POLITICA DE ADMINISTRACIÓN DE RIESGOS

PERSONERIA MUNICIPAL DE PUERTO COLOMBIA

DICIEMBRE DE 2023

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Para la PERSONERIA MUNICIPAL DE PUERTO COLOMBIA, la administración de riesgos es una herramienta fundamental para asegurar el cumplimiento de su función constitucional y legal, misión institucional, los objetivos trazados dentro del Plan de Acción Municipal y aquellos planteados dentro del marco de la implementación del Modelo Integrado de Planeación y Gestión MIPG, en lo que respecta a la Dimensión de Control Interno.

Teniendo en cuenta que los riesgos son posibilidades de ocurrencia de toda situación que pueda desviar el normal desarrollo de las actividades de los procesos e impidan el logro de los objetivos estratégicos para el cumplimiento de la misión institucional, la PERSONERIA MUNICIPAL DE PUERTO COLOMBIA, ha fortalecido el sistema de control interno en sus componentes: Ambiente de control, evaluación de riesgos, actividades de control, información y comunicación y actividades de monitoreo, en lo que respecta a la Dimensión de Control Interno, articulada con el Modelo Integrado de Planeación y Gestión – MIPG.

El objetivo principal de esta Política es gestionar la identificación, valoración, tratamiento, manejo y seguimiento a los riesgos de gestión, corrupción y Seguridad Digital, con el fin de mitigar o eliminar efectos negativos en el logro de los objetivos estratégicos en pro de asegurar una gestión pública efectiva.

Los lineamientos aquí previstos, buscan establecer una identificación del riesgo adecuada a las necesidades de la entidad, con un enfoque preventivo que permita la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a todas sus partes interesadas aspectos fundamentales frente a la generación de valor público, eje fundamental en el quehacer de todas las organizaciones públicas.

Atendiendo lo anterior, la estructura metodología de la gestión de riesgos presentada corresponde a los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6. De noviembre de 2022 dispuesta por el Departamento Administrativo de la Función Pública DAFP y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), del Modelo Estándar de Control Interno en lo pertinente al modelo de las líneas de defensa.

2. OBJETIVO

La política de administración del riesgo de la Personería Municipal de Puerto Colombia, tiene como objetivo orientar la toma de decisiones para minimizar o eliminar efectos adversos que pudieran interferir en el cumplimiento de los fines que le fueron encomendados conforme a la Constitución, la Ley y el Plan de Acción de la entidad.

3. ALCANCE

La política de administración del riesgo es aplicable a todos los procesos, servicios, proyectos y planes de la entidad durante toda su gestión y a todos los servidores públicos en el ejercicio de sus funciones, de la Personería Municipal de Puerto Colombia, de acuerdo con las responsabilidades establecidas en el presente documento; por lo tanto, debe ser conocida y cumplida por todos los funcionarios que apoyan la gestión de la entidad. Así mismo, será la metodología adoptada para la identificación, análisis y evaluación de los riesgos de gestión, corrupción y seguridad de la información.

4. DEFINICIONES

A	**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.
C	**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:** 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 modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
D	**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

F	**Factores de Riesgo:** Son las fuentes generadoras de riesgos.
G	**Gestión del Riesgo**: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
I	**Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo. **Integridad:** Propiedad de exactitud y completitud.
M	**Mapa de Riesgos**: Documento para organizar la información que describe los riesgos de la entidad. El mapa de riesgos es una representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa. Un mapa de riesgos puede adoptar la forma de un cuadro resumen que muestre cada uno de los pasos llevados a cabo para su levantamiento.
N	**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.
P	**Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal. **Política de Administración de Riesgos:** Declaración de la dirección y las intenciones generales de una organización con respecto a la administración del riesgo. **Probabilidad:** Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.
R	**Riesgo:** Efecto de la incertidumbre en un resultado esperado **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 Inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias. **Riesgo Residual**: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento. **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).
T	**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.
V	**Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. MARCO LEGAL:

NORMA	CONTENIDO
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 Objetivos del control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
Ley 489 de 1998	Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno
Decreto 2145 de 1999	Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art. 8º. de la ley 1474 de 2011)
Directiva Presidencial 09 de 1999	Lineamientos para la implementación de la política de lucha contra la corrupción.
Decreto 2593 de 2000	Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999.
Decreto 1537 de 2001	Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado. El parágrafo del Artículo 4º señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (…) y en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su Artículo 4º la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…)
Decreto 1599 de 2005	Por el cual se adopta el Modelo Estándar de Control Interno para el Estado colombiano y se presenta el anexo técnico del MECI 1000:2005. 1.3 Componentes de administración del riesgo.
Decreto 4485 de 2009	Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g) "establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder". Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades
Decreto 1474 de 2011	Estatuto Anticorrupción. Artículo 73. "Plan Anticorrupción y de Atención al Ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias antitrámites y los mecanismos para mejorar la atención al ciudadano.
Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018 versión 4	Se mantiene estructura conceptual, se articulan las políticas de lucha contra la corrupción y seguridad de la información. Se define metodología para el diseño de controles.

Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2020 versión 5	Se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo
Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2022 versión 6	Se mantiene estructura conceptual para la administración del riesgo. Se incluye capítulo específico sobre riesgo fiscal, que se complementa con el Anexo denominado catalogo indicativo de puntos de riesgo fiscal para facilitar el análisis en el marco del modelo de operación por procesos.

6. METODOLOGIA PARA LA ADMINISTRACIÓN DEL RIESGO

Siguiendo la metodología establecida en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades públicas (Riesgos de Gestión, Corrupción y Seguridad Digital) – Versión 6, se definen los siguientes pasos para una adecuada administración del riesgo:

6.1. Paso 1: Política de Administración de Riesgos

La Política de Administración de Riesgos hace referencia al propósito de la Alta Dirección de gestionar el riesgo. Así, tomando como base el plan de desarrollo, los objetivos institucionales y de los procesos, la Personería Municipal de Puerto Colombia, define su política de administración del riesgo como mecanismo para identificar, analizar, evaluar, monitorear y revisar los riesgos que pudieran afectar el logro de sus objetivos institucionales.

De acuerdo con lo anterior, la Alta Dirección definió la Política de Administración del Riesgo así:

> "La Alta Dirección de la Personería Municipal de Puerto Colombia, en desarrollo del compromiso institucional que le asiste y con el propósito de estimular la cultura del autocontrol y mejora continua, promoverá la identificación de riesgos, su valoración y seguimiento en aras de que se adopten los controles que resulten más apropiados para minimizar la ocurrencia y/o impacto de situaciones o actos de corrupción que puedan afectar el logro de los objetivos de la entidad, para lo cual se propiciaran los

6.2. Paso 2: Identificación de Riesgos

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la Personería Municipal de Puerto Colombia, para ello se debe tener en cuenta

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

6.2.1. Análisis de los objetivos estratégicos y de los procesos.

El contexto estratégico es la base para la identificación del riesgo, dado que su análisis contribuirá a establecer las causas del riesgo.

Para ello, se requiere que se realice un análisis de los objetivos estratégicos planteados dentro del Plan de Acción y objetivos de procesos, formulando aquellos posibles riesgos que puedan afectar el logro de los mismos. Es necesario revisar que los mismos se encuentren alineados con la misión, visión institucional y en general con el direccionamiento estratégico de la Personería, así mismo, verificar que la formulación de los objetivos planteados tenga como mínimo los siguientes criterios (especifico, medible, alcanzable y proyectado en el tiempo) (metodología SMART).

6.2.2. 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.

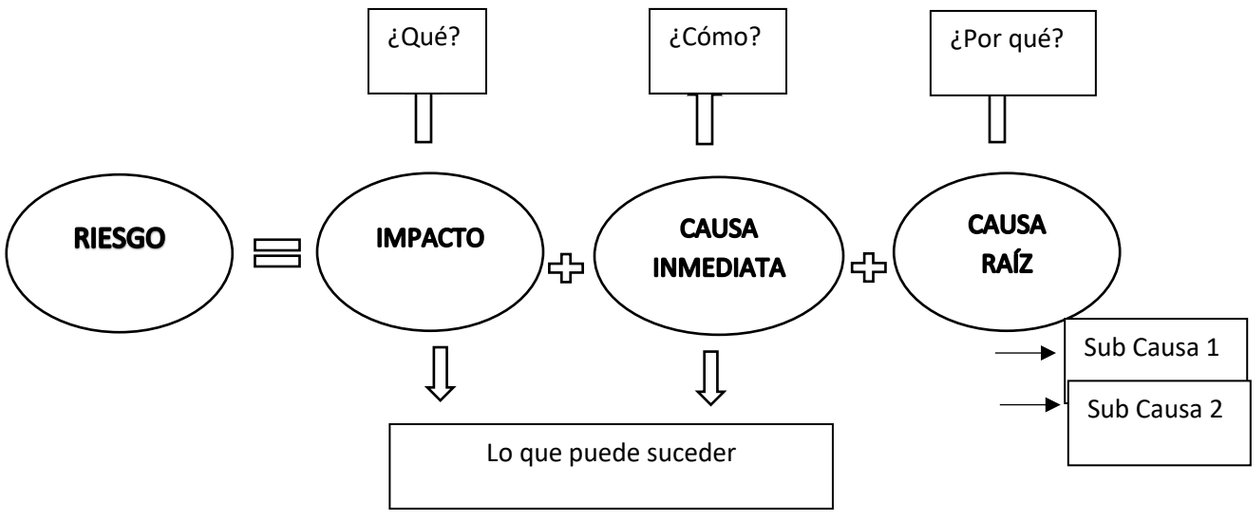
6.2.3 Identificación de áreas de impacto: El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

6.2.4 Identificación de áreas de factores de riesgo: Son las fuentes generadoras de riesgos. La Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. (diciembre de 2020) dispuesta por el Departamento Administrativo de la Función Pública DAFP, establecer el siguiente listado con ejemplo de factores de riesgo que puede tener una entidad., sin embargo, el proceso de Direccionamiento Estratégico Institucional, como coordinador en el levantamiento de riesgos por proceso, podrá establecer otros factores de riesgos que se consideren asociados al contexto de la Personería Municipal de Puerto Colombia.

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

6.2.5 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**:**



- **¿QUÉ PUEDE SUCEDER?** Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso. Establece el **Impacto**: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **¿CÓMO PUEDE SUCEDER?** Establecer las causas a partir de los factores determinados en el contexto. Establece la **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

- **¿POR QUÉ PUEDE SUCEDER?** Responde a la **causa raíz**, determina la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizada

Se debe tener en cuenta que los controles deben apuntar atacar las sub causas.

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

Entre las clases de riesgos que pueden presentarse están:

6.2.6 Clasificación del Riesgo: Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías**:**

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales 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.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

De lo anterior, la Guía contempla factores de riesgo asociados, como se describe a continuación:

6.3. Paso 3: Valoración de Riesgos

En esta etapa se busca establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente). Se desarrolla a través de 2 elementos:

6.3.1 Análisis de Riesgo: En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto**.**

6.3.1.1 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.**[1]

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

A continuación, se presenta el nivel de probabilidad establecido en la Guía de Administración de Riesgo (DAFP), a fin de determinar el nivel de probabilidad del riesgo en la Personería Municipal de Puerto Colombia. [2]

	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%

6.3.1.2 Determinar el Impacto: 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**.**

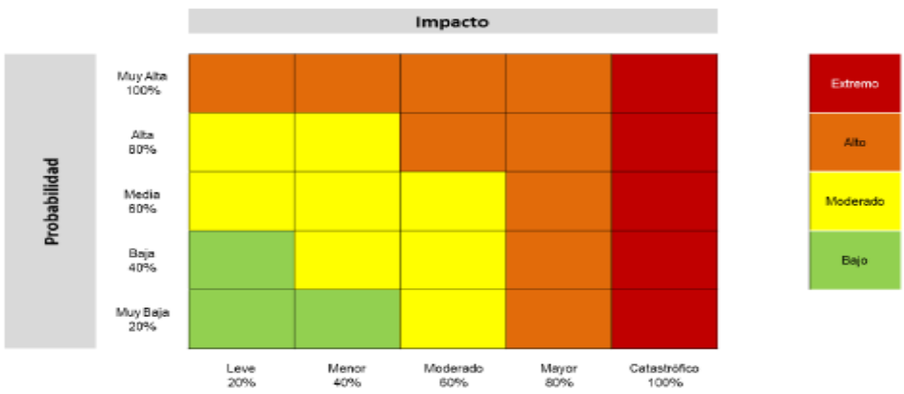
[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. (diciembre de 2020) dispuesta por el Departamento Administrativo de la Función Pública DAFP
[2] Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. (diciembre de 2020) dispuesta por el Departamento Administrativo de la Función Pública DAFP

A continuación, se presenta una tabla con los criterios para definir niveles de impacto [3]

	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

6.4. 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).

6.4.1 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**.**



6.4.2 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:

[3] Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. (diciembre de 2020) dispuesta por el Departamento Administrativo de la Función Pública DAFP

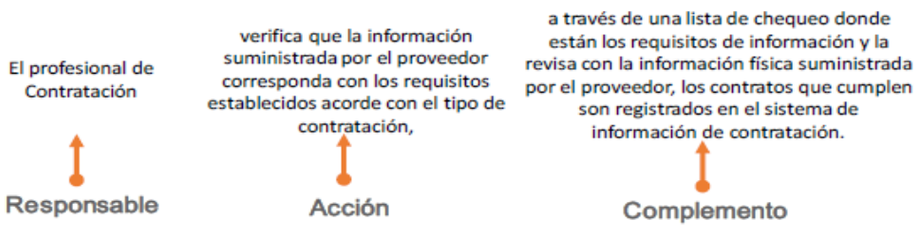
Dir.: Calle 7 8-46 ***/ Cel.:*** 301 6482527
E-mail: personeriamunicipalptocol@hotmail.com - compersoneriapto2020@gmail.com
Facebook: personería de Puerto Colombia ***/ Twitter:*** PERSONERIAPTO1 ***/ Instagram:*** personeriapto2020
Puerto Colombia – Atlántico

 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.

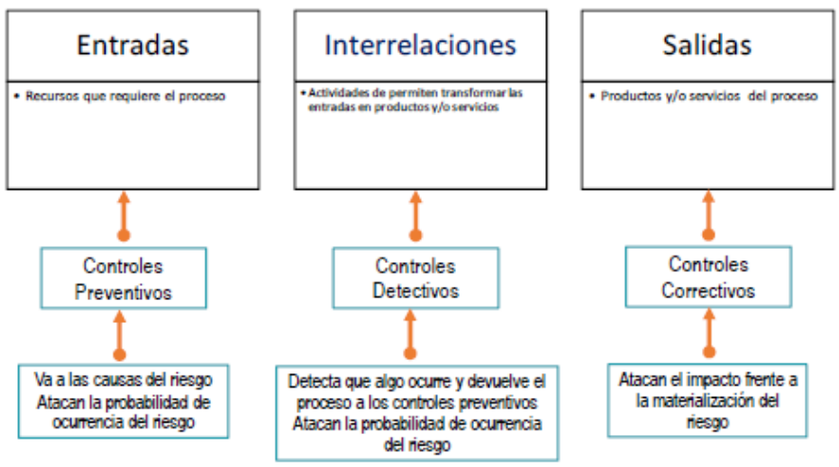
 Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

6.4.2.1 Estructura para la descripción del control: Para una adecuada redacción del control la Guía para la administración de riesgos de la DAFP, 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.



6.4.2.2 Tipología de controles y los procesos: A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión.



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.

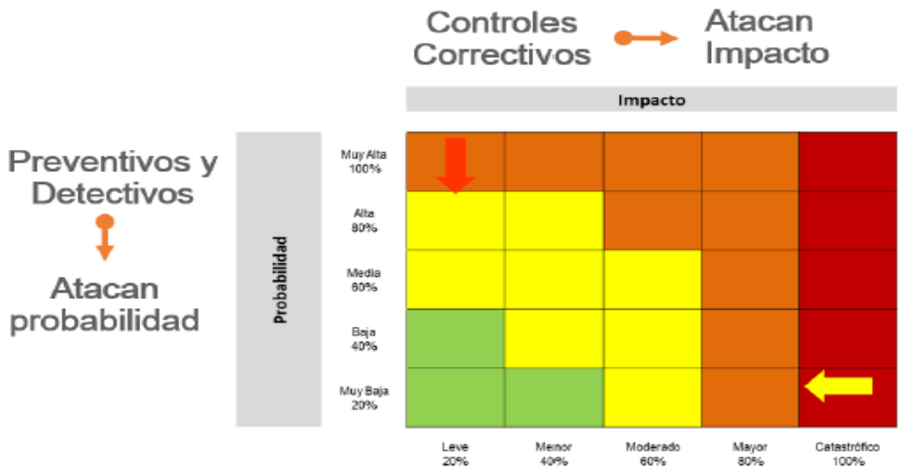
Así mismo, de acuerdo con la forma como se ejecutan tenemos:

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

6.4.2.3 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**.**

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

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



A continuación, se establece la tabla de controles y características que debe utilizarse por los procesos de la entidad:

CONTROLES Y SUS CARACTERISTICAS			PESO (%)
Control 1	Tipo	Preventivo	25%
		Detectivo	15%
		Correctivo	10%
	Implementación	Automático	25%
		Manual	15%
	Documentación	Documentado	-
		Sin Documentar	-
	Frecuencia	Continua	-
		Aleatoria	-
	Evidencia	Con registro	-
		Sin registro	-

6.4.3 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.

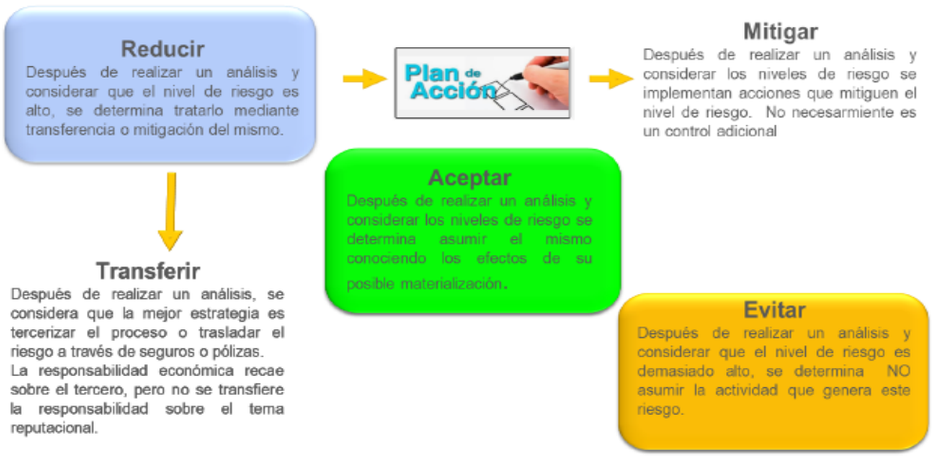
A continuación, se muestra la tabla para aplicación de controles para establecer el riesgo residual:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

6.5. **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.

Con base en la valoración de los riesgos de gestión, los responsables de los procesos deben tomar decisiones adecuadas para el manejo de los riesgos teniendo en cuenta las siguientes opciones:



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.

6.6. 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:

6.6.1 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)

6.6.2 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.

A continuación, un ejemplo de indicadores calve de riesgos [4]

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

[4] Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. (diciembre de 2020) dispuesta por el Departamento Administrativo de la Función Pública DAFP

Dir.: Calle 7 8-46 ***/ Cel.:*** 301 6482527
E-mail: personeriamunicipalptocol@hotmail.com - compersoneriapto2020@gmail.com
Facebook: personería de Puerto Colombia ***/ Twitter:*** PERSONERIAPTO1 ***/ Instagram:*** personeriapto2020
Puerto Colombia – Atlántico

6.7. **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:

Lineas de Defensa	Responsables	Roles
Linea Estrategica	Alta dirección y del comité institucional de coordinación de control interno	Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes
Primera Linea de Defensa	Líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la organización)	Identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.
Segunda Linea de Defensa	Jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, comités de riesgos (donde existan), comité de contratación, áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación	Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente Supervisar la implementación de prácticas de gestión de riesgo eficaces Consolidar y analizar información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos Asesoría a la 1ª línea de defensa en temas clave como riesgos y controles
Tercera Linea de Defensa	Jefes de Control Interno	Asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso sobre las responsabilidades en materia de riesgos. Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos

6.7.1 Aspecto relevantes:

- 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 estará a cargo de los responsables de los procesos y la oficina de control interno. Los responsables de los procesos serán los encargados de realizar las acciones asociadas a los controles establecidos para cada uno de los riesgos identificados para su proceso.
- Por su parte, la oficina de control interno realizará seguimiento a los riesgos que a nivel institucional hayan sido consolidados, durante la ejecución de las auditorias independientes dicha oficina debe analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos auditados.
- En cuanto a los riesgos asociados a posibles actos de corrupción, la periodicidad del seguimiento debe cumplir las fechas establecidas en la Ley 1474 de 2011.

- La frecuencia de medición y reporte para la gestión de riesgos será la establecida por el Personero, de manera que el seguimiento realizado sea la base para la toma de decisiones, y que se logren introducir correctivos en el momento adecuado.

7. RIESGOS DE CORRUPCIÓN:

7.1. Generalidades:

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

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL 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.

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

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción.

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo de corrupción	**Acción u omisión**	**Uso del poder**	**Desviar la atención de lo público**	**Beneficio privado**
(…)				

Al respecto, la Guía expedida por el DAFP, propone el siguiente ejemplo:

EJEMPLO

Información anonimizada:

N.°	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	

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.

7.2. Valoración de riesgos

La valoración del riesgo se realiza mediante el cálculo de la probabilidad e impacto

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

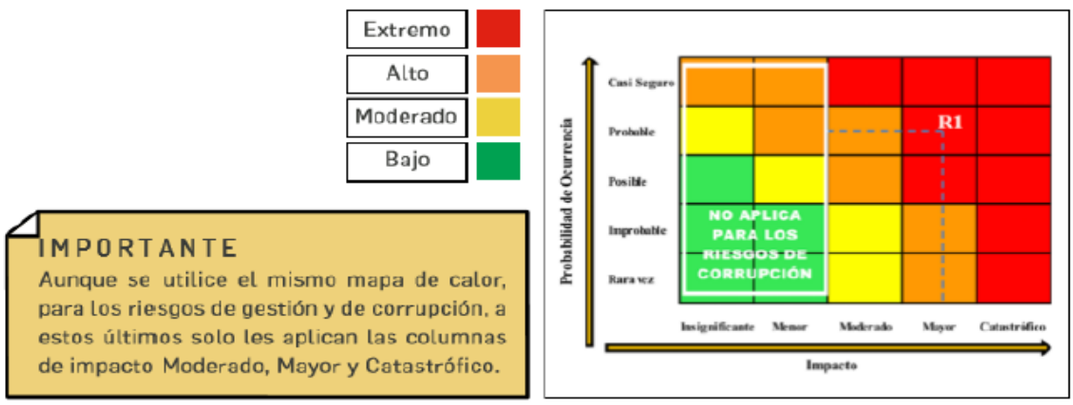
A continuación, la siguiente tabla contentiva de los criterios para calificar la probabilidad:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

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

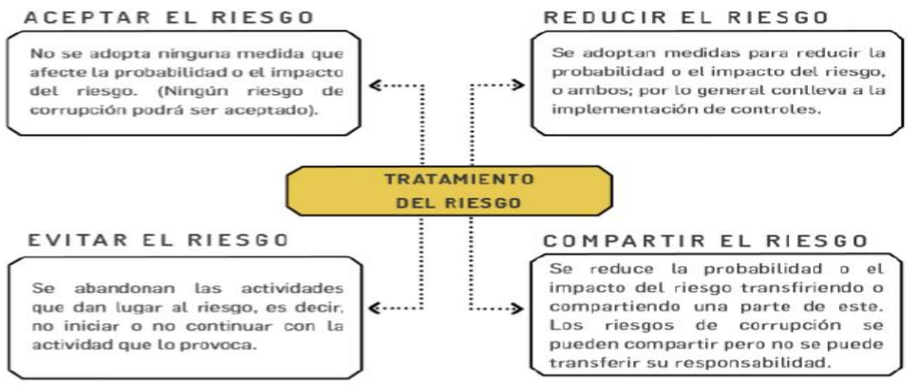
7.2.2.1. Análisis del impacto en riesgos de corrupción: Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.



7.2.3. Valoración de los controles – diseño de controles: El diseño de controles, se realizarán con base en los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018**.**

7.2.4. Tratamiento del riesgo: A diferencia de los riesgos de gestión, para los riesgos de corrupción, no aplica el criterio de aceptación de riesgo.



7.2.5. Monitoreo y Revisión: Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a quien asuma las obligaciones o funciones de planeación estratégica adelantar el monitoreo (segunda línea de defensa), dicho monitoreo será en los tiempos que determine la Personería Municipal de Puerto Colombia**.**

7.2.5.1. Reporte de la gestión del riesgo de corrupción: A continuación, se describen los plazos vigentes de reporte, si llegare a existir modificación de los mismos, se realizará el reporte en los términos establecidos sin que llegare afectar el contenido de la presente Política

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. En las fechas:

- 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 Personería Municipal de Puerto Colombia.

En caso de que exista materialización del riesgo de corrupción, se deberá adelantar las siguientes actividades:

Tipo de riesgo	Oficina de Control Interno	Líder de proceso
Riesgo de corrupción	1. Convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectado s, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. 2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. 3. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. 4. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.	1. Informar a la Alta Dirección sobre el hecho encontrado. 2. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo 3. Iniciar las acciones correctivas necesarias. 4. Realizar el análisis de causas y determinar acciones preventivas y de mejora. 5. Análisis y actualización del mapa de riesgos.

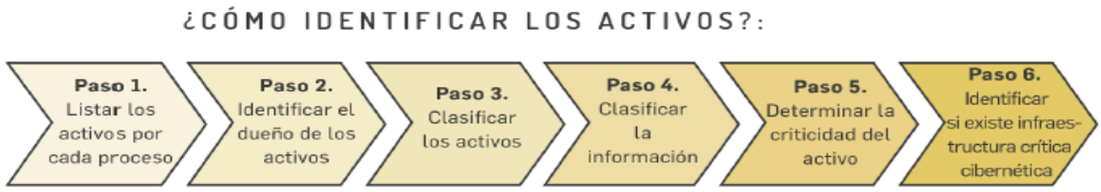
8. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN:

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

¿Qué son los activos?	¿Por qué identificar los activos?

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización -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	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Pasos para la identificación de activos:



8.2. 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 *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas* donde se encuentran las siguientes tablas necesarias para este análisis:

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

9. SOCIALIZACIÓN:

Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de: gestión, corrupción y seguridad de la información.

Con respecto al mapa de corrupción, El Personero o quien haga sus veces, deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y

propuestas sobre el proyecto del mapa de riesgos de corrupción, antes de su publicación.

Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias, sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

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