MANUAL PARA LA ADMINISTRACIÓN DEL RIESGOS Y EL DISEÑO DE CONTROLES DE LA PERSONERIA DISTRITAL

2021

Tabla de contenido

INTRODUCCION

La personería Distrital de Cartagena en virtud de su misión y sus objetivos estratégicos, ha establecido acciones encaminadas al control preventivo de los riesgos, con el propósito de garantizar la adecuada prestación de sus servicios y el cumplimiento de sus objetivos institucionales, determinando lineamientos a la administración de la gestión del riesgo teniendo en cuenta el contexto de la Entidad y la Planeación Estratégica.

La siguiente política, pretende orientar y guiar a los servidores públicos de la entidad, sobre la identificación, análisis y valoración de los riesgos con el fin de poder identificar las posibles desviaciones que pueden crear incertidumbre sobre el logro de los objetivos.

Así mismo, se establecen los lineamientos generales, responsabilidades y mecanismos para la administración de los riesgos que permitan brindar seguridad para controlar y responder a los acontecimientos potenciales o aquellos en los que puedan provocar situaciones de corrupción en concordancia con las directrices en materia de gestión pública y el enfoque del Modelo de Planeación y Gestión MIPG.

Para la formulación de la Política se contó con los lineamientos de carácter técnico establecidos por el Departamento Administrativo de la Gestión Pública –DAFP-, tales como la “Guía para la administración del riesgo y el diseño de controles en entidades públicas.” V5 Diciembre 2020, “Guía para la Gestión de Riesgo de Corrupción” y “Estrategias para la construcción del Plan Anticorrupción y Atención al Ciudadano”.

1. 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 controles al riesgo inherente.	**Control:** Medida que permite reducir o mitigar 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.
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, 2020

2 ALINEACION DE LA POLITICA CON LA PLATAFORMA ESTRATEGICA DE LA ENTIDAD Y MIPG

La Personería Distrital de Cartagena de Indias, atendiendo a las funciones constitucionales y legales que le asisten, los cuales se demarcan en la guarda y protección de los derechos humanos, la protección y garantía del interés público, veeduría del tesoro público y de la correcta ejecución de la función pública a nivel local, ha establecido su plataforma estratégica la cual hace parte integral en la definición de los lineamientos de administración de riesgos descritos en esta política, en concordancia con lo establecido en Modelo de Planeación y Gestión-MIG.

2.1 MISIÓN

La Personería de Cartagena ejerciendo como Ministerio Público promueve y vigila el cumplimento de los derechos humanos; ejerce vigilancia administrativa sobre quienes desempeñan funciones públicas, atiende y apoya en forma permanente y personalizada los requerimientos de la comunidad, con criterios de compromiso social, equidad, oportunidad, efectividad y mejoramiento continuo; velando por el crecimiento integral de sus servidores y la preservación del medio ambiente.

2.2 VISIÓN

La Personería de Cartagena ejerciendo como Ministerio Público promueve y vigila el cumplimento de los derechos humanos; ejerce vigilancia administrativa sobre quienes desempeñan funciones públicas, atiende y apoya en forma permanente y personalizada los requerimientos de la comunidad, con criterios de compromiso social, equidad, oportunidad, efectividad y mejoramiento continuo; velando por el crecimiento integral de sus servidores y la preservación del medio ambiente.

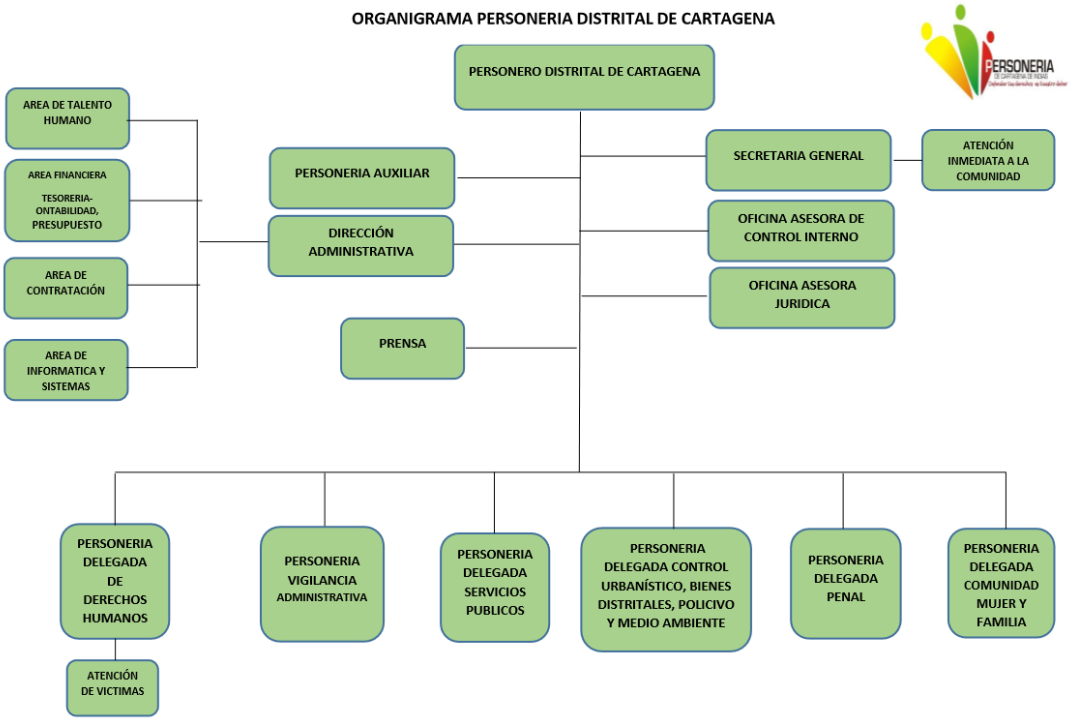
2.3 OBJETIVOS ESTRATÉGICOS

- **Objetivo 1.** Promover actividades de promoción, prevención, protección y concientización sobre los Derechos Humanos
- **Objetivo 2**. Fortalecer la atención al ciudadano de manera permanente con el fin de generar confiablidad en la prestación de los servicios de la entidad.

- **Objetivo 3.** Prestar servicios de asistencia y asesoría jurídica bajo criterios de calidad oportunidad y calidez humana.
- **Objetivo 4**. Activar mecanismos eficaces que permitan realizar seguimiento evaluación y vigilancia a los programas de la Administración Distrital y al comportamiento de los servidores públicos.
- **Objetivo 5**. Sensibilizar y promover el conocimiento, el respeto, la preservación de los derechos, el cumplimiento de los deberes y el correcto actuar de los servidores públicos a través de acciones preventivas, así como el ejercicio de un control disciplinario eficiente y eficaz
- **Objetivo 6**. Diseñar implementar y consolidar la tecnología de la información y las comunicaciones, para una gestión institucional eficiente y eficaz que brinde orientación oportuna a los usuarios y acerquen a la entidad a la comunidad.
- **Objetivo 7.** Diseñar e implementar una gestión del talento humano destinada a elevar el nivel de formación competencias, sentido de pertenencia y crecimiento personal de los servidores públicos de la ciudad
- **Objetivo 8**. Implementar una estrategia de lucha contra la corrupción mediante la sociabilización de los funcionarios, participación ciudadana, el acceso a la información pública y la rendición de cuentas
- **Objetivo 9.** Promover una cultura de calidad buen servicio y mejora continua en los procesos institucionales en el marco de los estándares internacionales y la normativa vigente

FUENTE:PEI “PERSONERIA SOMOS TODOS”2020-2024 PERSONERIA DISTRITAL DE CARTAGENA

2.4 ESTRUCTURA ORGANICA Y DE FUNCIONES



FUENTE: PEI “PERSONERIA SOMOS TODOS”2020-2024 PERSONERIA DISTRITAL DE CARTAGENA

2.5 MAPA DE PROCESOS

La Institución en aras del cumplimiento de la Ley y de nuestras funciones, está conformada por procesos y dependencias, con el propósito de ofrecer resultados con calidad en beneficio de la población, asegurando un ejercicio con eficacia, eficiencia y oportunidad.

FUENTE:PEI "PERSONERIA SOMOS TODOS"2020-2024 PERSONERIA DISTRITAL DE CARTAGENA

2.6 LA ESTRUCTURA DEL MECI

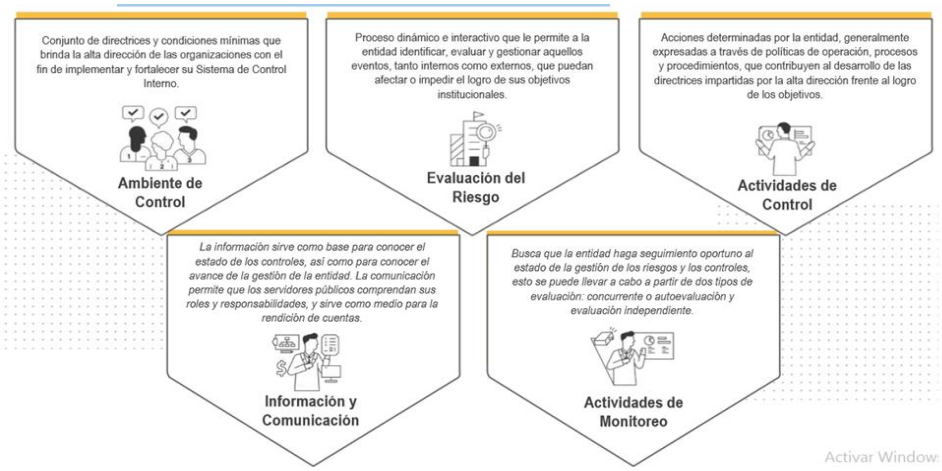
A través de la 7ma Dimensión del Modelo Integrado de Planeación y Gestión MIPG, el MECI actualizado busca proporcionar una estructura de control de la gestión que especifica los elementos necesarios para construir y fortalecer el Sistema de Control Interno, busca dejar de ser entendido como una herramienta de gestión más de las organizaciones.

La estructura del Modelo Estándar de Control Interno contempla dos elementos fundamentales:

A. La estructura del MECI actualizado está integrada por cinco componentes teniendo como referente el modelo COSO y permeada por una asignación clara de responsabilidades frente a la gestión de riesgos y del control (enmarcado los Lineamientos Estratégicos y las Tres Líneas de Defensa), no siendo tarea exclusiva de las oficinas de control interno.

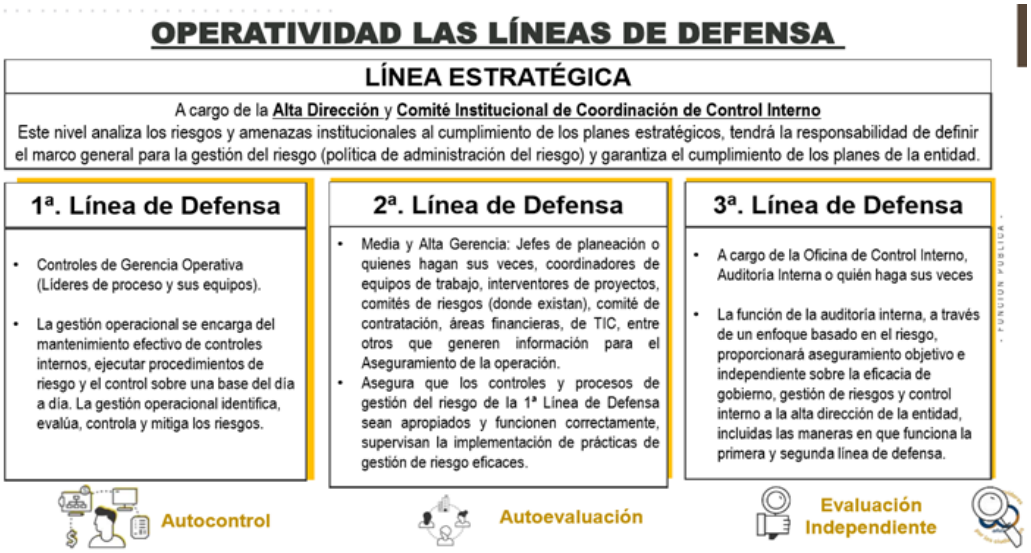
Los componentes que contempla la actualización son: Ambiente de control, Evaluación de riesgos, Actividades de control, Información y comunicación y Actividades de monitoreo.

Componentes de la Estructura del MECI



B. Un esquema de responsabilidades integrada por cuatro líneas de defensa, el cual se configura a partir de la adaptación del esquema de “Líneas de Defensa”, que “proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados. Este modelo proporciona una mirada nueva a las operaciones, ayudando a asegurar el éxito continuo de las iniciativas de gestión del riesgo, y este modelo es apropiado para cualquier entidad – independientemente de su tamaño o complejidad” (IIA 2013:2). Las responsabilidades de la gestión de riesgos y del control están distribuidas en varias áreas y no se concentran en las oficinas de control interno; de allí que deban ser coordinadas cuidadosamente para asegurar que los controles operen. La adaptación este enfoque se presenta en la siguiente gráfica.

2.7 ESQUEMA LÍNEAS DE DEFENSA



LINEA ESTRATEGICA COMITÉ INSTITUCIONAL DE CONTROL INTERNO		
1ra. Línea de Defensa	**2da Línea de Defensa**	**3ra. Línea de Defensa**
TODOS LOS LIDERES DE PROCESO	**Personero Auxiliar** **Director Administrativo** **Secretario General** **Jefe de Oficina Jurídica**	**Asesora Control Interno**

2.7.1 1ra. Línea de Defensa

Esta línea está bajo la responsabilidad, principalmente, de los líderes de Procesos, programas, procesos y proyectos y de sus equipos de trabajo.

TIPO DE PROCESO	RESPONSABLE	PROCESO
PROCESOS ESTRATÉGICOS	Personero Auxiliar	Líder del proceso de Gestión de Direccionamiento y Planeación Estratégica
		Líder del proceso de Gestión del Desempeño y la Calidad
		Líder Control Interno Disciplinario
	Jefe de Oficina Asesora de Prensa	Líder del Proceso de Tecnología, Información y Comunicación
PROCESOS MISIONALES	Secretaria General	Líder del Proceso de Atención inmediata a la comunidad (sede principal y localidades)
	Personero Delegado	Líder del proceso de Gestión de Vigilancia a la conducta Oficial
GESTIÓN DE PROMOCIÓN Y PROTECCIÓN DE LOS DERECHOS HUMANOS	Personero Delegado	Líder de la P. Delegada para los derechos humanos
	Personero Delegado	Líder de la P. Delegada en lo Penal
	Jefe de Oficina	Atención a Víctimas y Trabajo Social
GESTIÓN DEL INTERÉS COLECTIVO Y PARTICIPACIÓN CIUDADANA	Personero Delegado	Líder de la P. Delegada para la Comunidad, Menor y Familia
	Personero Delegado	Líder de la P. Delegada para Urbanístico, Policivo y Medio Ambiente
	Personero Delegado	Líder de la P. Delegada para los Servicios Públicos
PROCESOS DE APOYO	Secretaria General	Líder del Proceso de Gestión Documental y Archivo
	Jefe de Oficina Jurídica	Líder del Proceso de Gestión Jurídica
PROCESO DE APOYO	Asesor TH	Área del Talento Humano (Seguridad y salud en el trabajo, Bienestar Social, Código de Integridad, Capacitación, inducción y reinducción) Nomina
	Asesor	Contratación
	Jefe de Oficina Presupuesto	Presupuesto y Contabilidad
	Almacenista	Almacén
PROCESO DE EVALUACIÓN	Asesora	Líder del Proceso del Control y Seguimiento

2.7.2 2da. Línea de Defensa

La 2da. Línea de Defensa responde de manera directa por el aseguramiento de la operación; en la Personería Distrital de Cartagena está bajo la responsabilidad de:

RESPONSABLE	PROCESO

Personero Auxiliar	Líder del Proceso de Gestión de Direccionamiento y Planeación Estratégica
Director Administrativo	Líder del Proceso de Gestión Administrativa y Financiera
Secretaria General	Líder del Proceso de Gestión Documental y Archivo
Jefe de Oficina Jurídica	Líder del Proceso de Gestión Jurídica

2.7.3 3ra. Línea de Defensa

Esta 3ra Línea de Defensa en la Personería Distrital de Cartagena está bajo la responsabilidad de la asesora de control interno.

Dado lo anterior, se muestra la alineación de la presente política la Modelo Integrado de Planeación y Gestión MIPG, dimensión 7 implementada en la Personería Distrital de Cartagena.

3. PASO 1- POLITICA DE ADMINISTRACION DE RIESGO

La Personería Distrital de Cartagena, asume el compromiso de administrar los riesgos por proceso, corrupción y de seguridad digital que puedan afectar de manera negativa el alcance de los objetivos estratégicos y objetivos de procesos de la entidad; del mismo modo busca forjar una entidad más proactiva que reactiva, previniendo y reduciendo los efectos no deseados promoviendo la mejora continua, propendiendo una organización basada en la acción preventiva automática enfocada en la administración del riesgo, con control en todos los niveles de la entidad, brindando seguridad razonable destinando los esfuerzos necesarios para administrar los riesgos que se puedan presentar en la entidad.

3.1 LINEAMIENTOS DE LA POLITICA

3.2 OBJETIVOS:

3.2.1 Objetivo General de la Política de Administración de Riesgos

Definir la política de Administración de Riesgo de la Personería Distrital de Cartagena de forma articulada con las normas aplicables a la Entidad y a su Sistema Integrado de Gestión, como mecanismo para identificar, medir, valorar, monitorear, administrar y tratar los riesgos de gestión y corrupción, que pudieran afectar el logro de sus objetivos institucionales.

3.2.2 Objetivos Específicos

- Crear una estrategia sistemática, estructurada y oportuna para la administración de los riesgos.
- Alinear el apetito de riesgo con la estrategia adoptada por la entidad
- Proteger los recursos de la entidad, resguardándolos contra la materialización de los riesgos valorados como amenazas de corrupción.
- Introducir y fortalecer dentro de los procesos y procedimientos puntos de control, que permitan evitar, reducir o mitigar, las vulnerabilidades o potenciales amenazas que se puedan presentar.
- Mejorar el aprendizaje organizacional frente a la eficaz identificación y administración de los riesgos.
- Permitir la mejora continua de los procesos de la organización

3.3 ALCANCE

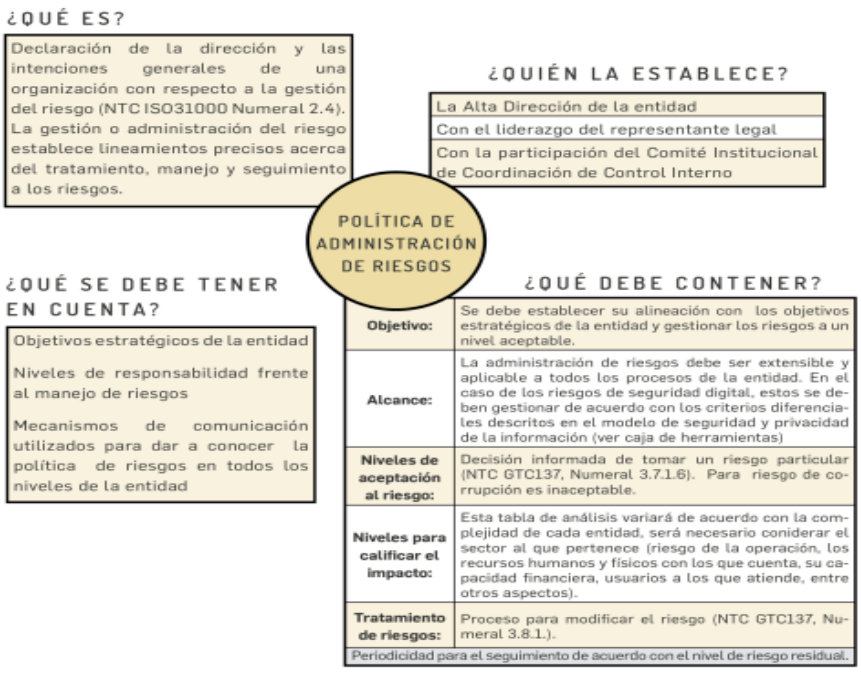
La Política de Administración de Riesgo de la Personería de Cartagena será aplicable a todos los procesos de la entidad y todos los controles serán aplicados en todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones dándoles el tratamiento necesario bajo la metodología establecida y la tipología del riesgo.

3.4 METODOLOGIA

Se aplicará la metodología establecida por el Departamento Administrativo de la Función Pública, descrita en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas." V5 Diciembre 2020, así como los lineamientos del Modelo Integrado de Planeación y Gestión MIPG- Según lo contemplado en la normatividad vigente, Decreto 1499 de 2017.

La política que desarrollara la Personería Distrital de Cartagena a fin de realizar una adecuada identificación de los riesgos iniciará determinando las causas que pueden originar los mismos, en consecuencia, se tendrán como base los factores internos y/o externos y que amenazan con interrumpir el cumplimiento de los objetivos misionales e institucionales de la entidad.

Figura 5 Estructuración de la política de administración de riesgos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas." V5 Diciembre 2020

Los formatos, metodología y herramientas para el manejo de los riesgos serán los establecidos en el procedimiento Administración de Riesgo. El mapa o matriz de riesgos será la herramienta conceptual y metodología para la valoración de los riesgos en la Personería Distrital de Cartagena.

Se construirá el mapa de riesgos por cada uno de los procesos de la entidad y se construirá por parte de la oficina de control interno el mapa de riesgo institucional, el cual contendrá los riesgos con valoración en zona de riesgo externa.

La Personería Distrital de Cartagena cuenta con un Sistema de Información para el Registro del Sistema de Gestión en Calidad –SIGPER, el cual es utilizado en la entidad para administrar los riesgos, en identificación, valoración, seguimiento y evaluación, tanto los institucionales y por procesos.

Los factores internos y externos determinados por la Guía de Administración del Riesgo de la Función pública para tener en consideración para la administración del Riesgo en la Personería Distrital de Cartagena son los siguientes:

- **Contexto externo:** Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:
  - Políticos
  - Económicos y financieros
  - Sociales y culturales
  - Tecnológicos
  - Ambientales
  - Legales y reglamentarios
  - Grupos de interés externos y partes interesadas.

- Clientes, proveedores de servicio y empresas.
- Cantidad de ciudadanos afectados por el servicio

- **Contexto interno:** Cuales son los rasgos distintivos que dictan la manera en la cual opera internamente la entidad y busca alcanzar sus objetivos:
  - Misión
  - Visión
  - Valores
  - Estructura organizacional
  - Funciones y responsabilidades
  - Políticas, procesos y procedimientos. Objetivos y estrategias implementadas.
  - Sistema integrado de gestión.
  - Recursos y conocimientos con que se cuenta (económicos, social, ambiental, físico, financiero, jurídico, personas, procesos, sistemas, tecnología, información)
  - Relaciones con las partes involucradas
  - Cultura organizacional

- **Contexto del Proceso:** Cuales son las características o aspectos esenciales del proceso, si este está directamente relacionado con un objetivo estratégico de la entidad, cuál es su alcance, cuáles son las entradas y las salidas derivadas de las actividades que se realizan en su interior:
  - Objetivo del proceso
  - Alcance del proceso
  - Caracterización del proceso
  - Interrelación con otros procesos
  - Procedimientos asociados
  - Responsables del proceso
  - Cantidad de ciudadanos afectados por el proceso
  - Procesos de gestión de riesgos actualmente implementados
  - Activos de seguridad digital del proceso

3.5 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 la alta dirección consideran que no sería posible el logro de los objetivos de la entidad**.**

4. PASO 2- IDENTIFICACIÓN DEL RIESGO

La alta dirección, identificará los riesgos que estén o no bajo el control de la misma, se tendrá en cuenta 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. En cumplimiento de lo anterior se desarrollara lo siguiente:

4.1 Análisis de objetivos estratégicos y de los procesos: los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

Dado que los objetivos estratégicos y de proceso se alcanzan por medio de actividades, el paso a seguir corresponde a identificar las actividades cruciales para la consecución de los objetivos, de esta manera la

identificación de los riesgos que se llevará a cabo en la siguiente etapa estará focalizada en estas actividades.

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

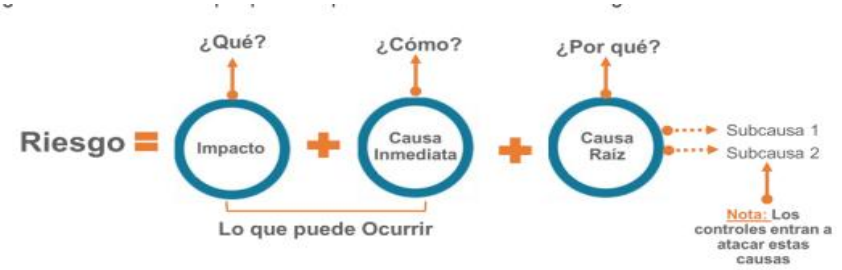
Fuente: Comitte of Sponsoring Orgizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio. p. 73. 2013.

4.2 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.

4.3 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.

4.4 Identificación de áreas de factores de riesgo: son las fuentes generadoras de riesgos.

4.5 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:



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

Es necesario aclarar que al definir el riesgo se debe evitar comenzar con palabras negativas como las siguientes palabras: “No”, “Que no”. O con palabras que denoten una causa como: “ausencia de…”, “falta de…”, “deficiente…”.

Se debe especificar que <u>TODOS</u> los procesos de la entidad deben tener al menos un riesgo de gestión identificado, el cual debe estar debidamente estructurado en la Matriz de Riesgos por Proceso, definida por la entidad para el efecto.

Desglosando la estructura propuesta tenemos:

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

se deben establecer las causas que pueden provocar que los eventos de riesgos se materialicen; para que esta identificación se elabore de una manera robusta se recomienda que se lleve a cabo por medio de un análisis de matriz DOFA el cual se explica a continuación:

La matriz **DOFA** (**Debilidades**, **Oportunidades**, **Fortalezas** y **Amenazas**) es una técnica para organizar los factores internos y externos que afectan positiva y negativamente la forma en la cual una organización alcanza sus objetivos.

Las debilidades y fortalezas son de carácter interno y estas provienen del análisis del contexto interno y el contexto del proceso; por otro lado, las oportunidades y las amenazas provienen del análisis del contexto externo de la entidad.

DEBILIDADES	OPORTUNIDADES
• Contexto interno • Contexto del proceso	• Contexto externo
FORTALEZAS	**AMENAZAS**
• Contexto interno • Contexto del proceso	• Contexto externo

Una vez este diligenciada la matriz DOFA, si se observan las casillas de **Debilidades** y **Amenazas**, en estas estarán consignadas las causas más significativas que facilitarán la materialización de los eventos de riesgo

4.6 Clasificación del riesgo: permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías :

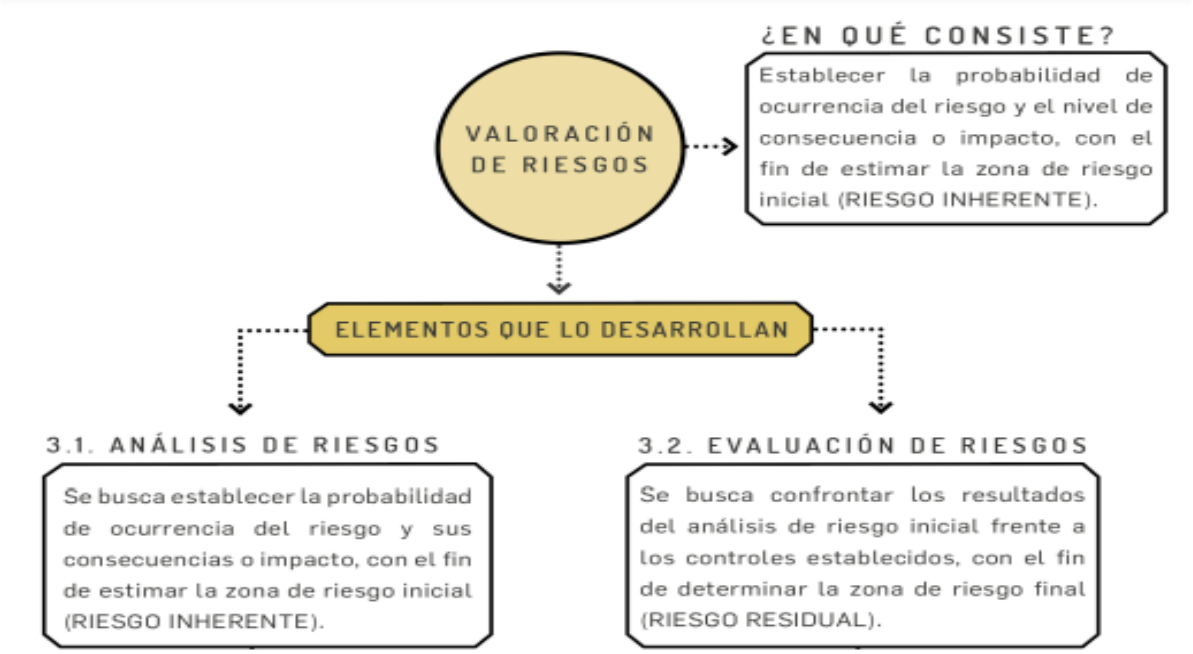
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones 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.

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

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

5. PASO 3- VALORACION DEL RIESGO

se busca determinar cuál es el nivel de riesgo derivado de la probabilidad de materialización del riesgo junto con el impacto que este tendría en los objetivos del proceso (en los objetivos estratégicos, si es el caso).



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

5.1 Análisis de riesgos; La entidad establecerá la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

5.2 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.

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

Fuente: 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

5.3 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

5.4 Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. La afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional 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 facilitará 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.

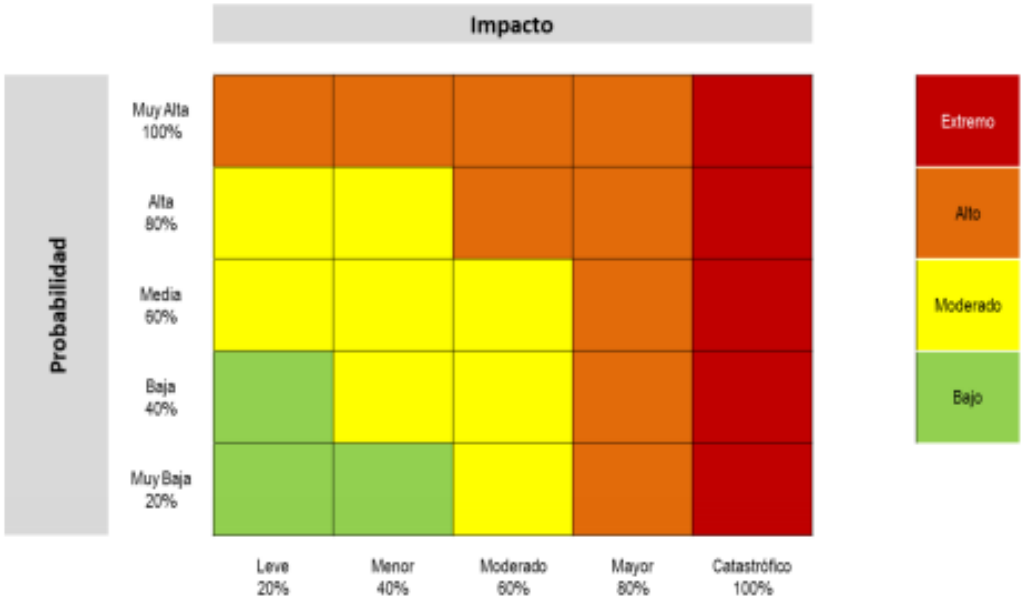
A continuación se muestra los criterios para definir el impacto:

	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.

5.5 Evaluación de riesgo : a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto s, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE)

Análisis preliminar (riesgo inherente): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor



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

Si el nivel del riesgo inherente es **bajo**, el líder del proceso puede tomar la decisión de aceptar el riesgo y no será necesaria la implementación de una medida de mitigación, en otras palabras, la entidad solo tendrá un nivel de tolerancia al riesgo **bajo.**

Por otro lado, si el nivel de riesgo inherente es mayor a **bajo**, obligatoriamente se debe implementar una medida de mitigación, ya sea **reducir el riesgo** *(implementar*

un control), **evitar el riesgo** *(dejar de realizar la actividad con la cual está relacionada el riesgo)* o **compartir el riesgo** *(transfiriéndolo o compartiéndolo con un agente externo al proceso implementando un nuevo control)*.

6. CONTROLES

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

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

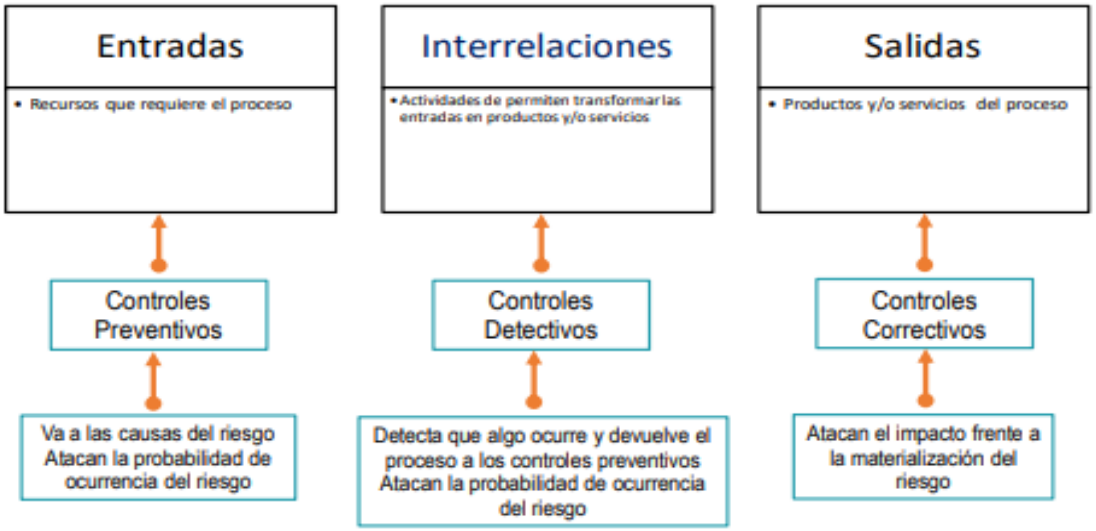
6.2 Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración.

La estructura es la siguiente:

Responsable de ejecutar el control: identifica	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	Este corresponde a los detalles que permiten identificar claramente el objeto del control.

6.3 Tipología de controles y los procesos: a través del mapa de procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su

tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura a continuación se consideran 3 fases globales del ciclo de un proceso así:



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

Según 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.
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 Análisis y evaluación de los controles – Atributos: se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

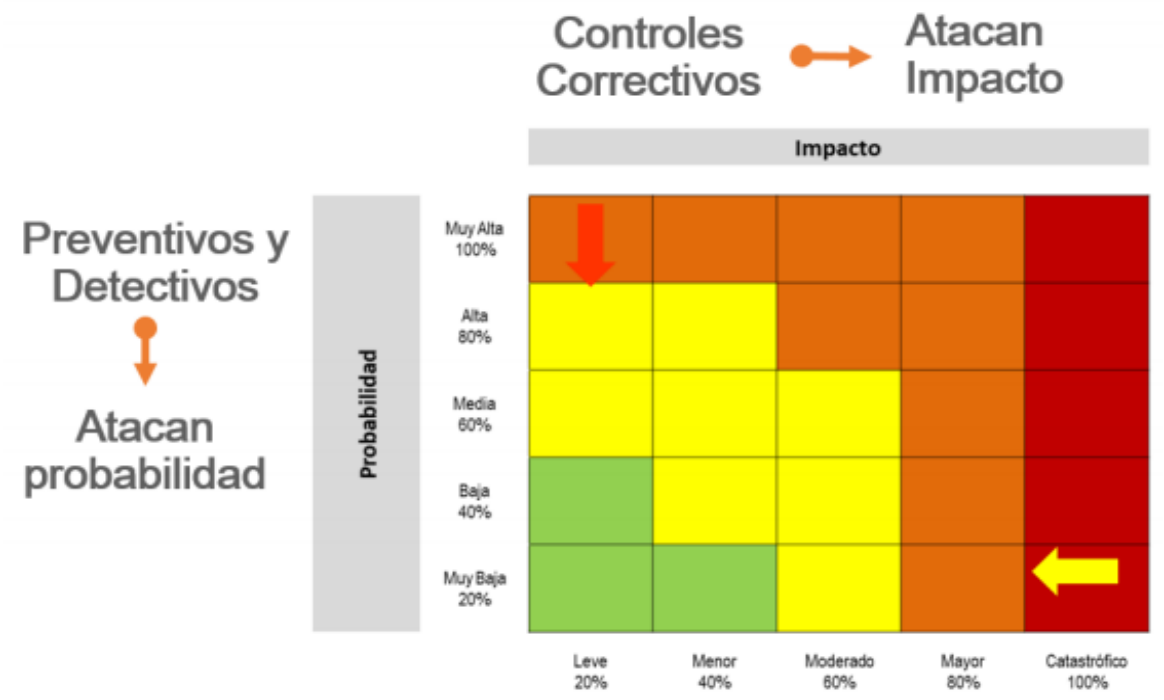
Se puede observar la descripción y peso asociados a cada uno así:

CARACTERISTICAS			DESCRIPCION	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 e n su implementación.	10%
	IMPLEMENTACION	AUTOMATICO	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		MANUAL	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
		DOCUMENTADO	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-

ATRIBUTOS INFORMATIVOS	DOCUMENTACION	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. Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la siguiente matriz de calor que corresponde se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



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

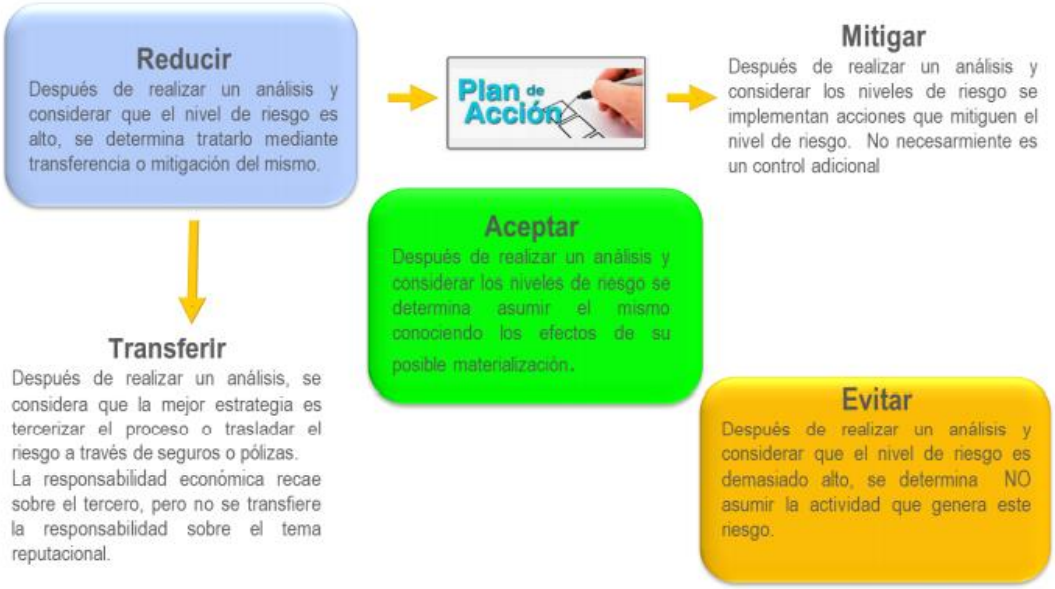
6.5 Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles,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

7. ESTRATEGIAS PARA COMBATIR EL RIESGO

En la Personería Distrital de Cartagena, la decisión que se toma frente a un determinado nivel de riesgo, puede ser aceptar, reducir o evitar, (tomando los lineamientos de la guía)

Para los procesos que se encuentran en funcionamiento se analiza frente al riesgo residual, y cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

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.

Con respecto al plan de acción mencionado en esta política, 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.

8. HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO

Como producto de la aplicación de la metodología se contará con los mapas de riesgo.

Además de esta herramienta, se tienen las siguientes:

Gestión de eventos: un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles.

En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología. Algunas fuentes para establecer una base histórica de eventos pueden ser:

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

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

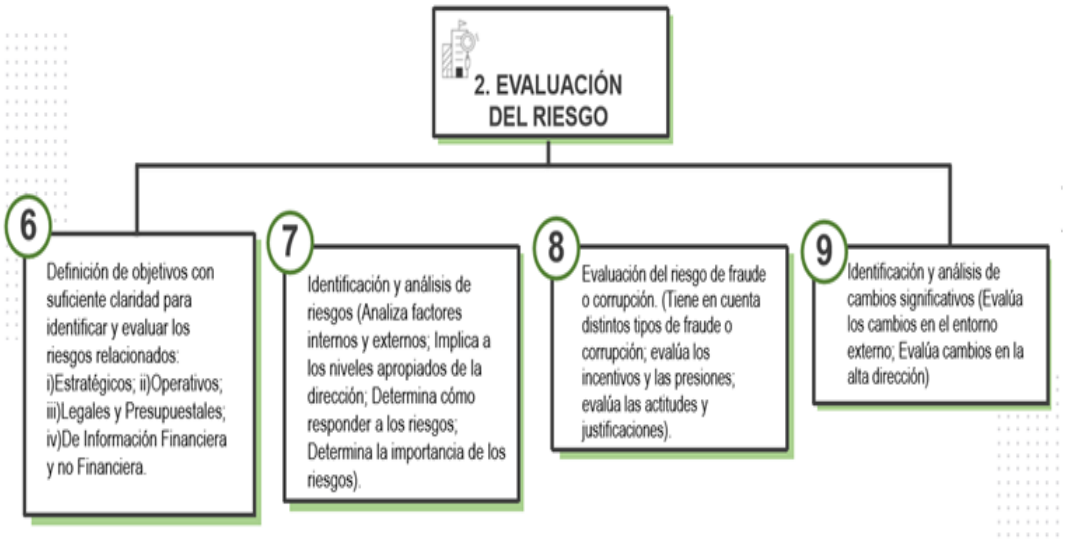
Desempeño del control= # eventos / frecuencia del riesgo (# veces que se hace la actividad)

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.

9. MONITOREO Y REVISIÓN

El modelo integrado de plantación 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 mostramos en la alineación de la Política con el MIPG, a continuación se muestra una gráfica que nos presenta la evaluación del riesgo en nuestra entidad, su fuente es el Manual 7ma Dimensión MIPG Control Interno y las Líneas de Defensa:



PROCESOS ASOCIADO	ASPECTO A IMPLEMENTAR	LINEA DE DEFENSA RESPONSABLE	ASPECTO A EVALUAR DEL SISTEMA DECONTROL INTERNO	EVIDENCIAS
Todos los procesos	Definición de objetivos con suficiente claridad para identificar y evaluar los riesgos	1era y 2da línea de defensa	Generación de reportes periódicamente al Comité Institucional de Coordinación de Control Interno acerca del cumplimiento de las metas y los objetivos en relación a la gestión integral del riesgo.	Caracterización del proceso Mapa de procesos Política de operaciones Procedimientos Mapa de riesgo por proceso Indicadores de gestión Informes de gestión y cumplimiento de plan de acción
Todos los procesos	Identificación y análisis de riesgos (Analiza factores internos y externos; Implica a los niveles apropiados de la dirección; Determina cómo responder a los riesgos; Determina la importancia de los riesgos).	1era y 2da línea de defensa	Monitoreo permanentemente los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI. Revisión de las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico). Verificación, en el marco de la política de riesgos institucional, que la identificación y valoración del riesgo de la primera línea sea adecuada frente al logro de objetivos y metas	Política de Riesgos Institucionales Mapa de aseguramiento Mapa de riesgo por proceso Mapa de riesgos institucionales Seguimientos y monitoreo
Todos los procesos	Evaluación del riesgo de fraude o corrupción. (Tiene en cuenta distintos tipos de fraude o corrupción; evalúa los incentivos y las presiones; evalúa las actitudes y justificaciones).	1era y 2da línea de defensa	Verificación de la adecuada identificación de los riesgos relacionados con fraude y corrupción	Plan anticorrupción y de atención al ciudadano Mapa de riesgos de corrupción Seguimiento a los riesgos de corrupción

Fuente: Manual 7ma Dimensión MIPG y Las Líneas de defensa Personería de Cartagena


LÍNEA 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 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.

10. GESTION DE RIESGOS DE CORRUPCION

De acuerdo con las políticas de transparencia, acceso a la información pública y lucha contra la corrupción liderada por la Secretaría de Transparencia y la de Gobierno Digital, y siguiendo los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018(vigente para la gestión de riesgos de corrupción) se establecen las pautas para el tratamiento la gestión de riesgos de corrupción de la Personería Distrital de Cartagena

A continuación se brindan los parámetros para administrar correctamente los Riesgos por corrupción reiterando que se debe partir de los lineamientos básicos precisando y analizando el contexto general de la Personeria Distrital de Cartagena enmarcando principalmente la planeación institucional, el modelo de operación, la cadena de valor, el mapa de procesos, los objetivos estratégicos, la caracterización de los procesos, la misión y la visión para lograr establecer su complejidad y de esta forma conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general reiterando que se hace necesaria una participación integral entre el líder del proceso, y los funcionarios del mismo buscando que la identificación, el análisis, el tratamiento y el seguimiento de los riesgos se lleven a cabo con una visión integral de todas las actividades propias de la oficina que podrían desencadenar en un evento de riesgo.

10.1 Identificación de riesgos

Definición de riesgo de corrupción: Es la 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).

En la descripción del riesgo se agrupan 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, estos deben estar descritos de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Facilitando la identificación de los riesgos de corrupción y evitar que se lleguen a confundir entre un riesgo de gestión y uno de corrupción se sugiere utilizar la matriz de definición de riesgo de corrupción, esta incorpora cada uno de los componentes de su definición. En la siguiente matriz, si se marca con u na 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	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

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

10.2 Generalidades

- 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 de trabajo.
- **Consolidación:** en la entidad la oficina de Direccionamiento y planeación Estratégica, en colaboración con la oficina de control y seguimiento le

corresponderá liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

10.3 Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.

En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación. Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

10.4 Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción. Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

10.5 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.

10.6 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.

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

A continuación se muestra una gráfica de información anonimizada que nos presenta la Guía de administración de riesgos para entidades públicas.

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.

Fuente Secretaría de Transparencia.

11. VALORACIÓN DE RIESGOS

11.2 Cálculo de la probabilidad e impacto

11.2.1 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 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.

(Fuente DAFP)

11.2.2 Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo Criterios para calificar el impacto en riesgos de corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA 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.	10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

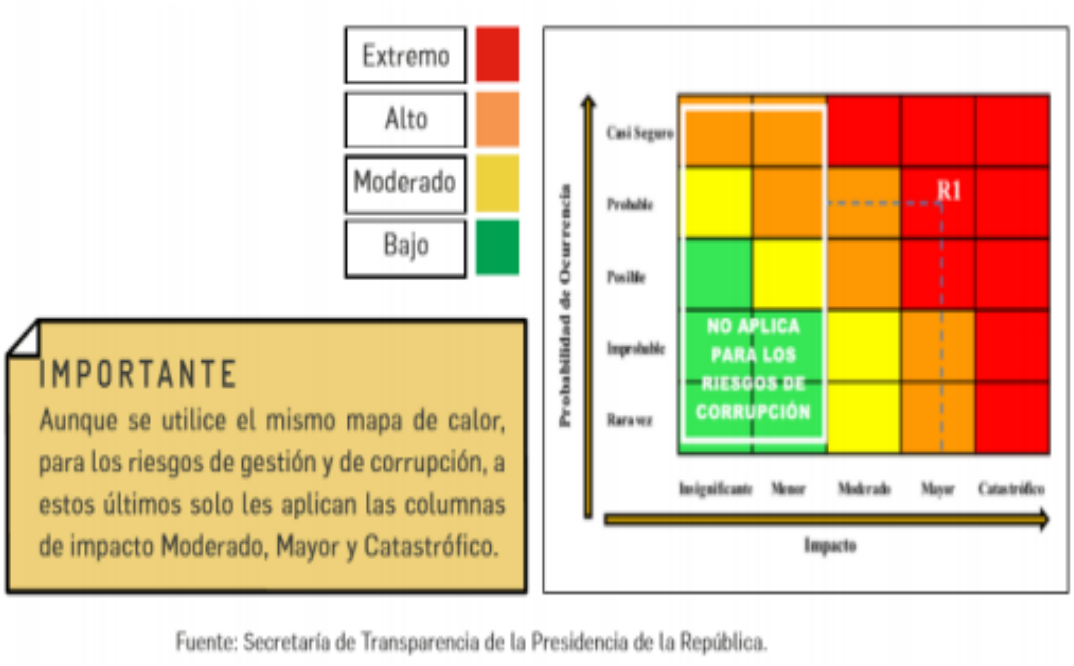
Nivel de impacto MAYOR

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

.

11.2.3 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.

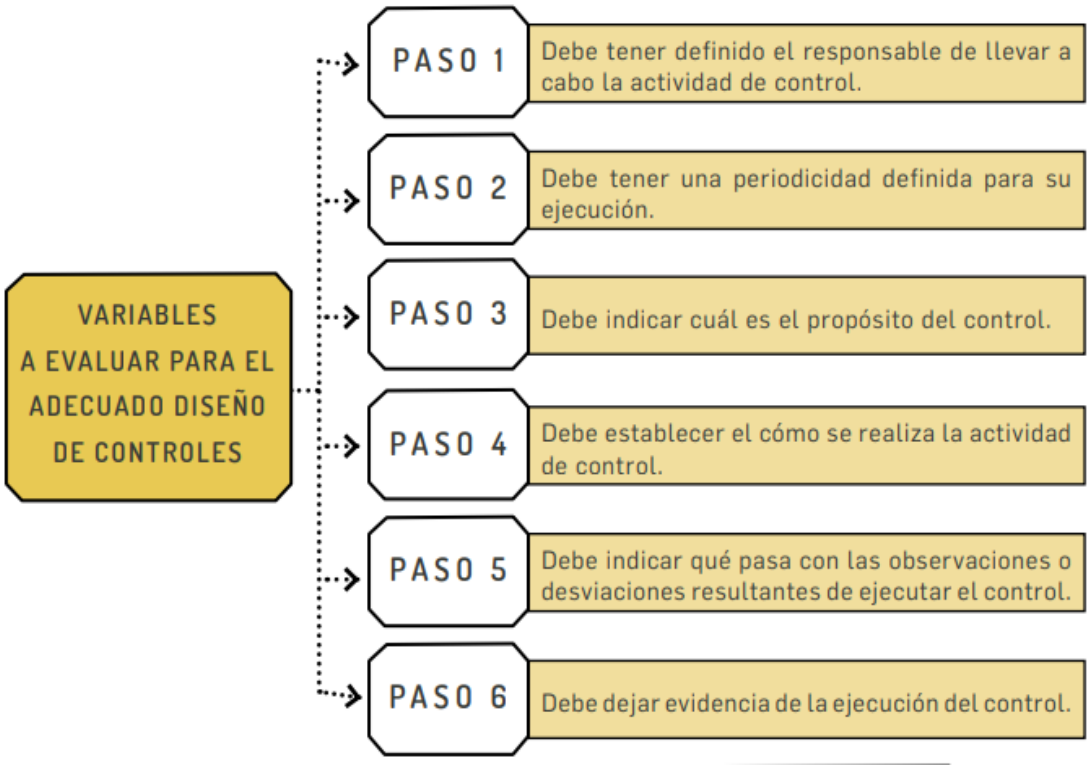


Fuente: Secretaría de Transparencia de la Presidencia de la República.

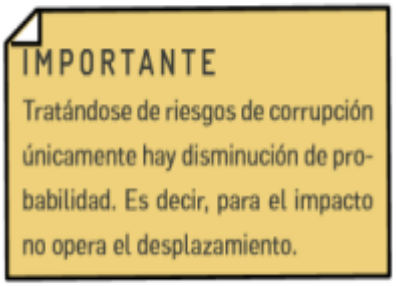
12. VALORACIÓN DE LOS CONTROLES – DISEÑO DE CONTROLES

Antes de valorar los controles es necesario conocer cómo se diseña un control, para lo cual daremos respuesta a las siguientes interrogantes: ¿Cómo defino o establezco un control para que en su diseño mitigue de manera adecuada el riesgo?

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:



Nivel del riesgo (riesgo residual) Desplazamiento del riesgo inherente para calcular el riesgo residual.

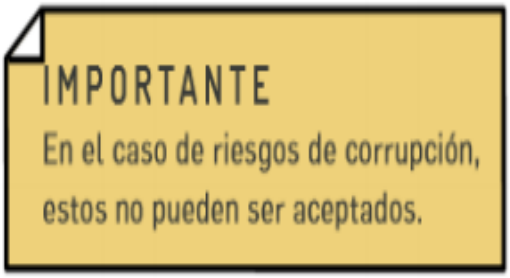


13. TRATAMIENTO DEL RIESGO

Para el tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Fuente: DAFP

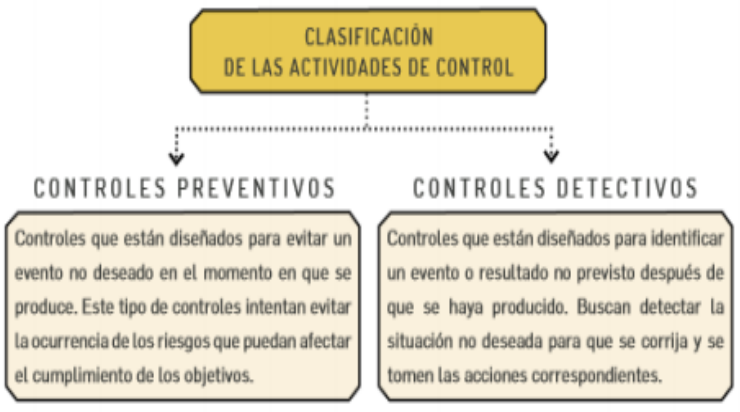


EVITAR EL RIESGO Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

COMPARTIR EL RIESGO Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

REDUCIR EL RIESGO El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo. Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

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



(Fuente DAFP)

14. MONITOREO DE RIESGOS DE CORRUPCIÓN

Los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de Direccionamiento y planeación Estratégica de la Personería Distrital de Cartagena, adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz.

El **monitoreo** se realizara trimestralmente. Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar. Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

Reporte de la gestión del riesgo de corrupción, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado

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 un lugar de fácil acceso para el 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.

Acciones a seguir en caso de materialización de riesgos de corrupción

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

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.

2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.

3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.

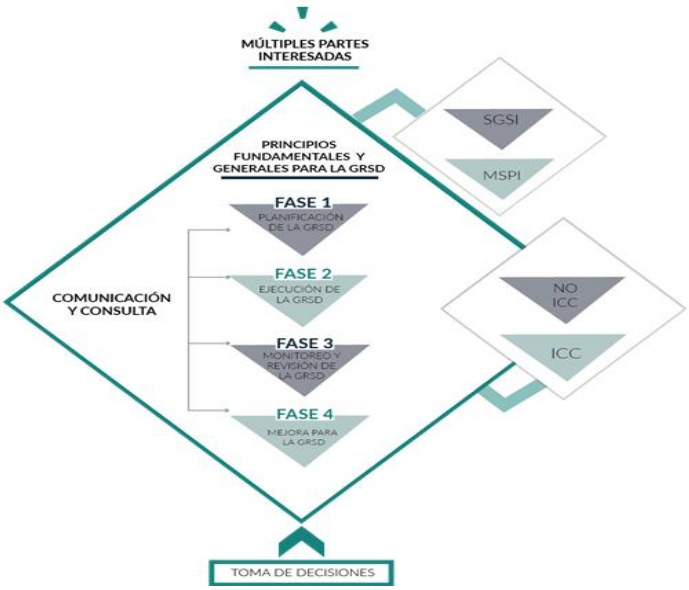
4) Llevar a cabo un monitoreo permanente. La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

■ Determinar la efectividad de los controles.
■ Mejorar la valoración de los riesgos.
■ Mejorar los controles.
■ Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
■ Determinar si se adelantaron acciones de monitoreo.
■ Revisar las acciones del monitoreo.

15. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos mencionados en este capítulo hacen referencia a los riesgos asociados a la Seguridad Digital (datos Personales y de seguridad y privacidad de la Información) están asociados a información en cualquier medio dentro de la entidad, en la siguiente gráfica se definen las fases que la Personería Distrital de Cartagena adelanta para dicha gestión y la integración con el SGSI (Sistema de Gestión de Seguridad de la Información) o MSPI (Modelo de Seguridad y Privacidad de la Información), así como la relación con todos los activos de información de la entidad incluyendo las ICC (Infraestructuras Criticas Cibernéticas), adoptando lo establecido por el MGRSD (Modelo de Gestión de Riesgos de Seguridad Digital) determinado por MINTIC de la siguiente forma:



Marco conceptual del MGRSD. Fuente: Modelo de Gestión de Riesgos de Seguridad Digital – MINTIC

16. CONOCIMIENTO DE LA ACTUAL POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La presente es de conocimiento general para los funcionarios y contratistas de la Personería Distrital de Cartagena, en este documento se especifican los lineamientos técnicos con los cuales se ejecuta la gestión del riesgo en la entidad por ende toda persona que interactúe con procesos y procedimientos debe actuar activa y oportunamente considerando su conocimiento, punto de vista y percepciones, desencadenando en una mayor toma de conciencia y una gestión de riesgo informada.

A continuación, se detallan los Principios fundamentales y generales establecidos para la gestión del riesgo de seguridad digital:

Los Principios Fundamentales están en el documento CONPES 3854 del 11 de abril de 2016; a continuación, se presenta su interacción con el Modelo de Gestión de Riesgos de Seguridad Digital:

- Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia
- Todas las partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales.
- Adoptar un enfoque incluyente y colaborativo
- La personería distrital de cartagena debe involucrar a todas las partes interesadas, a través de la comunicación y a consulta, con el fin de promover la seguridad digital del país.
- Asegurar una responsabilidad compartida entre las múltiples partes interesadas
- La personería distrital de cartagena debe establecer el rol y grado de responsabilidad de cada una de las partes interesadas para gestionar los riesgos de seguridad digital.
- Adoptar un enfoque basado en la gestión de riesgos

Los Principios Generales están basados en lo definido por la norma para la gestión del riesgo: principios y directrices. NTC-ISO 31000:2011.

La gestión de riesgos de seguridad digital:

a) Crea y protege el valor
b) Es una parte integral de todos los procesos de la organización

c) Es parte de la toma de decisiones
d) Se basa en la mejor información disponible
e) Está adaptada
f) Toma en consideración los factores humanos y culturales.
g) Es transparente e inclusiva
h) Facilita la mejora continua de la organización

16.1 Planificación de la GRSD

La Planificación de la gestión de riesgo de seguridad digital está basada en la directriz otorgada por el Modelo de Gestión de Riesgos de Seguridad Digital.

Planificación de la GRSD. Fuente: Modelo de Gestión de Riesgos de seguridad digital

Se definen las siguientes actividades las cuales han sido efectuadas de la siguiente forma:

16.2 Compromiso de la Alta Dirección: La alta dirección con el compromiso de facilitar el cumplimiento de los objetivos sobre la gestión del riesgo de seguridad digital, estableció mediante la presente política los roles y responsabilidades, que aportan los recursos necesarios para que el proceso se desarrolle en la entidad de forma efectiva

16.3 Establecimiento de contexto: Se identifican los aspectos que generan mayor impacto en los procesos, los objetivos y la relación con el medio digital (usuarios, infraestructura, servicios y aplicaciones)

Se deben considerar los siguientes factores relacionados con el entorno digital:

CONTEXTO EXTERNO

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 1499 de 2017.
- Dependencias económicas y financieras por parte de otras empresas.
- Entorno cultural.
- Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local.
- Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web.
- Aspectos externos que pueden verse afectados con los riesgos de seguridad de la información, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad pública.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

- **Identificación de las partes interesadas y procesos** Se desarrolla con la gestión del contexto de la entidad identificando las partes interesadas y procesos que se afecten o puedan verse afectadas en el entorno digital
- **Armonización de la política de seguridad de la información existente:** La entidad cuenta con los lineamientos establecidos por los diferentes sistemas de gestión de riesgos ya implementados internamente y adopta las determinaciones otorgadas por el Departamento Administrativo de la Función Pública.
- **Definición de roles y responsabilidades para la gestión de riesgos de seguridad digital.**
- **Definición los recursos necesarios para la gestión de riesgos de seguridad digital**: La Personería Distrital de Cartagena, debe disponer de los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad digital; recursos tales como:
  - ✓ Personal capacitado e idóneo para la gestión de riesgos de seguridad digital

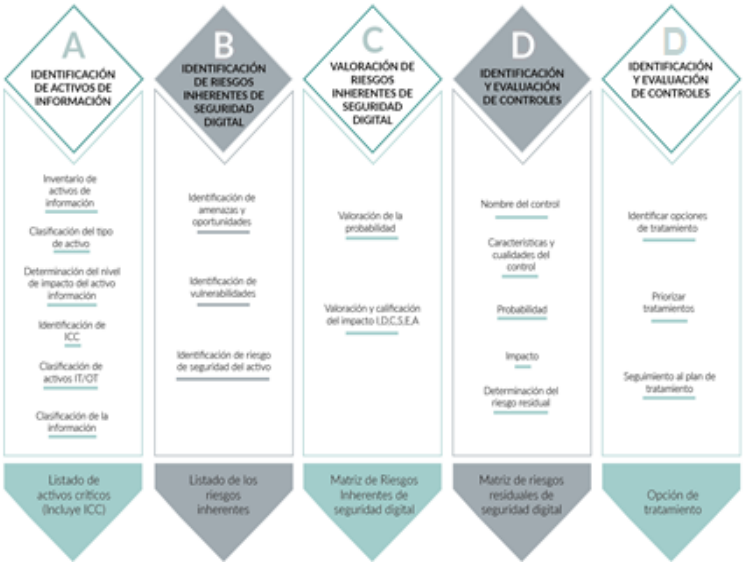
- ✓ Recursos económicos para la implementación de controles
- ✓ Recursos para los aspectos de mejora continua, monitoreo y auditorias

- **Definición de los criterios para la gestión de riesgos de seguridad digital:** La personería establece los niveles de referencia frente a los cuales se determina la importancia del riesgo. Lo anterior con los criterios de probabilidad e impacto, su valoración, el tratamiento de riesgo, el apetito de riesgo y la zona de aceptación de riesgos. De igual manera para la gestión de riesgos de seguridad digital, se tienen en cuenta los principios de confidencialidad, integridad y disponibilidad de los activos de información digital, así como los aspectos social, económico y ambiental.

16.4 Ejecución de la GRSD

La ejecución de la Gestión de Riesgos de Seguridad digital consiste en el desarrollo de las actividades para la Identificación de activos de la información, identificación de riesgos Inherentes, Valoración de riesgos, Identificación y evaluación de controles terminado con la Identificación y evaluación de tratamiento a controles lo cual ha sido adoptado de la Fase 2 del Modelo de Gestión de Riesgos de Seguridad Digital-MINTIC que se describe a continuación.

Ejecución de la gestión de riesgos de seguridad digital (GRSD)



Ejecución de la GRSD. Fuente: Modelo de Gestión de Riesgos de Seguridad Digital-MINTIC

16.5 Identificación de los activos de información

La Personeria Distrital de cartagena tiene identificados, clasificados y valorados los activos de información digital teniendo en cuenta que en el contexto de seguridad digital estos se refieren a las aplicaciones, servicios web, redes, información física y digital, TI (Tecnologías de la Información), TO (Tecnologías de la Operación) que se utilizan para el funcionamiento de la entidad.

16.6 Contexto interno y externo de la entidad

Para determinar el contexto externo, la entidad debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:
El contexto interno considera factores que impactan directamente a:

- La entidad pública, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.
- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

PARA LA ENTIDAD PÚBLICA	PARA LOS PROCESOS
• Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros • Flujos de información y los procesos de toma de decisiones • Empleados, contratistas • Objetivos estratégicos y la forma de alcanzarlos • La misión, visión, valores y cultura de la organización • Sus políticas, procesos y procedimientos	• Identificación de los procesos y su respectiva caracterización • Detalle de las actividades que se llevan a cabo en el proceso • Flujos de información • Identificación y actualización de los activos en la cadena de valor de la entidad pública • Recursos • Alcance del proceso • Relaciones con otros procesos de la entidad pública
• Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) • Toda la estructura organizacional • Roles y responsabilidades • Sistemas de información o servicios.	• Cantidad de ciudadanos afectados por el proceso • Procesos de gestión de riesgos que se tienen actualmente implementados • Personal involucrado en la toma de decisiones

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

El contexto interno considera factores que impactan directamente a:

- La entidad pública, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.
- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

Se debe realizar una lista en la que estén enumeradas las partes interesadas externas e internas que tengan relación con la entidad pública y con sus objetivos, misión o visión.

16.7 Alcance

El alcance de la administración del riesgo de seguridad de la información debe ser extensible y aplicable a los **procesos** de la Personería Distrital de Cartagena que indiquen los criterios diferenciales del **Modelo de Seguridad y Privacidad de la Información.**

16.8 Alineación o creación de la política de gestión de riesgo de seguridad de la información.

La personería Distrital de Cartagena debe establecer una política de gestión de riesgo integral, donde se incluya el compromiso en la gestión de los **riesgos de seguridad de la información** en todos sus niveles. Esta actividad es responsabilidad de la **Línea estratégica** dispuesta por el MIPG.

16.9 Definición de roles y responsabilidades

Responsable de Seguridad Digital

La Personería Distrital de Cartagena designó como **responsable de Seguridad Digital** que también es el responsable de la **Seguridad de la Información al Personero Auxiliar o quien haga sus veces,** deberá cumplir las siguientes funciones:

- Actuizar el procedimiento para la Identificación y Valoración de Activos de la Entidad, de acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

16.10 Definición de recursos para la Gestión de riesgos de seguridad de la información

La entidad pública debe disponer los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad de la información, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la

implementación de controles y seguimiento de los riesgos de seguridad de la información.

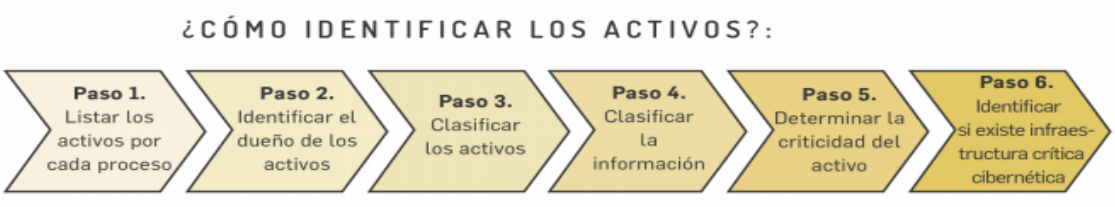
La línea estratégica o alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad de la información.
- Recursos económicos para la implementación de controles para la mitigación de riesgos (con base al análisis de riesgo realizado, teniendo en cuenta el alcance de la política de riesgos de la Entidad en cuanto a seguridad de la información), que permita ser incluido dentro de la gestión presupuestal y eficiencia del gasto público de la Entidad.
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

16.11 Identificación de los activos de seguridad de la 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 **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

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



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

La entidad pública puede decidir si realiza la gestión de riesgos en todos los activos identificados en este punto o si desea hacerlo a los activos más críticos. Esta decisión debe estar debidamente formalizada en el procedimiento de gestión de activos que solicita el **Modelo de Seguridad y Privacidad de la Información**. Adicionalmente, debe quedar explícita en la Política de Administración de Riesgos de la entidad pública, debidamente aprobada por el Comité Institucional de Coordinación de Control Interno.

La identificación y valoración de activos será realizada por la **PRIMERA LÍNEA DE DEFENSA** – líderes de proceso, gestor de proceso orientados por el responsable de seguridad digital y responsable de gestión documental.

La Personería Distrital de Cartagena ha establecido el Registro De Activos De Información http://www.personeriacartagena.gov.co/webnew/index.php/transparencia/instrumentos-de-gestion-de-informacion-publica, el cual detalla cada uno de los activos de información de la entidad, por proceso, teniendo en cuenta la normatividad vigente y las recomendaciones del Modelo de Gestión de Riesgos de seguridad Digital. A continuación, se describe el formato de identificación de activos de información a detalle:

Información del proceso: Se identifica la información de proceso, procedimiento y/o formato al que está asociado el activo de información

Tipo Documental: Se identifican y se describen los activos de información (documentos de archivo o registros).

Tipo de soporte: Se especifican los medios en los cuales se contiene la información del activo de información.

Clasificación Documental: Se registra el nombre de la serie o subserie documental, a la cual pertenece el activo de información.

Clasificación y custodia de la información: Se identifica si la información del activo tiene datos personales, es información pública, clasificada o reservada, si requiere etiquetado y quien hace las veces de custodio y propietario de la información del mismo, así como el estado del activo.

Clasificación del Activo de información: Se indica si el activo de información es crítico tanto para las operaciones internas como externas.

Componentes de Seguridad de la Información: Se realiza la valoración de los activos de información identificados, teniendo en cuenta los principios de seguridad de la información, confidencialidad, integridad y disponibilidad, contemplando el impacto que causaría la pérdida de alguno de estos componentes.

Importancia del activo/Criticidad del Activo: Se calcula automáticamente, de acuerdo con los criterios seleccionados en la Confidencialidad, Integridad y Disponibilidad, teniendo en cuenta la siguiente tabla de valoración:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o más componentes (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta o media en al menos uno (1) de sus componentes
BAJA	Activos de información en los cuales la clasificación de la información en **todos** sus componentes es baja.

16.12 Identificación de Infraestructuras Críticas Cibernéticas (ICC):

Una vez realizada la identificación, clasificación y valoración de los activos de información, y determinada la importancia de estos para la entidad, la entidad identifica si cuenta con ICC o si alguno de los activos identificados corresponde a una ICC y verifica si su impacto o afectación supera alguno de los criterios siguientes:

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

Identificación de Infraestructuras Críticas Cibernéticas (ICC). Fuente: Modelo de Gestión de Riesgos de Seguridad Digital-MINTIC

Impacto Social: La variable de población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de la población va a estar asociada a las personas a las cuales se les presta servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectados por la materialización de algún riesgo en los activos identificados como ICC.

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

Impacto Ambiental: La variable ambiental estará alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Podría no ser utilizada en la mayoría de los casos

Nota. Si la entidad cuenta con ICC esta es reportada al CCOCI (Comando Conjunto Cibernetico)

ID ACTIVO	NOMBRE ACTIVO	NIVEL DE CRITICIDAD/ACTIVO	ICC			
			SOCIAL 250.000 personas	ECONOMICO	AMBIENTAL	SE DEBE REPORTAR CCOCI
Indicar Id del Activo	Indicar Nombre del Activo	Indicar Nivel de criticidad, definido en tabla de registro de activos	Indicar con x si hay afectación social	Indicar con x si hay afectación económica	Indicar con x si hay afectación ambiental	Indicar con x si se debe reportar a CCOCI

16.13 Identificación de los riesgos inherentes de seguridad digital

Para la identificación de los riesgos inherentes, la personería de cartagena tiene en cuenta las amenazas y vulnerabilidades asociadas a cada activo. Se pueden identificar entonces los siguientes 3 riesgos inherentes de seguridad digital:

- **Integridad**: se refiere a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros no autorizados.
- **Confidencialidad**: se refiere a cómo los datos se mantienen al acceso únicamente de las personas o sistemas que se encuentran autorizados.
- **Disponibilidad**: se refiere al acceso de la información en el momento que debe estar disponible; se aclara que la información de la entidad no debe estar disponible todo el tiempo durante el año.

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente se analizan las posibles amenazas y vulnerabilidades que podrían causar su materialización.

A continuación, se detallan algunas amenazas que pueden hacer daños a los activos y materializar los riesgos y algunas vulnerabilidades (debilidades) descritas en el anexo 4. Lineamientos para la GRSD y complementadas por la Guía De Gestión De Riesgos emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea para la Seguridad y privacidad de la información:

D= Deliberadas, A= Accidentales, E= Ambientales

Identificación de Amenazas:

Tipo	*Amenaza*	*Origen*
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A

Tipo	*Amenaza*	*Origen*
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D

Tipo	*Amenaza*	*Origen*
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

- Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Fuente de amenaza	*Motivación*	*Acciones amenazantes*
Pirata informático, intruso ilegal	• Reto • Ego • Rebelión • Estatus • Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	• Destrucción de la información • Divulgación ilegal de la información • Ganancia monetaria • Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	• Chantaje • Destrucción • Explotación • Venganza • Ganancia política • Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas,	• Ventaja competitiva	• Ventaja de defensa • Ventaja política

Fuente de amenaza	*Motivación*	*Acciones amenazantes*
gobiernos extranjeros, otros intereses)	• Espionaje económico	• Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad • Ego • Inteligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema

Fuente de amenaza	*Motivación*	*Acciones amenazantes*
		• Acceso no autorizado al sistema.

Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable

Tipo	Vulnerabilidades
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Nota: Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

De acuerdo con lo descrito en la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP, para la identificación del riesgo y el análisis de las posibles amenazas y vulnerabilidades que podrían causar la materialización del mismo, adopto la siguiente tabla:

Riesgo	Descripción del riesgo	Activo	Tipo de Activo	Amenaza	Vulnerabilidades	Consecuencia/ Impacto
Identificar el tipo de riesgo de acuerdo con la identificación	Detallar el riesgo	Asociar activo o grupo de activos según lo identificado en el		Detallar la amenaza a la cual está expuesta	Describir cuales son las vulnerabilidades asociadas a la amenaza identificada.	Describir las consecuencias que tendría el grupo de activos al verse afectado por la amenaza asociada.

establecida		formato de registro de activos de información		el grupo de activo		

16.14 Valoración del riesgo de seguridad digital:

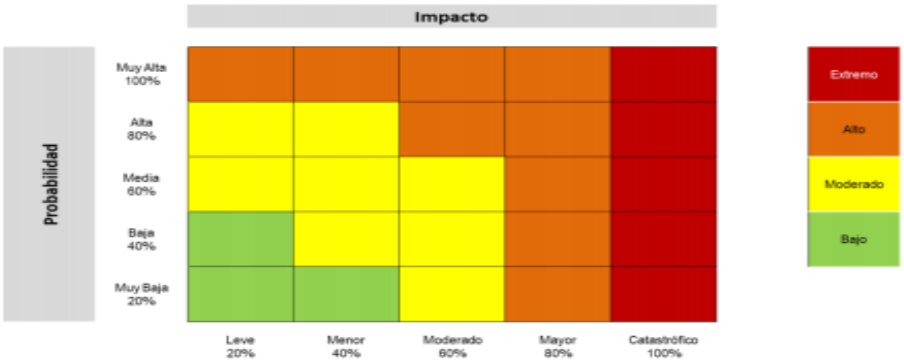
Una vez identificados los riesgos inherentes de seguridad digital para cada grupo de activos identificados, se determina la probabilidad e impacto de los criterios para lo cual se da uso de los criterios establecidos por el Modelo nacional de Gestión de riesgos de seguridad digital descritos a continuación:

	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%

Para determinar el impacto se debe llevar a cabo de acuerdo con lo establecido en lo anterior expuesto en el documento, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo. Por lo anterior 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



Definición de Apetito de Riesgo o Zona de Riesgo Aceptable Seguridad Digital

16.15 Definición de Apetito de Riesgo o Zona de Riesgo Aceptable Seguridad Digital

Si el nivel del riesgo inherente es **bajo**, el líder del proceso puede tomar la decisión de aceptar el riesgo y no será necesaria la implementación de una medida de

mitigación, en otras palabras, la entidad solo tendrá un nivel de tolerancia al riesgo **bajo**.

Por otro lado, si el nivel de riesgo inherente es mayor a **bajo**, obligatoriamente se debe implementar una medida de mitigación, ya sea **reducir el riesgo** (*implementar un control*), **evitar el riesgo** (*dejar de realizar la actividad con la cual está relacionada el riesgo*) o **compartir el riesgo** (*transfiriéndolo o compartiéndolo con un agente externo al proceso implementando un control*).

16.16 Controles asociados a la seguridad de la información

Para 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.

16.17 Tratamiento del riesgo del proceso Seguridad Digital

En esta etapa la primera línea de defensa (líderes de procesos) determinan, tomando en cuenta cual es el nivel del riesgo inherente, que acción es la más adecuada para su tratamiento, estas acciones pueden ser:

- **Aceptar el riesgo:** Se decide no aplicar ninguna acción que disminuya la probabilidad de ocurrencia o que atenué el impacto.
- **Reducir el riesgo:** Se toman acciones para disminuir la probabilidad y/o el impacto, esto se logra por medio de la implementación de controles.
- **Evitar el riesgo:** Se elimina la implementación de las actividades críticas que facilitan la materialización del riesgo.
- **Compartir el riesgo:** Se busca disminuir el impacto y/o la probabilidad del riesgo compartiéndolo con otro proceso de la entidad o con un actor tercero, por ejemplo, mediante una póliza de seguro con una compañía exógena a la entidad.

Si el líder del proceso decide que la acción de tratamiento al evento de riesgo será la de **reducir el riesgo** o **compartir el riesgo** se debe diseñar una actividad de control, la cual podrá ser diseñada por el líder operativo, pero deberá tener el aval del líder del proceso.

16.18 Identificación y evaluación de controles Seguridad Digital:

Para los casos en los cuales se determine Reducir el Riesgo o Compartir el riesgo se deben estructurar controles que cumplan con las características establecidas en el presente documento.

16.18.1 Tipos De Controles:

- **Control preventivo:** buscan evitar que el evento de riesgo se materialice (disminuyen la probabilidad) y están orientados a atacar las causas que facilitan la materialización del evento de riesgo:
- **Control detectivo:** buscan identificar la situación no deseada, una vez se haya presentado, y tiene por objetivo minimizar el impacto de la materialización del evento de riesgo, por eso este tipo de riesgo está encaminado a disminuir las consecuencias del riesgo.

Se propenderá estructurar un Control que permita dar cobertura de carácter preventivo y detectivo.

16.18.2 Características de un control adecuadamente estructurado

Para que un control este adecuadamente diseñado y que su implementación sea efectiva a la hora de mitigar un riesgo éste debe cumplir con los siguientes lineamientos:

- Debe tener un **responsable** de su ejecución (evitar colocar áreas generales o nombres propios), por ejemplo: responsable de inventarios.
- Cada causa del riesgo debe tener **por lo menos un control** asignado a su mitigación.
- La ejecución del control **debe tener un soporte documental**, por ejemplo, una base de datos, una lista de chequeo, un acta de reunión, etc.
- En la descripción del control se debe **especificar como se ejecuta** el control,
- En la definición del control se debe especificar cuál es la **periodicidad de la aplicación** de este; por ejemplo: el coordinador debe revisar (mensualmente, trimestralmente, cada vez que se presente…)
- La definición debe incluir **cual es el propósito** del control (valida, coteja, compara, concilia…)
- La definición del control debe incluir en que situaciones se presentan **desviaciones entre el resultado esperado y el resultado obtenido** y que acciones se deben tomar si se presentan dichas desviaciones.

16.19 Calificación del control

Una vez se haya estructurado el control se debe pasar a una etapa de calificación de su efectivad en la tarea de mitigar el riesgo, para esto se debe presentar una evaluación del control. Esta evaluación estará a cargo del encargado de la gestión del riesgo de la entidad y del líder operativo del proceso.

A continuación, se presentan los criterios para calificar la efectividad del control:

Criterio de evaluación.	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del Responsable.	Asignado	15
	No Asignado	0
1.2 Segregación y Autoridad del Responsable.	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un Control	0
4. Como se realiza la actividad de control.	Confiable	15
	No Confiable	0
5. Que pasa con las observaciones o desviaciones.	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente.	0
6. Evidencia de la ejecución del control.	Completa	10
	Incompleta	5
	No Existe	0

59

Ilustración 23 Criterios de calificación del diseño del control, tomado del DAFP

Se debe resaltar que no solo basta con que el control esté debidamente diseñado, sino también se tiene que velar por que su implementación sea la adecuada. Al momento de determinar si el control se ejecuta, inicialmente es una confirmación por parte del responsable del proceso, y posteriormente se confirma con las actividades de evaluación realizadas por Auditoría Interna o Control Interno.

De este modo se establecerá la calificación de la ejecución del control con base en la siguiente tabla:

Rango de Calificación de la Ejecución	Resultado - Peso de la Ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

60

Calificación de la ejecución del control, tomado del DAFP

Una vez se tienen las dos calificaciones se ponderan para dar la calificación de solidez individual que se especifica en la siguiente tabla para definir si se hace necesaria la aplicación de un plan de acción para fortalecer el control:

Peso del diseño individual o promedio de los Controles. (DISEÑO)	El Control se ejecuta de manera consistente por los responsables. (EJECUCION)	Solidez individual de cada control Fuerte:100 Moderado:50 Debil:0	Aplica plan de acción para fortalecer el Control Si / NO
Fuerte Calificación Entre 96 y 100	**Fuerte** (Siempre se ejecuta)	Fuerte + Fuerte = Fuerte	No
	Moderado (Algunas veces)	Fuerte + Moderado = Moderado	Si
	Débil (No se ejecuta)	Fuerte + Débil = Débil	Si
Moderado Calificación Entre 86 y 95	**Fuerte** (Siempre se ejecuta)	Moderado + Fuerte = Moderado	Si
	Moderado (Algunas veces)	Moderado + Moderado = Moderado	Si
	Débil (No se ejecuta)	Moderado + Débil = Débil	Si
Débil Entre 0 y 85	**Fuerte** (Siempre se ejecuta)	Débil + Fuerte = Débil	Si
	Moderado (Algunas veces)	Débil + Moderado = Débil	Si
	Débil (No se ejecuta)	Débil + Débil = Débil	Si

Calificación de solidez individual del control, Tomado del DAFP

Si hay más de un control que mitiga una causa estos dos se promedian para verificar cual es la solidez del promedio de los controles de la siguiente manera:

Calificación de la Solidez del conjunto de controles.	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación está entre 50 y 99
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación es menor a 50.

Calificación de solidez del promedio de los controles, Tomado del DAFP

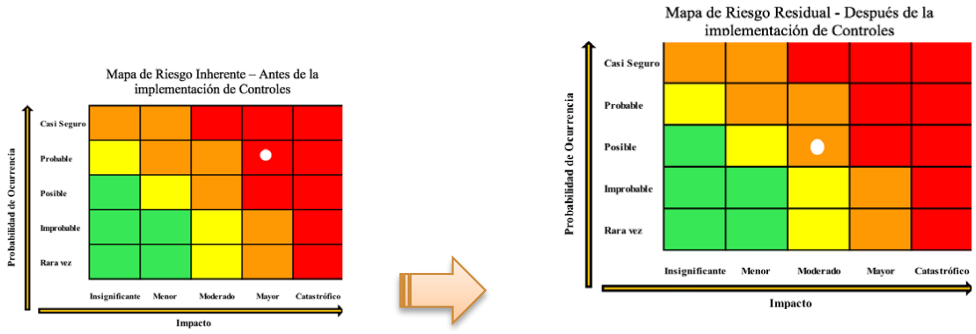
16.20 Nivel de riesgo residual

Una vez se tiene esta calificación de solidez del promedio de los controles se determina la lógica con la cual el nivel del riesgo residual se va a desplazar en el mapa de calor

Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.				
Solidez del conjunto de los controles.	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir Impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la Probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de Impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No Disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No Disminuye	1	0
Moderado	No disminuye	Directamente	0	1

Desplazamiento de riesgo inherente a riesgo residual, Tomado del DAFP

Con lo anterior se determina la posición del riesgo después de la ejecución del control considerando que los controles están correctamente diseñados y que efectivamente estos mitigan las causas que permiten que el riesgo se materialice. El desplazamiento en la gráfica debe ser similar a la siguiente.



Mapa de calor, Tomado del DAFP

Por lo anterior y para garantizar que el control elaborado se está efectuando, se hace necesario el seguimiento a la ejecución del mismo que debe ser correspondiente al periodo dado de cargue de evidencias dentro del control.

16.21 Mejora para la gestión del riesgo de seguridad digital

Mejora de la GRSD: Componente que tiene una orientación para establecer los mecanismos que permitan alcanzar un mayor grado de madurez de la GRSD en cualquier entidad.

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

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

19.21 Planes de Tratamiento de Riesgos de Seguridad de la información e Indicadores para la Gestión del Riesgo

Una vez se han identificado los riesgos, la entidad pública debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional. El tratamiento de los riesgos es un proceso cíclico, el cual involucra

una selección de opciones para modificarlos, por lo tanto, la entidad pública puede tener en cuenta las opciones planteadas en la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP: Evitar, aceptar, compartir o mitigar el riesgo.

Corresponde al proceso de modificar el riesgo. (ISO/IEC 27000:2018). Durante esta etapa se define que acciones se deben tomar para afectar el nivel de riesgo, bien sea atacando la probabilidad, el impacto o en su defecto las dos variables. Lo primero es determinar cuáles son los niveles de riesgo en que la entidad aplicará el tratamiento. Para ello, en el presente documento se definen los dos niveles de mayor probabilidad, impacto y valor de riesgo.

Aquí la **Línea Estratégica** debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (**Primer Línea de Defensa** y la **Oficina de Tecnologías de la Información -TI-** generalmente) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

Tabla 8. Nivel de tratamiento de riesgo

NIVELES DE RIESGO	RESPUESTA A LOS RIESGOS	DESCRIPCIÓN
ALTO	MITIGAR EL RIESGO, EVITAR, COMPARTIR	El nivel del riesgo es Alto, por lo que es necesario implementar controles en la entidad para mitigar, evitar o compartir el riesgo y llevarlo a niveles aceptables.
EXTREMO	MITIGAR EL RIESGO, EVITAR, COMPARTIR	El nivel del riesgo es Extremo, por lo que es necesario implementar controles en la entidad para mitigar, evitar o compartir el riesgo y llevarlo a niveles aceptables.

19.22 Monitoreo y revisión

La entidad pública a través de las **Tres Líneas de defensa** definidas en el MIPG en la Dimensión 7 Control Interno, Componente **Actividades de control**, debe hacer

un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad de la información para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

19.23 Registro y reporte de incidentes de seguridad de la información

La entidad debe realizar el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

19.24 Auditorías internas y externas

Le corresponde a las **Unidades de Control Interno (tercera línea de defensa)**, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad de la información en la entidad pública, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

19.25 Medición del desempeño

La entidad deberá utilizar medidas de desempeño (indicadores[1]) para la gestión de los riesgos de seguridad de la información, las cuales deben reflejar el cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente alineadas con la revisión por la línea estratégica.

19.26 Mejoramiento continuo de la gestión del riesgo de seguridad de la información

La personería distrital de Cartagena en su compromiso de mejora continua de la gestión de riesgos de seguridad de la información, establecerá cuando existan hallazgos, falencias o incidentes de seguridad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad de la información de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizados.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.