POLITICA DE ADMINISTRACIÓN DEL RIESGO PERSONERÍA DE RIONEGRO

La Personería de Rionegro establece su Política de Administración y Gestión del Riesgo de acuerdo con los parámetros establecidos por el Departamento Administrativo de la Función Pública. Como una herramienta hacia la prevención de la materialización del riesgo para el manejo del Riesgo de gestión, riesgo de corrupción, riesgos de seguridad informática, así como el manejo de los controles en todos los niveles de la organización, buscando la protección del valor, la continuidad de las operaciones y la generación de confianza en las partes interesadas y comunidad en general.

OBJETIVO DE LA POLITCA: El objetivo principal de esta Política es asegurar los objetivos estratégicos de la Personería a través de gestionar la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento a los riesgos de los procesos y riesgos de corrupción, con el fin de mitigar y minimizando los efectos negativos en la Entidad para lograr la satisfacción de nuestros usuarios y poner eliminar efectos negativos, que pueden llevar a la entidad a la posibilidad de incurrir en pérdidas o afectaciones a nivel económico o reputacional por deficiencias, fallas o inadecuaciones, en el recurso humano, procesos, tecnología, infraestructura o por la ocurrencia de acontecimientos externos.

Implementar en los procesos y procedimientos estrategias u acciones con el fin de mitigar el riesgo como resultado de la administración y control de riesgo.

ALCANCE DE LA POLITICA: Esta política será aplicable a todos los procesos a los planes, programas y servicios de la Personería el manejo de los Riesgos será de carácter prioritario y estratégico, fundamentado en el Modelo de Operación por Procesos.

La identificación, análisis, valoración y monitoreo de los riesgos corresponderá a cada proceso de acuerdo con los objetivos estratégicos planteados dentro del Plan Estratégico.

Está bajo la responsabilidad de los líderes de procesos, las tres líneas de defensa y de la Línea Estratégica de Defensa el diseño y control del mapa de riesgos así:

PRIMERA LINEA DE DEFENSA: Personero y el Comité de Coordinación de Control Interno: Definir la política de riesgo y aprobarla

SEGUNDA LINEA DE DEFENSA: lideres de los Procesos: Identificar con el equipo de trabajo los riesgos y sus controles.

Oficina de Planeación o quien haga sus veces: Asesor en la identificación de los riesgos, consolidar el mapa de riesgos.

TERCERA LINEA DEFENSA: Control Interno: Analizar el diseño y eficacia de los controles establecidos en el mapa de riesgos, realizar seguimiento periódico y reportar el seguimiento.

TERMINOS Y DEFINICIONES:

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 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 de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado	**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.
Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo	**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.	**Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.	**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	**Control:** Medida que permite reducir o mitigar un riesgo.	**Causa Inmediata:** Circunstancias bajo las cuales se	**Causa Raíz:** Causa principal o básica, corresponde a las

controles al riesgo inherente.		presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.	razones por la cuales se puede presentar el riesgo.
Factores de Riesgo: Son las fuentes generadoras de riesgos.	**Confidencialidad**: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados	**Integridad**: Propiedad de exactitud y completitud.	**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.	**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.	**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	**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.

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 se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.	**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.	**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.

Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2022**.**

Tipología de riesgos

Riesgos de gestión: aquellos asociados a los procesos que pueden afectar el cumplimiento de la misión y objetivos institucionales**.**

Riesgos de corrupción: eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado**.**

Riesgos digitales (seguridad de la información): aquellos que pueden afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

IDENTIFICACIÓN DEL RIESGO

Esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias, Para sus análisis 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 estratégicos.

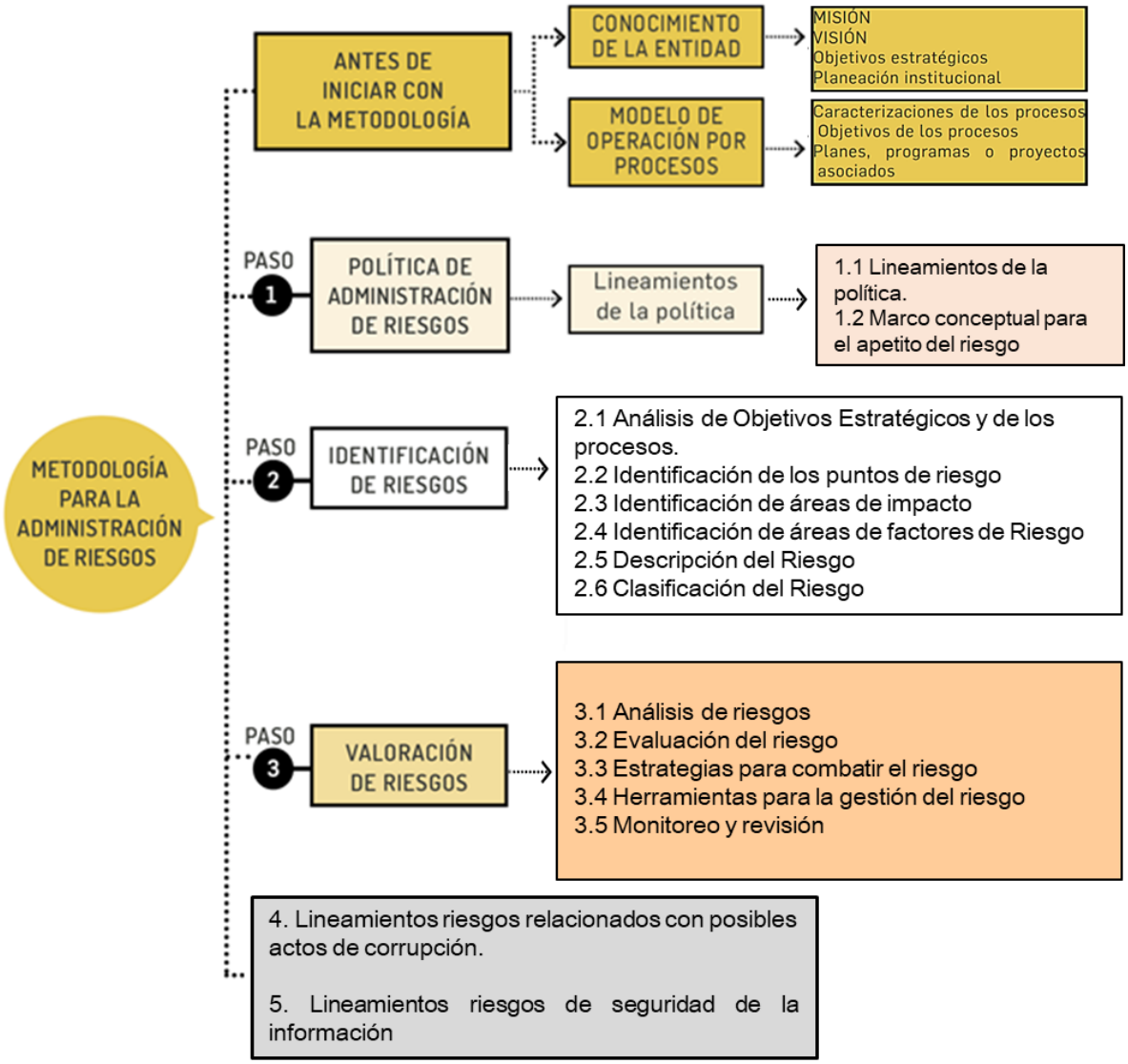
Se aplican las siguientes fases contenidas en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6 de diciembre de 2022.

Análisis de objetivos estratégicos y de los procesos: Para la identificación se tuvo en cuenta el contexto estratégico el cual se construyo fue con la participación de todos los integrantes de la Personería y de la comunidad y de allí se generó el Plan Estratégico 2024-2028

Identificación de los puntos de riesgo: Son las actividades dentro del flujo del proceso donde existe evidencia o se ha determinado que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo y el riesgo no se materialice.

Identificación de áreas 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.

METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO:



Fuente: Guía para la Gestión del Riesgo y Diseño de Controles para las Entidades Públicas V6-2022.

CONTEXTO ESTRATÉGICO

Se analizo el entorno estratégico de la Personería a partir de los siguientes factores externos (amenazas y oportunidades), internos (fortalezas y debilidades) y de procesos para el adecuado análisis de las causas del riesgo y la gestión de este:

DEBILIDADES		FORTALEZAS	
1	Manual de Funciones desactualizado	**1**	Disposición de canales de comunicación internos y externos.
2	Personal de planta insuficiente para el funcionamiento interno.	**2**	Avance en la adecuación del Sistema Integrado de Gestión.
3	Manual de contratación desactualizado	**3**	Seguimiento y evaluación constante al Sistema Integrado de Gestión.
4	Falta de presupuesto para una adecuada gestión.	**4**	Procesos documentados.
5	Ausencia de un análisis de necesidades y expectativas de los grupos de valor.	**5**	Alto nivel de cumplimiento de la planeación institucional.
6	Niveles bajos de conveniencia y eficacia del Sistema Integrado de Gestión.	**6**	Oportunidad en la atención al ciudadano.
7	Inadecuada gestión de la información interna y de cara al ciudadano	**7**	Personal de planta capacitado y con competencias suficientes.
8	Inadecuada gestión del conocimiento.		
9	Falta de recursos tecnológicos.		
AMENAZAS		**OPORTUNIDADES**	
1	Cambios en la normatividad aplicable.	**1**	Relacionamiento con otras entidades e instituciones.
2	Cambios en lineamientos metodológicos por parte del Gobierno Nacional / Departamento Administrativo de la Función Pública	**2**	Guías metodológicas proporcionadas por el Gobierno Nacional / Departamento Administrativo de la Función Pública
3	Asignación de recursos insuficientes para el funcionamiento de la entidad.	**3**	Avances en las Tecnologías de la Información y Comunicación
4	Afectación de la imagen institucional.	**4**	Oferta de capacitaciones en asuntos de gestión pública y promoción de derechos humanos
5	Pandemias o epidemias.	**5**	Reconocimiento de la entidad a nivel regional.
6	Alteraciones en el orden público.		
7	Escasez en la oferta de insumos básicos para el funcionamiento de la entidad.		

ANALISIS DEL RIESGO:

Al efectuar el análisis de riesgos la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 de diciembre de 2022, precisa que "se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.18

Señala la guía que se debe determinar la probabilidad, entendiéndose esta como la posibilidad de ocurrencia del riesgo.

VALORACION DEL RIESGO:

PROBABILIDAD: Es la probabilidad 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.

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: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6 de diciembre de 2022

El análisis de la frecuencia deberá ajustarse al proceso y la disponibilidad de datos históricos sobre el evento o riesgo identificado.

IMPACTO: Son las consecuencias o efectos que puede ocasionar a la organización la materialización del Riesgo.

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

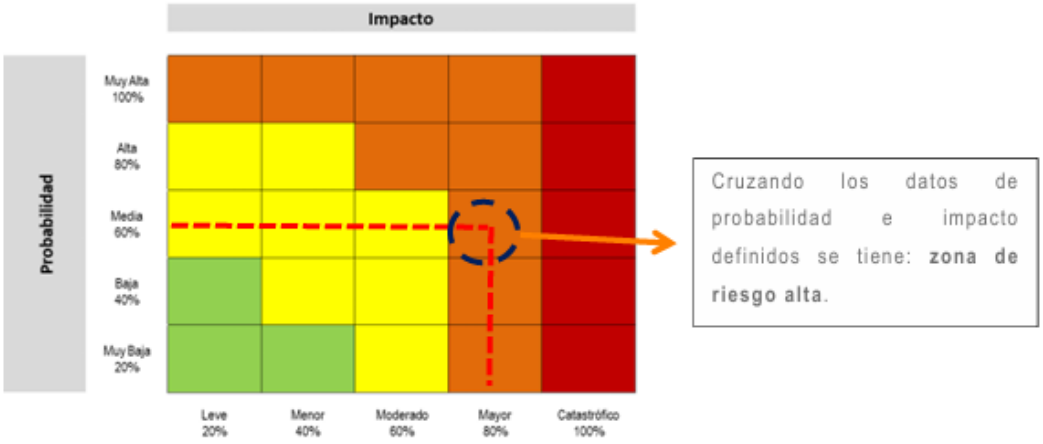
Tabla 5 Criterios para definir el nivel de impacto

	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: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6 de diciembre de 2022

MATRIZ DE CALOR:

Aplicando la matriz de calor tenemos:



Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos.

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.

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. Son las fuentes generadoras de riesgos y los factores de riesgo que puede tener una entidad.

MATERIZALIZACION DEL RIESGO:

Ante la materialización de algún riesgo se deberá medir el impacto y las consecuencias que puede ocasionar en los objetivos de la personería, se deberán revisar y ajustar los controles asociados determinando el grado de efectividad, eficiencia y eficacia que garantice la mitigación ocurrencia.

SEGUIMIENTO Y MONITOREO DE LOS RIESGOS:

La Asesora de Control y Seguimiento asegura que en todos los casos los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva, mediante acciones como:

Determinar la efectividad de los controles.

Mejorar la valoración de los riesgos.

Mejorar los controles.

Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.

Determinar si se adelantaron acciones de monitoreo.

Revisar las acciones del monitoreo.

Tipo de Riesgo	**Zona de Riesgo Residual**	**Estrategia de Tratamiento -Controles**
Riesgos de Gestión, y seguridad digital	Baja	Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en la matriz de Riesgos
	Moderada	Se realiza seguimiento a los controles con periodicidad CUATRIMESTRAL y se registran sus avances en la matriz de Riesgos
	Alta	Se realiza seguimiento a los controles con periodicidad BIMESTRAL y se registran sus avances en la matriz de Riesgos
	Extrema	Se realiza seguimiento a los controles con periodicidad MENSUAL y se registran sus avances en la matriz de Riesgos
Riesgos de corrupción	Todos los riesgos de corrupción, independientemente de la zona de riesgo en la que se encuentran debe tener un seguimiento CUATRIMESTRAL y se registra en la Matriz de Riesgos de corrupción	

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de tratamiento -Plan de acción
Riesgos de Gestión	Baja	No se debe realizar plan de acción porque está dentro del nivel de aceptación del riesgo
y Seguridad digital	Moderada, Alta o Extrema	El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles. Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.