratos en el año.
- Cálculo probabilidad: acorde con la anterior información, el nivel de probabilidad es MEDIA.
- Cálculo impacto: acorde con la tabla de criterios (19 preguntas), el nivel es MAYOR.

En la tabla 14 se desarrolla un ejemplo aplicando la metodología propuesta.

Formato mapa de riesgos

Parte 1 identificación del riesgo de corrupción:

Tabla 14. Ejemplo formato mapa riesgos de corrupción

Gestión de la contratación								
Ejecutar las etapas precontractual y contractual en las diferentes modalidades en esta materia, acorde con el plan anual de adquisiciones aprobado para cada vigencia.								
Inicia con el análisis de las contrataciones aprobadas en el plan anual de adquisiciones y termina con las compras, contrataciones requeridas y la asignación de supervisores o interventores (según aplique).								
* Referencia	Riesgo de corrupción	Clasificación riesgo	*Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente
1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin celebrar un contrato.	Ejecución y administración de procesos	240	media	60%	mayor	80%	alta

Parte 2 Valoración del riesgo:

N.º Control	Descripción del control	Afectación		Atributos				Probabilidad residual (2 controles)	Probabilidad residual Final	%	Impacto residual Final	%	Zona de riesgo final	Tratamiento		
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación								Frecuencia	Evidencia
1	Para la etapa precontractual, el (la) secretario(a) general, en el marco del comité de contratación, valida los estudios previos presentados por los líderes de proceso responsables de acuerdo con la modalidad de contratación en cada caso, las decisiones tomadas son registradas en las actas del comité, firmadas por los miembros de este, lo que permite continuar con las etapas subsiguientes de los	X		Preventivo	Manual	40%	Documentado	Continua	Con registro	36%	muy baja	25,2%	mayor	80%	alta	Reducir

N.º Control	Descripción del control	Afectación		Atributos				Probabilidad residual (2 controles)	Probabilidad residual Final	%	Impacto residual Final	%	Zona de riesgo final	Tratamiento	
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación								Frecuencia
	procesos contractuales correspondientes.														
2	Para la etapa contractual, el jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto (secretario(a) general). En el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	X		Detectivo	Manual	30%	Documentado	Continua	Con registro	25,2%					

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 47 de 62</b>

Parte 3 Planes de acción (para la opción de tratamiento reducir):

Plan de Acción	Responsable	Fecha implementación	Fecha seguimiento	Seguimiento	Estado
El jefe del área de contratos, como 2ª línea de defensa, mensualmente adelanta un análisis por modalidad de contratación sobre el avance y resultados con base en los informes de supervisión e interventoría y genera las alertas ante el Comité Institucional de Coordinación de Control Interno los retrasos o incumplimientos de los contratistas, así como sobre posibles riesgos asociados a situaciones irregulares.	Coordinador área de contratación	30/10/2020	30/11/2020	Mensualmente el jefe del área de contratos debe presentar reporte ante el Comité Institucional de Coordinación de Control Interno.	En curso

**Fuente:** Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y la Secretaría de Transparencia, 2020.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 48 de 62</b>

## 5. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)<sup>2</sup>, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

### 5.1. Identificación de los activos de seguridad de la información

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

Figura 14. Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar <b>qué es lo más importante que cada entidad y sus procesos poseen</b> (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).
¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber <b>qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano</b> , aumentando así su confianza en el uso del entorno digital.

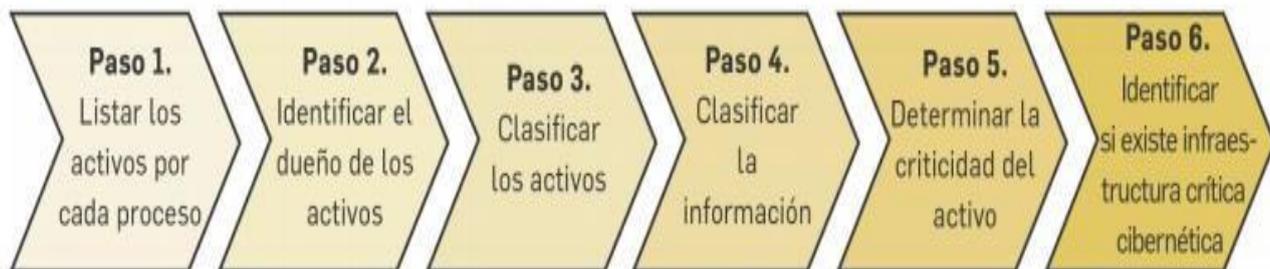
**Fuente:** Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

<sup>2</sup> Tomado de: <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 49 de 62</b>

Figura 15. Pasos para la identificación de activos

## ¿CÓMO IDENTIFICAR LOS ACTIVOS?:



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

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

Tabla 15. Ejemplo identificación activos del proceso

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

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

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 50 de 62</b>

## 5.2. Identificación del riesgo

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

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

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla 5. Tabla de amenazas comunes
- Tabla 6. Tabla de amenazas dirigida por el hombre
- Tabla 7. Tabla de vulnerabilidades comunes

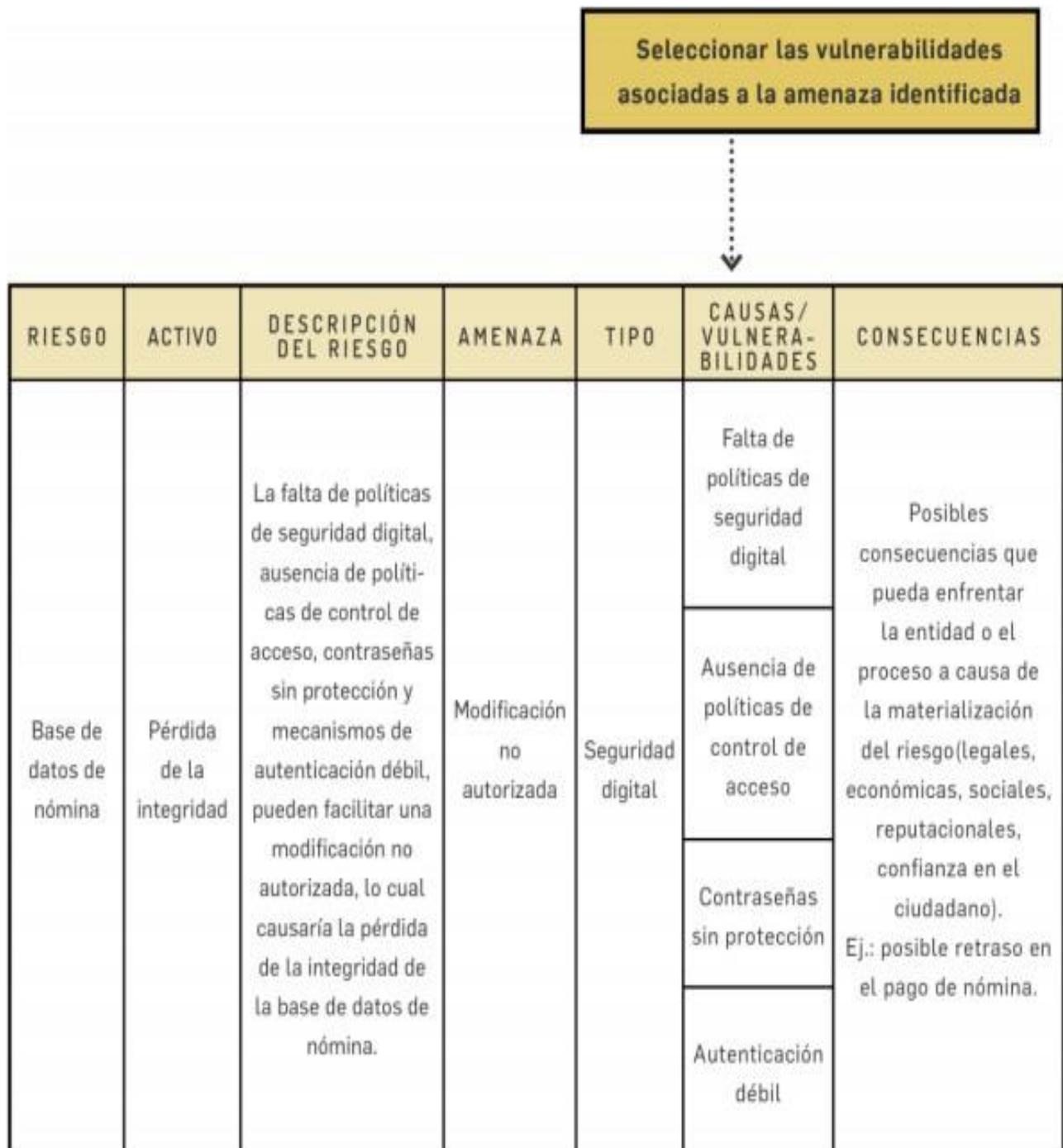
Nota: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Tabla 16. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

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

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

Figura 16. Formato de descripción del riesgo de seguridad de la información



## IMPORTANTE

- \* Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- \* Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas"**, el cual hace parte de la presente guía.
- \* **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
- \* **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

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

### 5.3. Valoración del riesgo

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía.

En este sentido, se debe considerar para este análisis la tabla 4 definida en el aparte 3.1.1, la cual se retoma a continuación:

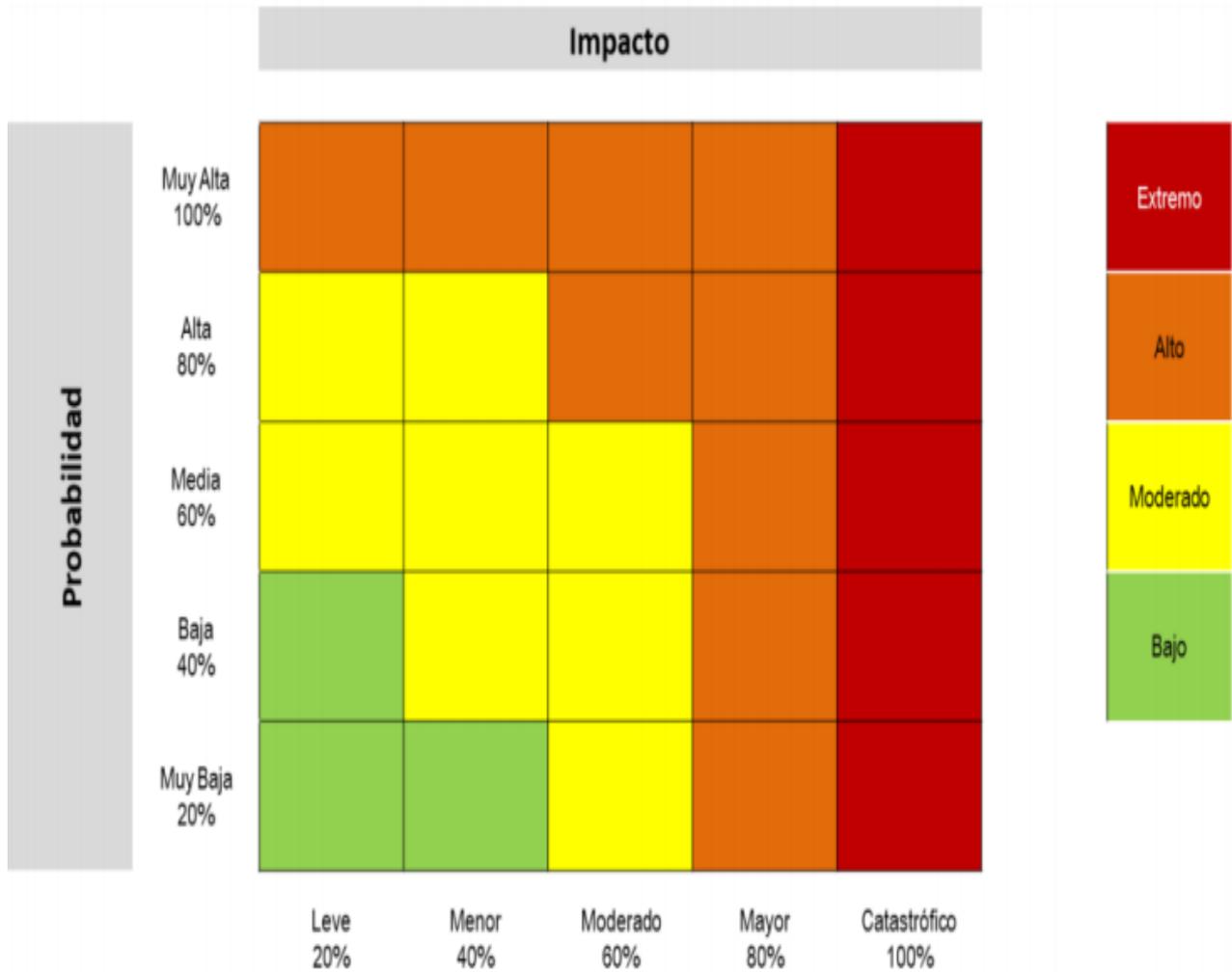
	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad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

La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.2 de la presente guía, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

En este sentido, se debe considerar para este análisis la tabla 5 definida en el aparte 3.1.2, que se retoma a continuación:

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

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor establecida en el numeral 3.2.1 de la presente guía, que se retoma a continuación:



	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b> <b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b> <b>TRD:</b> <b>PÁGINA: 56 de 62</b>

Figura 17. Valoración del riesgo en seguridad de la información

## IMPORTANTE

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

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

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

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

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

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

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

Extremo	
Alto	
Moderado	
Bajo	

### IMPORTANTE:

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

**Fuente:** elaboración conjunta entre la dirección de gestión y desempeño institucional de función pública y el ministerio tic, 2018.

## 5.4. Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 58 de 62</b>

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

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

Tabla 17. Controles para riesgos de seguridad de la información

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

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

Figura 18. Formato mapa riesgos seguridad de la información

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

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

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

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 60 de 62</b>

## 6. ESTRUCTURA ORGANIZACIONAL: ROLES Y RESPONSABILIDADES

### 6.1 Representante Legal

- a. Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva.
- b. Adelantar un seguimiento permanente de las etapas y elementos constitutivos del Sistema de Administración Integral del Riesgo.
- c. Designar el área o cargo que actuará como responsable de la implementación y seguimiento del Sistema de Administración Integral del Riesgo.
- d. Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural hacia la administración del Riesgo en la entidad.
- e. Velar por la correcta aplicación de los controles del Riesgo inherente, identificado y medido.
- f. Recibir y evaluar los informes presentados por el oficial de cumplimiento o persona encargada por la entidad para la ejecución del sistema.
- g. Conocer y discutir los procedimientos a seguir en caso de sobrepasar o exceder los límites de exposición frente a los riesgos, así como los planes de contingencia a adoptar respecto de cada escenario extremo.
- h. Hacer seguimiento y pronunciarse respecto de los informes periódicos que presente el Comité de Riesgos u Órgano equivalente sobre el grado de exposición de riesgos asumidos por la entidad y los controles realizados, además de los informes presentados por la Revisoría Fiscal. Lo anterior debe plasmarse en un informe a la Junta Directiva o, quien haga sus veces, y hacer énfasis cuando se presenten situaciones anormales como mínimo en algún riesgo prioritario o existan graves incumplimientos a las políticas, procesos y procedimientos para cada uno de los Subsistemas de Administración de Riesgos.
- i. Realizar monitoreo y revisión de las funciones del área de control interno.
- j. Velar porque se dé cumplimiento a los lineamientos establecidos en el Código de Conducta y Buen Gobierno de la entidad en materia de conflictos de interés y uso de información privilegiada que tengan relación con el Sistema Integrado de Gestión de Riesgos.
- k. Vigilar cuidadosamente las relaciones de todas las personas que hacen parte de la entidad tanto interna como externamente, para identificar y controlar de manera eficiente los posibles conflictos de interés que puedan presentarse.
- l. . Informar de manera oportuna mediante Oficio a la Superintendencia Nacional de Salud, acerca de cualquier situación excepcional que se presente o prevea que pueda presentarse como mínimo en el ámbito de la administración de los riesgos prioritarios, de las causas que la originan y de las medidas que se propone poner en marcha por parte de la entidad para corregir o enfrentar dicha situación, si procede”.

### 6.2 Oficial de Cumplimiento o Persona Encargada

- a. Diseñar y someter a aprobación de la Junta Directiva, el manual del Sistema de Administración Integral del Riesgo y sus actualizaciones.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 61 de 62</b>

- b. Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva.
- c. Diseñar y proponer la estructura, instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente sus Riesgos en concordancia con los lineamientos, etapas y elementos.
- d. Desarrollar e implementar el sistema de reportes internos y externos de la entidad.
- e. Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los Riesgos.
- f. Establecer y monitorear el perfil de riesgo de la institución e informarlo al Comité de Riesgos y a la Junta Directiva.
- g. Desarrollar los modelos de medición del riesgo.
- h. Desarrollar los programas de capacitación de la entidad.
- i. Presentar un informe periódico, como mínimo semestral, a la Junta Directiva y al representante legal, sobre la evolución y aspectos relevantes del Sistema, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.

### 6.3 Comité de Riesgos

Las responsabilidades del Comité de Riesgos de cara al SICOF son:

- a. Impulsar junto con el Oficial de cumplimiento o persona encargada una cultura de gestión de riesgos al interior del Hospital
- b. Evaluar y aprobar el Manual, procedimientos, metodologías e instrumentos propuestos por el Oficial de cumplimiento o persona encargadas para el efectivo y eficiente funcionamiento.
- c. Supervisar la Implementación de la Gestión de los riesgos conforme a lo establecido en las disposiciones legales, lineamientos de la institución.
- d. Evaluar el avance en los planes de acción y de mejoramiento
- e. Formular las iniciativas de mejora que considere necesarias sobre la infraestructura y la gestión de los riesgos.
- f. Solicitar rendición de cuentas a los líderes de procesos donde se hayan materializado riesgos que comprometan la continuidad de la operación y la viabilidad de la institución.

### 6.4 Area de Gestión de Riesgos o Area Encargada

- a. Apoyar en el diseño de las metodologías de segmentación, identificación, medición, control y monitoreo de los riesgos a los que se expone la entidad, para mitigar su impacto.
- b. Sugerir al Comité de Riesgos, en los casos que aplique, los ajustes o modificaciones necesarios a las políticas de los diferentes Subsistemas de Administración de Riesgos.
- c. Velar por el adecuado diseño e implementación de los controles a los diferentes riesgos

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – Ext 104, Ext 221, Urgencias 2221011

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)  
[gerencia@hospitalsanrafaelzarzal.gov.co](mailto:gerencia@hospitalsanrafaelzarzal.gov.co) – [siau@hospitalsanrafaelzarzal.gov.co](mailto:siau@hospitalsanrafaelzarzal.gov.co)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 62 de 62</b>

para mitigar su impacto, en todos los niveles de la organización y su operatividad.

- d. Realizar seguimiento o monitoreo a la eficiencia y la eficacia de las políticas, procedimientos y controles establecidos.
- e. Apoyar a las áreas en la identificación y evaluación de los límites de exposición para cada uno de los riesgos identificados, y presentar al Comité de Riesgos, en los casos que aplique, las observaciones o recomendaciones que considere pertinentes.
- f. Velar por el adecuado archivo de los soportes documentales y demás información relativa al Sistema Integrado de Gestión de Riesgos de la entidad.
- g. Participar en el diseño y desarrollo como mínimo de los programas de capacitación sobre los riesgos identificados y velar por su cumplimiento. Incluir por lo menos los riesgos de los Subsistemas de Administración de Riesgos.
- h. Analizar los informes presentados por la Auditoría Interna o quien haga sus veces, y los informes que presente el Revisor Fiscal para que sirvan como insumo para la formulación de planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.
- g. Monitorear e informar al Comité de Riesgos, en los casos que aplique, el avance en los planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos”.

## 6.5 Líderes de Procesos

Las responsabilidades de los Líderes de Procesos son:

- a. Identificar el riesgo al que se ve expuesto el Hospital, teniendo en cuenta los factores de riesgo.
- b. Medir la probabilidad de ocurrencia de un evento de riesgo y su impacto en caso de materializarse.
- c. Controlar el riesgo inherente al que se ve expuesta el Hospital con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que dicho riesgo se materialice.
- d. Velar por el cumplimiento y políticas en los procesos de los cuales hacen parte.
- e. Velar por el cambio cultural de los funcionarios bajo su cargo frente al Sistema de Administración Integral del Riesgo.
- f. Participar de las sesiones de gestión de riesgo dejando constancia de los temas tratados y las decisiones tomadas con relación a la identificación de riesgos, medición de probabilidad e impacto, identificación de controles y su evaluación de efectividad.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 63 de 62</b>

## 7. SUBSISTEMAS DE RIESGOS

El Hospital implementara los siguientes subsistemas de riesgos prioritarios definidos en la circular 202117000000045:

1. Riesgo en Salud
2. Riesgo Operacional
3. Riesgo Actuarial
4. Riesgo de Crédito
5. Riesgo de Liquidez

Para gestionar estos riesgos prioritarios, deberán examinarlos a la luz de los parámetros y lineamientos mínimos dispuestos en el presente manual y realizar las modificaciones a que haya lugar.

Es deber de la entidad revisar periódicamente las etapas que comprenden el ciclo y los elementos que hacen parte de cada Subsistema, con el fin de realizar los ajustes que consideren necesarios para su efectivo, eficiente y oportuno funcionamiento, de tal forma que se tenga en cuenta en todo momento las condiciones particulares de Hospital

## 8. MONITOREO Y REVISION

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas.

El monitoreo debe estar a cargo de:

### 8.1. RESPONSABLES DE LOS PROCESOS

El monitoreo y revisión de la gestión de riesgos, está alineado con la dimensión del MIPG de “Control Interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue:

**LINEA ESTRATÉGICA:** Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

**1ª. Línea de defensa.** Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b>
		<b>PÁGINA: 64 de 62</b>

entidad.

Rol principal: Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.

Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

**2ª. Línea de defensa.** Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.

Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

**3ª. Línea de defensa.** Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa

A cargo de la oficina de control interno, auditoría interna o quien haga sus veces.

El rol principal: Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I.

El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

## **8.2. REPORTE PLAN DE TRATAMIENTO DE RIESGOS CONSOLIDAR INFORMACIÓN PARA LA GESTIÓN DEL RIESGO**

- Una vez analizado el nivel de riesgo residual y definido el tratamiento a implementar con el establecimiento de controles preventivos y detectivos, es necesario generar un reporte que consolide la información clave del proceso de gestión del riesgo.
- En el formato de Mapa y Plan de Tratamiento de Riesgos, se inicia con el registro del riesgo identificado, luego se especifica la clase de riesgo, se transcriben las causas raíz o causas priorizadas, así como la probabilidad e impacto que quedaron después de valorar los controles para determinar el riesgo residual
- A partir de allí se deben analizar las estrategias DO y FA o estrategias de supervivencia formuladas en la etapa de establecimiento del contexto, que contrarresten las causas

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – Ext 104, Ext 221, Urgencias 2221011

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)  
[gerencia@hospitalsanrafaelzarzal.gov.co](mailto:gerencia@hospitalsanrafaelzarzal.gov.co) – [siau@hospitalsanrafaelzarzal.gov.co](mailto:siau@hospitalsanrafaelzarzal.gov.co)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 65 de 62</b>

raíz, para colocarlas en las actividades de control del formato y con base en su contenido se establezca la opción de tratamiento a la que corresponden.

- Luego se relaciona el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.
- Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice, para ello se deben analizar las estrategias DA o estrategias de fuga provenientes de la Matriz DOFA, seleccionando la(s) más apropiada(s) para el riesgo identificado.
- No olvidar colocar el soporte, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso o la estrategia.
- Por último, se formulan los indicadores clave de riesgo (KRI por sus siglas en ingles) que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (Por riesgo identificado en los procesos)

### **8.3. INDICADORES - GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL**

Igualmente, en el caso de los riesgos de seguridad digital, se deben generar indicadores, para medir la gestión realizada, en esencia la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad debería definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

- 1 indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.
- 1 indicador de efectividad, para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 66 de 62</b>

### EFICACIA:

Porcentaje de controles implementados =  $(\# \text{controles implementados} / \# \text{controles definidos}) \times 100$

### EFFECTIVIDAD:

# Riesgos materializados de confidencialidad = (# de incidentes que afectaron la confidencialidad de algún activo del proceso)

Variación de incidentes de confidencialidad (para entidades con mediciones anteriores) =

$((\# \text{ de Incidentes de Confidencialidad Periodo Actual} - \# \text{ de Incidentes de Confidencialidad Periodo Previo}) / \text{ Incidentes de Confidencialidad Periodo Previo}) * 100\%$

## 8.4. SEGUIMIENTO RIESGOS DE CORRUPCIÓN

### GESTION RIESGOS DE CORRUPCIÓN

- **Seguimiento:** El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.
  - **Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
  - **Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
  - **Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.
- El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la Entidad o en lugar de fácil acceso al ciudadano.

En especial deberá adelantar las siguientes actividades:

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

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>NIT: 891900441-1</b>	<b>CÓDIGO: DE-GG-FO-04</b>
		<b>VERSIÓN: 04</b>
	<b>MANUAL PARA LA ADMINISTRACION INTEGRAL DEL RIESGO</b>	<b>FECHA: 08/01/2021</b>
		<b>TRD:</b> <b>PÁGINA: 67 de 62</b>

## 9. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas tanto internas como externas debería tener lugar durante todas las etapas del proceso para la gestión del riesgo.

Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios.

Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

VERSION	FECHA REVISION	DESCRIPCION DEL CAMBIO
1	08/jun/2022	Definición de objetivos, alcance y contexto de la entidad
2	01/sep/2023	Se incluyen los subsistemas de riesgos definidos en la circular 202117000000045 que aplican para el Hospital
3	27/mar/2024	<ol style="list-style-type: none"> <li>1. Estructura organizacional: roles y responsabilidades.</li> <li>2. Periodicidad de la revisión de la política</li> <li>3. Asignación del área de planeación como responsable del Sistema de Administración Integral del Riesgo</li> <li>4. Características básicas de los usuarios y proveedores de insumos y medicamentos</li> </ol>
4	10/ene/2025	<ol style="list-style-type: none"> <li>1. Se completan las responsabilidades/funciones del Representante Legal</li> <li>2. Se adicionan las responsabilidades/funciones del Area de Gestión de Riesgo</li> <li>3. Se incluyo dentro del manual el apetito y la tolerancia de los riesgos aceptados por el Hospital, definiendo el nivel de riesgo BAJO y MODERADO como aceptado.</li> </ol>

<b>Actualizado por:</b> Alvaro Tamayo M Planeación	<b>Revisado por:</b> Erika Isabel Lasprilla Asesora Planeación	<b>Aprobado por:</b> Comité Institucional de Control Interno Acta 001 del 15 de junio de 2022
Alvaro Tamayo M Planeación	Alvaro Hernán Libreros Asesor Planeación	<b>Aprobado por:</b> Junta Directiva Acuerdo No 013 del 23JUL2024
Alvaro Tamayo M Planeación	Juan Carlos Buitrago Oficial de cumplimiento	<b>Aprobado por:</b> Junta Directiva Acuerdo No 004 del 19FEB2025