TABLA DE CONTENIDO

CAPITULO I
ASPECTOS GENERALES

INTRODUCCION

El presente documento establece los lineamientos para la identificación, análisis, valoración, evaluación , tratamiento, respuesta a los riesgos integrales de la Unidad que puedan afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales, tomando como referencia las directrices del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI, los requerimientos de la Guía para la administración del riesgo de FP, la Secretaria de Transparencia de la Presidencia de la República, el Ministerio de Tecnologías de la información y Comunicaciones, la Resolución 3783 de 2021 de la Unidad y las normas GNTC 45:2012, NTC 14001: 2015, NTC 27001: 2013

OBJETIVO

Establecer el marco general y lineamientos orientadores de actuación de todos los servidores públicos de la entidad bajo sus roles y responsabilidades de acuerdo con el esquema de las líneas de defensa, para la adecuada gestión integral de los riesgos, mediante la identificación, análisis, valoración, tratamiento y superación de las potenciales causas que se materialicen, generen siniestros o crisis, que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales.

ALCANCE

La metodología aplica para todos los procesos, dependencias y Direcciones Territoriales de la Unidad para la Atención y Reparación a las víctimas.

DEFINICIONES

Activo de información: Es la información que tiene valor para la organización y los elementos relacionados con la misma, como por ejemplo sistemas, elementos de hardware, personas e instalaciones.

Activo Crítico: Son activos de información que, debido a la criticidad dentro de un proceso, y que además al realizar el promedio en la calificación de los tres pilares de seguridad de la información: confidencialidad, integridad y disponibilidad, se localice entre una escala del 4 al 5 se categoría en activo crítico.

Amenaza: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).

Aspecto Ambiental: Elemento de las actividades, productos o servicios de una organización que puede interactuar con el medio ambiente.

Autocontrol: Capacidad que tiene una persona de evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública, comprende bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares.

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

Comité Manejo de Crisis: Analizar los hechos que originan la crisis y que por su complejidad y naturaleza requieren el análisis de la Alta Dirección para la toma decisiones

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

Contexto Interno: Hace referencia a los factores o condiciones del entorno interno, que pueden afectar el cumplimiento del objetivo de la Unidad.

Contexto Externo: Hace referencia a los factores o condiciones del entorno externo, que pueden afectar el cumplimiento del objetivo de la Unidad.

Control: Medida que permite reducir o mitigar 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

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

Efectividad de los controles: Medida de lo apropiado de un control, establecida bajo dos parámetros: su eficiencia y eficacia.

Efecto: Consecuencia que puede traer la ocurrencia del riesgo.

Eficacia de los controles: Medida de lo apropiado de un control establecida al determinar su contribución con el objetivo de este, es decir, con la disminución del riesgo.

Eficiencia de los controles: Medida del uso adecuado de los recursos en la aplicación de un control.

Evaluación de riesgos: proceso utilizado para determinar la magnitud de los riesgos en una organización, con relación a unos criterios determinados.

Evento: Suceso; particularmente suceso posible.

Factores de riesgo: Fuente generadora de los eventos de riesgo

Fraude: Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero

Gestión del riesgo: Es un proceso efectuado por la Dirección General y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Las consecuencias que puede ocasionar a la Entidad la materialización del riesgo

Impacto Ambiental: Cualquier cambio en el medio ambiente, ya sea adverso o beneficioso, como resultado total o parcial de los aspectos ambientales de una organización.

Información: Conjunto de datos organizados de manejo en la Unidad, que posee un valor para la misma.

Información Pública: Información que puede ser accedida sin restricciones por personal interno o externo a la Entidad y su publicación no representa ninguna consecuencia para la población, ministerio público, entes de control y para la Entidad.

Información Reservada: Corresponde a la información con restricción de acceso a la ciudadanía por daño a intereses públicos y bajo el cumplimiento de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

Información Clasificada: Corresponde a la información que solo puede ser accedida por personal autorizado y cuya divulgación no autorizada podría generar daños y perjuicios a la población víctima, a la Entidad y a sus funcionarios, contratistas y colaboradores.

Infraestructuras Críticas Cibernéticas -ICC: Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales". Fuente: Ministerio de Defensa.

Indicadores de riesgo: conjunto de variables cuantitativa y/o cuantitativas que se constituyen en herramientas para realizar el monitoreo de los riesgos.

Integridad: Propiedad de exactitud y completitud.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica.

Mapa de Riesgos: Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos. En este mapa se deberán incluir los riesgos identificados como posibles actos de corrupción, en cumplimiento del artículo 73 de la Ley 1474 de 2011.

Medidas de tratamiento: opciones contempladas para manejar o administrar un riesgo. Respuestas ante los riesgos.

MIPG: Modelo Integrado de Gestión y Planeación.

Monitoreo de riesgos: Evaluación permanente sobre la materialización de los riesgos.

Programa de Transparencia y Ética Pública: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Peligros de seguridad y salud en el trabajo: Fuente, situación o acto con un potencial de daño en términos de lesión o enfermedad o una combinación de estas.

Política de Administración de Riesgos: guía para la toma de decisiones o criterios de acción que rigen a todos los empleados con relación a la administración de riesgos. Trasmiten la posición de la Dirección respecto de su actitud ante los riesgos y fijan lineamientos para la protección de los recursos, conceptos de calificación de riesgos, prioridades en la respuesta y la forma de administrarlos.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo

Procedimiento: Método o sistema estructurado para ejecutar algunas cosas. Acto o serie de actos u operaciones con que se hace una cosa.

Proceso: Conjunto de actividades que realiza una organización, mediante la transformación de unos insumos, para crear, producir y entregar sus productos, de tal manera que satisfagan las necesidades de sus clientes.

Recurso público: Los dineros comprometidos y ejecutados en ejercicio de la función pública.

Reducir: medida de tratamiento de los riesgos que busca disminuir la posibilidad de ocurrencia de un riesgo, sus consecuencias o ambas.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo Ambiental: resultado de una función que relaciona la probabilidad de ocurrencia de un determinado escenario de accidente y las consecuencias negativas del mismo sobre el entorno natural, humano y socioeconómico.

Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo inherente: Nivel de riesgo propio de la actividad

Riesgos operativos: Posibilidad de incurrir en pérdidas por errores, fallas o deficiencias en el Talento Humano, Procesos, Tecnología. Infraestructura y Eventos Externos

Riesgo residual: El resultado de aplicar la efectividad de los controles al riesgo inherente

Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgos de emergencia, crisis y seguridad pública: Son riesgos asociados a aquellas amenazas que podrían afectar al personal, los activos u operaciones de la Unidad por la acción directa e indirecta de grupos armados, delincuencia común etc.

Riesgos de seguridad y salud en el trabajo: Combinación de la probabilidad de que ocurra una o más exposiciones o eventos peligrosos y la severidad del daño que puede ser causada por estos.

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de los objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales, incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Riesgo seguridad de la información: Hace referencia a la posibilidad de que una amenaza pueda explotar una vulnerabilidad de un activo de información, afectando la operación o la imagen de la Entidad.

Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).

Seguimiento: Es la observación minuciosa de la evolución y desarrollo de un proceso.

Valoración de riesgos: Es un Elemento del Componente Administración de Riesgos que comprende el conjunto de acciones por las cuales se estima la magnitud de los riesgos (frecuencia e impacto), y se evalúan para determinar si pueden aceptarse o no.

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

CAPITULO II
GESTION DEL RIESGO

La gestión del riesgo en todos los procesos y niveles (Nacional y Direcciones Territoriales) constituye un elemento estratégico dentro de la planeación de la Unidad para la Atención a las Víctimas, enfocado en el contexto externo e interno en el que se desarrollan sus actividades y la especialidad del servicio que presta a las víctimas en todo el territorio colombiano.

La adecuada gestión del riesgo en los procesos permite el logro de los objetivos institucionales, y también permite que la Unidad pueda monitorear y aplicar la acciones de mejora necesarias en su metodología y demás herramientas o mecanismos de administración del riesgo que faciliten el análisis de elementos tales como la probabilidad y el impacto de los riesgos, aplicación de controles y la evaluación de los mismos con el fin de prevenir, mitigar, controlar y superar los riesgos identificados.

Para ejercer una óptima gestión del riesgo es necesario contar con una metodología de administración de riesgos basada en el contexto general de la entidad para establecer su complejidad; marco estratégico, planeación institucional, mapa de proceso entre otros aspectos. Los aspectos mínimos por considerar son:

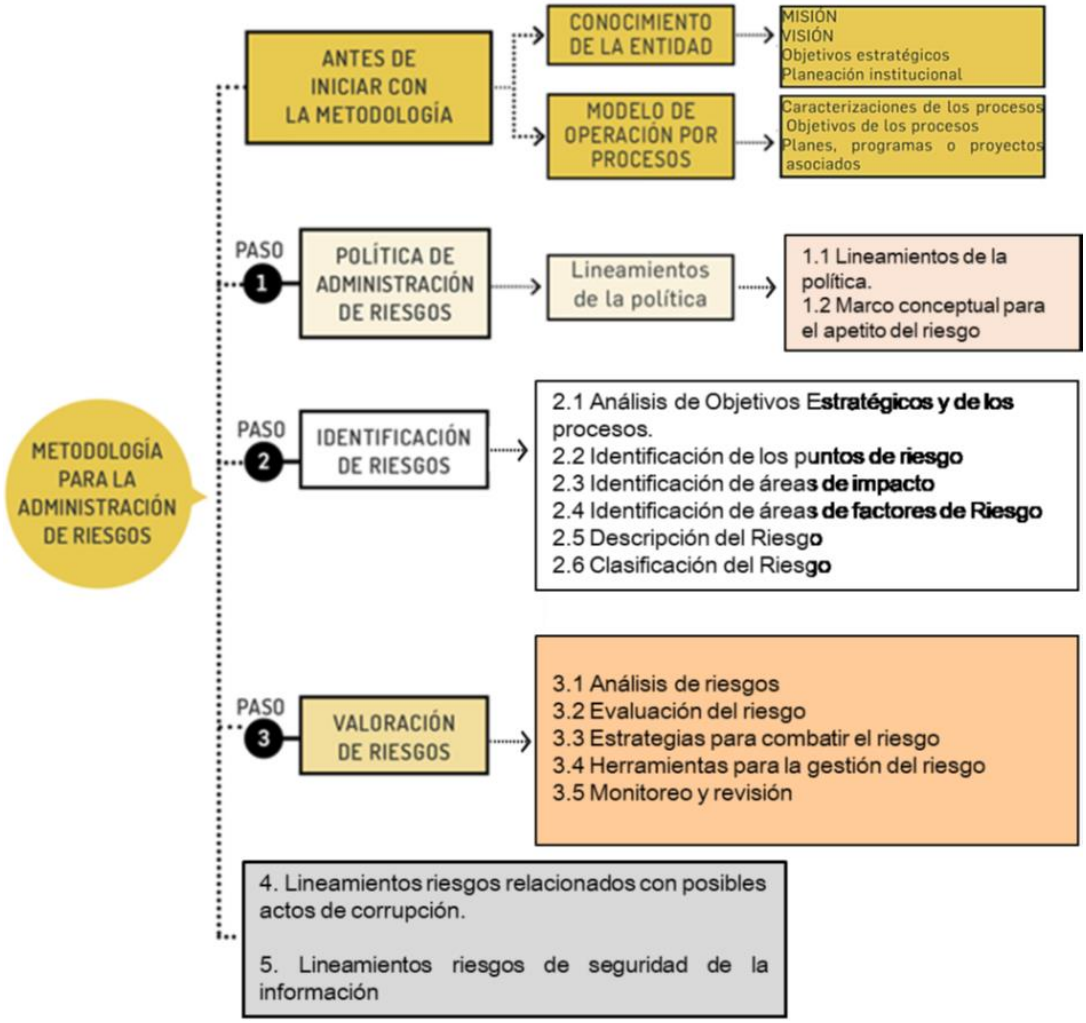
A. Marco metodológico

Este documento adopta los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública DAFP vigente, la cual integra las metodologías para la gestión de riesgos impartidos por el DAFP, la secretaria de Transparencia de la Presidencia de la Republica y el Ministerio de Tecnologías de la información y Comunicaciones.

Adicionalmente se tiene en cuenta las normas GTC 45:2012, NTC 14001: 2015, NTC 27001: 2013. Esta metodología cuenta con tres etapas para su desarrollo al interior de la entidad:

Para la identificación de los riesgos se parte del análisis de los objetivos y metas de la entidad, así como las actividades claves que se tiene que emprender para asegurar su cumplimiento; y a su vez determinar que eventos pueden afectar su cumplimiento y que acciones se pueden tomar para evitar o mitigar sus efectos (ver figura 1).

Figura 1. Metodología para la administración de riesgos

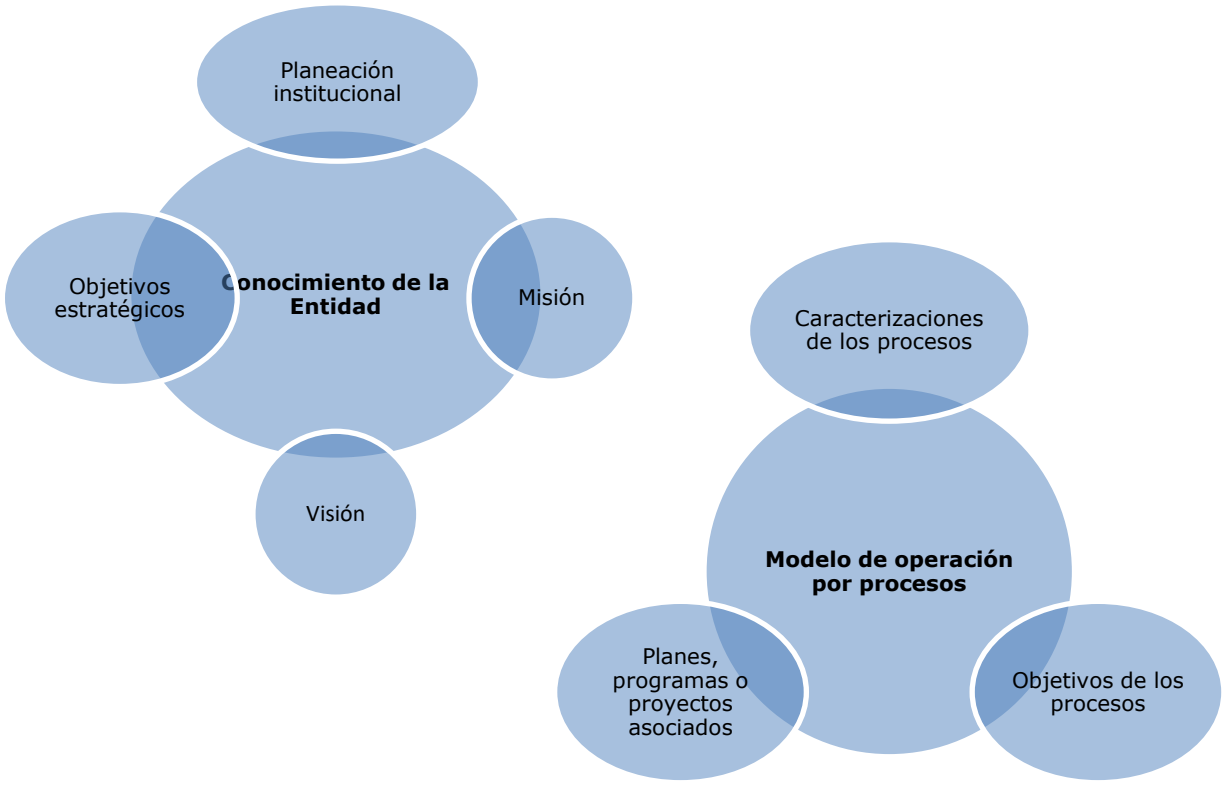


Fuente: Departamento Administrativo de la Función Pública

B. Conocimiento previo

Antes de iniciar la metodología, es preciso analizar el contexto general de la Entidad, para establecer su complejidad, procesos, planeación institucional, permitiendo conocer y entender la Entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la Metodología en general (ver figura 2).

Figura 2. Factores de conocimiento y análisis de la Entidad



Fuente: Departamento Administrativo de la Función Pública

Estos aspectos son fundamentales como punto de partida para determinar los riesgos y la implementación de la metodología en general.

Para mayor profundización con respecto a este conocimiento previo al interior de la Unidad pueden remitirse al Plan Indicativo

https://www.unidadvictimas.gov.co/es/plan-indicativo-estrategico-2023-2026/75481

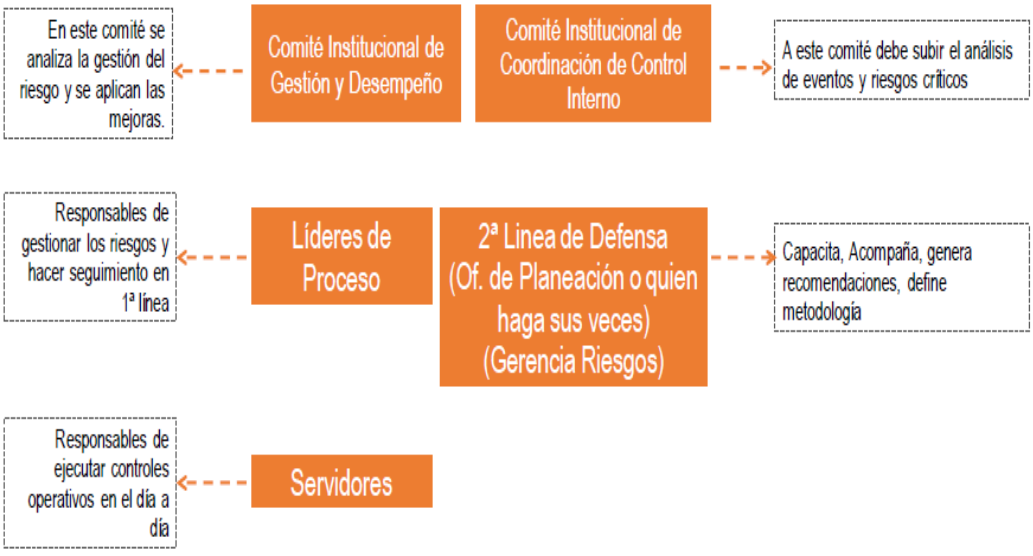
y al Manual del Sistema Integrado de Gestión SIG

https://www.unidadvictimas.gov.co/es/NODE/76622

2.1. GESTIÓN DEL RIESGO EN EL MARCO DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN – MIPG

Dentro de la metodología de administración del riesgo, se encuentran definidos para su operación articulada con el modelo integrado de planeación y gestión (MIPG), la creación del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, como un instrumento para la eficiente y adecuada gestión del riesgo, lo que permite establecer la institucionalidad de la Unidad en materia de riesgo de la siguiente manera (ver figura 3):

Figura 3. Operatividad Institucionalidad para la Administración del Riesgo



Fuente: Departamento Administrativo de la Función Pública

2.2. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Unidad para las Victimas desde la línea estratégica de defensa ha establecido la siguiente política:

"La Unidad administra integralmente los riesgos que pueden afectar el cumplimiento de sus objetivos estratégicos, trabajando para la reparación integral de las víctimas y la implementación de la ley 1448 del 2011, a fin de aumentar su eficacia y eficiencia a través de la identificación, análisis y valoración de riesgos que permita tomar acciones para evitar su materialización".

2.2.1. Objetivo

El objetivo principal es crear una cultura de prevención y control frente a la gestión del riesgo, que contribuya al cumplimiento de los objetivos de la Unidad y contribuyan a la lucha contra la corrupción, mitigación de los riesgos institucionales y la superación de los eventos que generen crisis que afecten la imagen y el funcionamiento de la Unidad.

Los objetivos específicos son:

- Generar conciencia sobre la necesidad de identificar y darle tratamiento a todos los riesgos institucionales de la Unidad
- Comprometer e involucrar a todos los servidores de la Unidad en la implementación de acciones encaminadas a evitar y mitigar los riesgos institucionales de la Unidad
- Prevenir o mitigar cualquier pérdida de recursos que pueda generar la materialización de los riesgos y la ocurrencia de crisis
- Prevenir de manera permanente la ocurrencia de riesgos de corrupción
- Prevenir la materialización de accidentes y enfermedades que pueden causar lesiones, daños serios o muerte a los funcionarios y colaboradores de la Unidad
- Buscar la mejora continua y suministrar insumos para la toma de decisiones de

la Entidad.

- Prevenir la materialización de un impacto ambiental negativo sobre el medio ambiente a causa del desarrollo de actividades propias de la entidad

- Fomentar en los procesos de la Entidad, la gestión de riesgos de seguridad de la información y seguridad digital, con base en los activos críticos previamente identificados y las acciones para tratar el riesgo.

- Realizar la gestión de riesgos de seguridad de la información, a través de una metodología medible y repetible, que permita la documentación de los controles de seguridad existentes y la definición del plan de tratamiento de los riesgos identificados, para el fortalecimiento de la protección de la información de la población víctima del conflicto en Colombia, en cumplimiento de la normatividad vigente.

- Realizar una eficiente gestión de riesgos de seguridad pública, con el fin de fortalecer los mecanismos de prevención y mitigación de los hechos que puedan generar crisis.

- Prevenir el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado

2.2.2 Alcance

La política de administración de riesgos aplica a todos los procesos y Direcciones Territoriales de la Unidad para la Atención y Reparación a las Víctimas.

2.2.3 Apetito del riesgo

Dentro de los lineamientos señalados por la Línea Estratégica se establece que dentro de la política de administración del riesgo se considere el siguiente aspecto:

Nivel de Aceptación del 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 este sentido, la Unidad para la Atención y Reparación Integral a las Víctimas ha establecido que todos los riesgos que se ubiquen en un nivel de severidad residual **BAJO** se aplica el nivel de aceptación, ya que los controles son suficientes y se determina **ASUMIR** el mismo conociendo los efectos de su posible materialización, exceptuando los riesgos de corrupción, no obstante, por lo anterior los riesgos no son eliminados del mapa de riesgos y se debe continuar con el seguimiento establecido en el presente documento por parte de los líderes de proceso.

2.2.4 Niveles para calificar probabilidad e impacto: es la calificación que se tiene establecida en las tablas que contienen los criterios de calificación (Probabilidad – Exposición al riesgo) e Impacto (Económica o Presupuestal y Reputacional) en las cuales podemos encontrar 5 niveles con una escala porcentual para su calificación, de acuerdo con lo señalado en los numerales 2.4.2 y 2.4.3 respectivamente de este documento.

2.2.5 Tratamiento del riesgo: es la capacidad de tomar decisiones frente a un determinado nivel de riesgo, con el fin de Aceptar, Reducir o Evitar un riesgo con el fin de analizarlo frente al riesgo residual, para el caso de procesos en funcionamiento, y cuando se trate de procesos nuevos, se procede a partir del riesgo inherente, de acuerdo con lo señalado en el numeral 2.5 de este documento.

2.2.6 Periodicidad y responsabilidad frente al seguimiento, revisión y actualización del mapa de riesgos

El seguimiento del mapa de riesgos institucional (controles y plan de acción) lo realiza los procesos o direcciones territoriales a través de sus respectivos líderes y enlaces en la periodicidad establecida en el apartado 2.5 de este documento. Adicionalmente, para el caso de los Riesgos de Corrupción la oficina de Control Interno realiza un seguimiento con una periodicidad cuatrimestral con corte a 30 de abril, 31 de agosto y 31 de diciembre de la vigencia correspondiente.

El líder o delegado de riesgos en cada proceso analizan los resultados del seguimiento y pueden determinar establecer un plan de mejoramiento ante cualquier desviación y socializa al interior de su dependencia las acciones a seguir.

La revisión y actualización de los mapas de riesgos se validan mínimo una (1) en cada vigencia atendiendo la metodología vigente y de manera puntual ante cualquier modificación del proceso, estructura organizacional, objetivos estratégicos, modificación de controles derivados del seguimiento o de los eventos (materialización del riesgo).

2.3 IDENTIFICACIÓN DE RIESGOS

Tiene como propósito identificar los riesgos que estén bajo el control de la Unidad, teniendo en cuenta el contexto estratégico en el que opera y la caracterización de cada proceso que contempla su objetivo y alcance que pueden generar riesgos que afecten el cumplimiento de los objetivos institucionales.

El objetivo de esta identificación que le corresponde a la primera línea de defensa consiste en generar un listado de los riesgos de los procesos y direcciones territoriales, basado en hechos o circunstancias que hayan afectado la consecución de los objetivos de la entidad.

Inicia con la identificación de las actividades claves y eventos que más impacto pueden generar en el cumplimiento de los objetivos de la Entidad, partiendo de los pasos que se citan en las Tablas 1 y 2.

Las fuentes de información que deben tenerse en cuenta para la identificación de riesgos son:

- Análisis de contexto
- Informes y hallazgos de Auditoria (Interna, externa, de Gestión etc.)
- Recomendaciones de entes de control y planes de mejoramiento
- Tramites y servicios de cara a la ciudadanía
- Proceso y procedimientos que impliquen manejo de recursos sobre los cuales se tenga injerencia (contratos, recurso humano, dinero, bienes, títulos valores etc.)
- Matriz de Identificación de Peligros, Valoración del Riesgo y Determinación de Controles
- Documento de identificación de activos de información (Activos críticos)

- Matriz de identificación y evaluación de aspectos e impactos ambientales

Tabla 1. Pasos identificación del riesgo

Paso 1. Identificación del objetivo proceso	**Paso 2.** Identificación Actividades Claves	**Paso 3.** Identificación áreas de impacto	**Paso 4.** Identificación factores de riesgos (ver tabla 2)	**Paso 5.** Descripción del riesgo
Todos los riesgos que se identifiquen deben tener impacto en el cumplimiento de este objetivo.	Son actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios que pueden ocurrir eventos de riesgo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.	Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo	Recurso Humano Procesos Infraestructura Tecnología Eventos Externos	Debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento para personas ajenas al proceso No describir como riesgos omisiones ni desviaciones del control No describir causas como riesgos operativos No describir riesgos como la negación de un control.

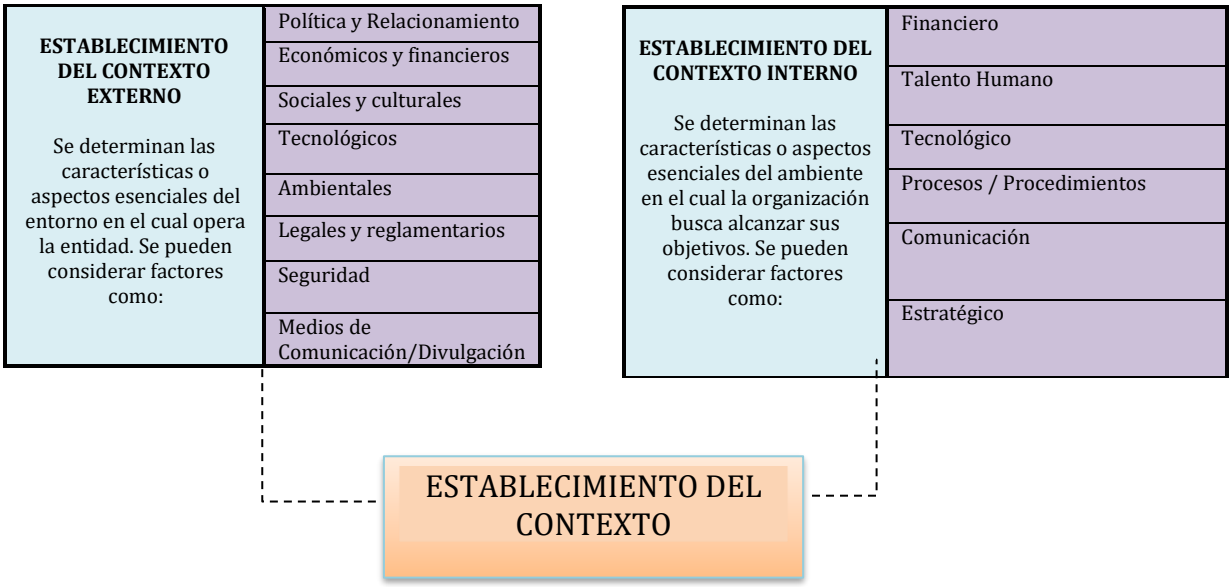
Tabla 2. Tipología, Factores y Clasificación del riesgo

Tipologías	Factores de Riesgo		Clasificación			
Gestión **Corrupción** **Seguridad de la Información/Digital** **Ambiental** **Seguridad y Salud en el Trabajo** **Emergencias. Crisis, Seguridad de las personas** **Documental** **Fiscales**	**Talento Humano**	Se analiza posible dolo e intención frente a la corrupción	**Fraude Interno (Corrupción)**	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.	**Grupos de Valor, Productos o servicios y prácticas de la Entidad** Fallas negligentes o involuntarias de las obligaciones frente a los Grupos de Valor y que impiden satisfacer una obligación profesional frente a estos	**Relaciones Laborales** Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleos, salud o seguridad, del pago de demandas por daños personales o de discriminación
			Daño antijurídico	Falencia administrativa que ocasiona litigiosidad y puede ser tanto una acción como una omisión de la Entidad en desarrollo de sus actividades		
			Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado		
	Eventos Externos	Situaciones externas que afectan la entidad	**Fraude Externo**	Pérdidas debidas a actos de fraude, apropiación indebida o incumplimiento de leyes por un externo		
	Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	**Ejecución y administración de procesos**	Pérdidas derivadas de errores en la ejecución y administración de los procesos		
	Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	**Fallas tecnológicas**	Pérdidas derivadas por fallas en hardware software, telecomunicaciones o interrupción en los servicios básicos		
	Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	**Daños a activos físicos**	Pérdidas por daños o extravíos de los activos físicos por desastres naturales y otros eventos		

2.3.1 Establecimiento del contexto

Comprende el análisis de los factores internos y externos que pueden afectar el proceso y que deben ser tenidos en cuenta para establecer las causas de los riesgos, para cual se debe tener en cuenta (ver figura 4):

Figura 4. Establecimiento del contexto



Para el desarrollo de este ejercicio la Unidad ha establecido la "Guía para la construcción contexto estratégico" la cual se encuentra en https://www.unidadvictimas.gov.co/es/NODE/41809

2.3.2 Identificación de Causas

Identificados los factores tanto internos como externos, se podrán determinar las causas, es decir los elementos o hechos que tienen la capacidad de originar un riesgo.

Una buena fuente de identificación de causas se contempla en el análisis DOFA (Debilidades y Amenazas) realizado en el contexto institucional

En la matriz de riesgo cada causa debe tener asociado un control, y en el caso de no contar con un control, se deberá proponer en el plan de tratamiento una actividad que de alguna manera apunte a controlar esa causa.

Ejemplos de Causas:

1. Falta de recursos para realizar las actividades
2. Ausencia de controles al interior del proceso
3. Exceso de actividades frente al personal disponible
4. Insuficiencia de los canales de comunicación
5. Desactualización en temas normativos
6. Desconocimiento de los procedimientos
7. Demora en la contratación del Operador
8. Falta de voluntad y cumplimiento de compromisos por parte de los entes territoriales
9. Deficiencia en los canales de comunicación internos
10. Falta de articulación de los procesos
11. Falta de lineamientos para la realización de las actividades

2.3.3 Identificación de Impactos

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:

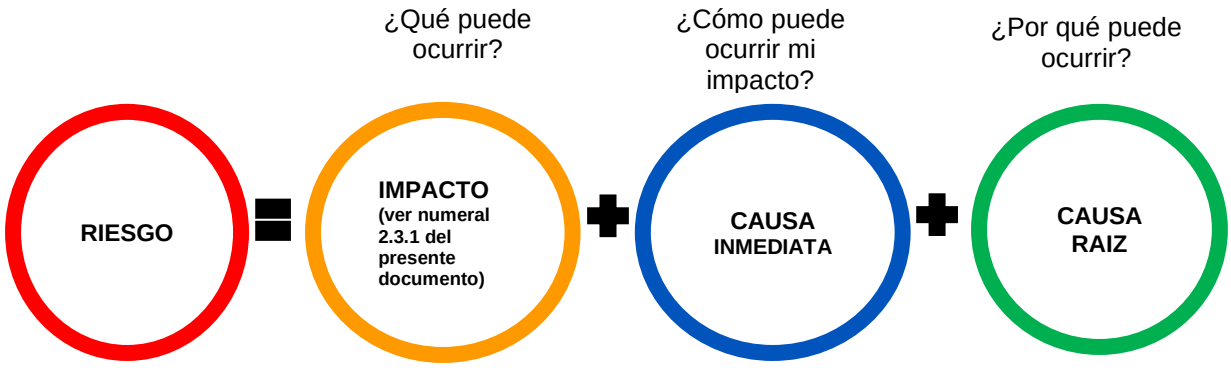
- Económicos
- Reputacionales
- Económicos y Reputacionales
- Efecto dañoso sobre bienes, recursos públicos e intereses patrimoniales de naturaleza pública
- Confidencialidad
- Disponibilidad
- Integridad

2.3.4 Descripción del riesgo

Inicia con la frase **POSIBILIDAD DE** y se analizan los siguientes aspectos dependiendo la clasificación del riesgo:

2.3.4.1 Estructura de redacción riesgos Gestión /Seguridad y Salud en el Trabajo/Ambientales/Emergencia, crisis y seguridad pública/Documental/Fiscal (ver figura5)

Figura 5. Estructura redacción riesgos



Objetivo del Proceso: Coordinar, administrar, controlar y hacer seguimiento al registro de las operaciones relacionadas con la ejecución del presupuesto, para el cumplimiento normativo del resultado del ejercicio financiero y contable.

Ejemplo:

Riesgo: Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

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 (es la forma como se puede visualizar la materialización del riesgo).

Causa raíz: Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que deben ser analizadas y controladas.

2.3.4.2 Estructura de redacción riesgos de corrupción

Es necesario que en la descripción del riesgo de corrupción concurran los componentes de su definición (ver figura 6):

Figura 6. Estructura redacción riesgos corrupción

Ejemplo:

Riesgo: Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

A manera de ilustración se señalan algunas situaciones causantes de riesgos de corrupción:

Direccionamiento estratégico (alta dirección).

- Concentración de autoridad o exceso de poder
- Extralimitación de funciones
- Ausencia de canales de comunicación

Financiero (está relacionado con áreas de planeación y Presupuesto)

- Inclusión de gastos no autorizados.
- Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración.
- Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.
- Inexistencia de archivos contables.
- Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.

De contratación (como proceso o procedimientos vinculados a este)

- Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. Estableciendo necesidades inexistentes o aspectos para beneficio de un tercero
- Direccionamiento en los pliegos de condiciones para beneficio de un grupo en particular. (Ej. media geométrica)
- Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación y violatorias de la norma
- Adendas que modifican sustancialmente las condiciones iniciales del proceso para favorecer a terceros
- Mala utilización de las modalidades de selección con el fin de favorecer a terceros
- Urgencia manifiesta sin la debida motivación y fundamentación
- Concentrar las labores de supervisión en poco personal
- Inadecuada selección objetiva
- Establecer requisitos habilitantes y factores de selección subjetivos y no coherentes con el objeto del proceso.

De información y documentación

- Ausencia o debilidad de medidas y/o políticas de conflictos de interés
- Concentración de información de determinadas actividades o procesos en una persona
- Ausencia de sistemas de información
- Ocultar la información considerada pública para los usuarios
- Ausencia o debilidad de canales de comunicación
- Incumplimiento de la Ley 1712 de 2014.

De investigación y sanción

- Ausencia o debilidad de canales de comunicación
- Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este
- Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación
- Exceder las facultades legales en los fallos

De trámites y/o servicios internos y externos

- Cobros asociados al trámite
- Influencia de tramitadores
- Tráfico de influencias: (amiguismo, persona influyente)
- Demorar su realización

De reconocimiento de un derecho (expedición de licencias y/o permisos)

- Falta de procedimientos claros para el trámite
- Imposibilitar el otorgamiento de una licencia o permiso
- Ofrecer beneficios económicos para aligerar la expedición o para amañar la misma
- Tráfico de influencias: (amiguismo, persona influyente)

2.3.4.2.1 Lineamientos para la identificación del riesgo de corrupción

Con el fin de realizar una adecuada identificación de los riesgos de corrupción se debe tener en cuenta los siguientes interrogantes: Las preguntas clave para la identificación del riesgo son:

¿Qué puede suceder?

¿Cómo puede suceder?

¿Cuándo puede suceder?

¿Qué consecuencias tendría su materialización?

2.3.4.2.2 Impacto riesgo de corrupción

Para la calificación del impacto de los riesgos de corrupción se debe utilizar la tabla No. 7, numeral 2.4.3.1 de este documento

2.3.4.3 Estructura de redacción riesgos de seguridad información / digital

Los riesgos de seguridad de la información se basan en la afectación de los tres pilares de seguridad de la información que son fundamentales en la identificación de los activos de información del proceso:

Los 3 pilares de la información "Integridad, confidencialidad o disponibilidad"

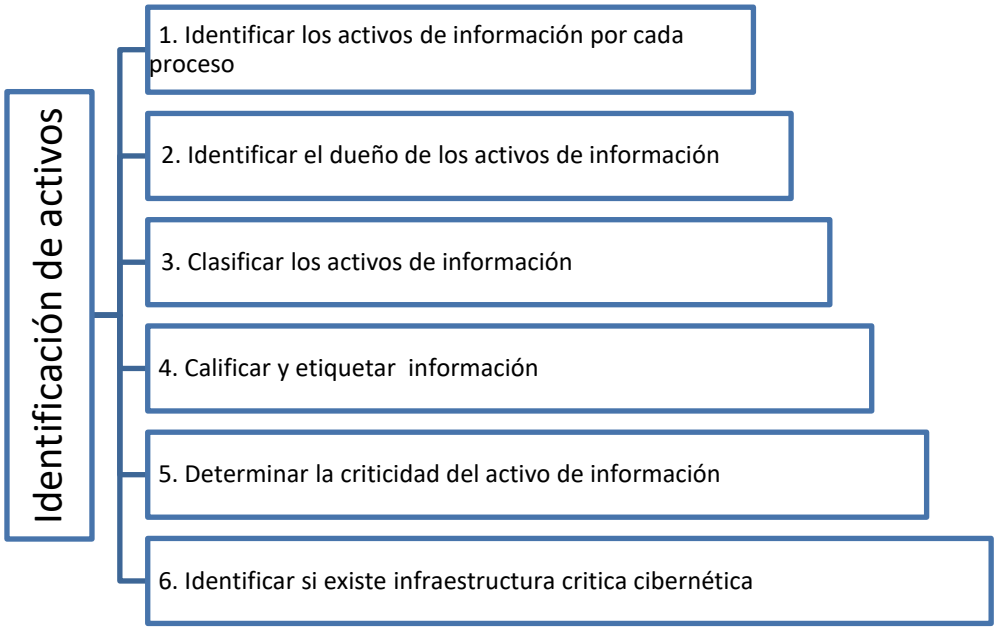
De acuerdo con la guía de administración de riesgo del DAFP, solo se pueden identificar los siguientes tres riesgos de seguridad:

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

Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

Para el riesgo identificado se deben asociar el grupo de activos de información o activos de información específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización (ver figura 7)

Figura 7. Identificación de activos



Ejemplo:

Riesgo: Posibilidad de pérdida reputacional por modificación no autorizada de la base de datos de nómina debido a la falta de políticas de control de acceso.

A continuación, se listan los ejemplos de vulnerabilidades y amenazas que pueden explotar las vulnerabilidades, según la norma ISO/IEC 27005:2008 (ver Tabla 3):

Tabla 3. Ejemplos Amenazas y vulnerabilidades

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
1	Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
2		Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	
3		Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	
4		Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	
5		Ausencia de auditorías (supervisiones) regulares	
6		Ausencia de procedimientos de identificación y valoración de riesgos	
7		Ausencia de reportes de fallas en los registros de administradores y operadores	
8		Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
9		Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	
10		Ausencia de procedimiento de control de cambios	
11		Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
12		Ausencia de procedimiento formal para la supervisión del registro del SGSI	
13		Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
14	Organización	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
15		Ausencia de planes de continuidad	Falla del equipo
16		Ausencia de políticas sobre el uso del correo electrónico	
17		Ausencia de procedimientos para la introducción del software en los sistemas operativos	
18		Ausencia de registros en las bitácoras (logs) de administrador y operario	
19		Ausencia de procedimientos para el manejo de información clasificada	
20		Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	
21		Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
22		Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
23		Ausencia de política formal sobre la utilización de computadores portátiles	
24		Ausencia de control de los activos que se encuentran fuera de las instalaciones	
25		Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
26		Ausencia de autorización de los recursos de procesamiento de la información	
27		Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	
28		Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
29		Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	
30		Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
31	Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
32		Ubicación en un área susceptible de inundación	Inundación
33		Red energética inestable	Pérdida del suministro de energía
34		Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
35	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
36		Procedimientos inadecuados de contratación	Destrucción de equipos o medios
37		Entrenamiento insuficiente en seguridad	Error en el uso
38		Uso incorrecto de software y hardware	
39		Falta de conciencia acerca de la seguridad	
40		Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
41		Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
42		Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
43	Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
44		Líneas de comunicación sin protección	Escucha encubierta
45		Tráfico sensible sin protección	
46		Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
47		Punto único de falla	
48		Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos

Tipo / Área	Ejemplos de vulnerabilidades		Ejemplos de amenazas
49	Red	Arquitectura insegura de la red	Espionaje remoto
50		Transferencia de contraseñas en claro	
51		Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
52	Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
53		Defectos bien conocidos en el software	
54		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	
55		Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	
56		Ausencia de pistas de auditoria	
57		Asignación errada de los derechos de acceso	
58		Software ampliamente distribuido	Corrupción de datos
59		En términos de tiempo utilización de datos errados en los programas de aplicación	
60		Interfaz de usuario compleja	Error en el uso
61		Ausencia de documentación	
62		Configuración incorrecta de parámetros	
63		Fechas incorrectas	
64		Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
65		Tablas de contraseñas sin protección	
66		Gestión deficiente de las contraseñas	

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
67	Software	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
68		Software nuevo o inmaduro	Mal funcionamiento del software
69		Especificaciones incompletas o no claras para los desarrolladores	
70		Ausencia de control de cambios eficaz	
71		Descarga y usos no controlados de software	Manipulación con software
72		Ausencia de copias de respaldo	
73		Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
74		Falla en la producción de informes de gestión	Uso no autorizado del equipo
75	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
76		Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o de medios.
77		Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
78		Sensibilidad a la radiación electromagnética	Radiación electromagnética
79		Ausencia de un eficiente control de cambios en la configuración	Error en el uso
80		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
81		Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
82		Almacenamiento sin protección	Hurto de medios o documentos
83		Falta de cuidado en la disposición final	
84		Copia no controlada	

2.3.4.4 Criterios de operación:

Los riesgos de seguridad de información son asociados a los activos críticos de información definidos y categorizados por cada proceso de la entidad con base al procedimiento de Generación de Inventario de Activos de Información, y sus documentos de alcance.

https://www.unidadvictimas.gov.co/es/NODE/53086

La calificación de acuerdo al impacto de los tres pilares de Seguridad de la Información, Confidencialidad, Integridad y Disponibilidad lo realiza el dueño del activo de información, sin embargo, el Sistema de gestión de seguridad de la Información realiza revisión sobre esta actividad, de esta manera se asegura la correcta identificación de los posibles activos críticos.

Los activos críticos son activos de información que, debido a la criticidad dentro de un proceso, y que además al realizar el promedio en la calificación de los tres pilares de seguridad de la información: confidencialidad, integridad y disponibilidad, se localice entre una escala del 4 al 5 se categoría en activo crítico y son posibles candidatos para asociar riesgos de seguridad de la información.

2.4 VALORACIÓN DE RIESGOS

La valoración del riesgo consiste en establecer la probabilidad de que ocurra el riesgo y su nivel de impacto, con el fin de determinar la zona de riesgo inicial (Riesgo Inherente); y se confronta los resultados del análisis de riesgos inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo residual).

2.4.1 Análisis del riesgo

En este punto se busca establecer la probabilidad de acuerdo a la exposición del riesgo y sus consecuencias o impactos. La Unidad establece la probabilidad de ocurrencia de sus riesgos y sus consecuencias o impactos a través de las tablas 4 y 5, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

2.4.2 Determinar la probabilidad

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 es el número de veces que se pasa por el punto de riesgo en el periodo de 1 año (ver tabla 4)

Tabla 4. Criterios calificación probabilidad

PROBABILIDAD		
Nivel	**Probabilidad**	**Descripción**
100%	**Muy Alta**	La actividad se realiza más de 3000 veces al año
80%	**Alta**	La actividad se realiza entre 1501 a 3000 veces al año
60%	**Media**	La actividad se realiza entre 366 y 1500 veces al año
40%	**Baja**	La actividad se realiza entre 13 y 365 veces al año
20%	**Muy Baja**	La actividad se realiza máximo 12 veces por año

Nota: Esta tabla es aplicable a todos los tipos de riesgos institucionales, excepto riesgos de corrupción, ver ítem 2.4.2.1

2.4.2.1 Determinación Probabilidad Riesgos de Corrupción

PROBABILIDAD			
Nivel	**Probabilidad**	**Descripción**	**Frecuencia**
100%	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de una (1) vez al año
80%	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos una (1) a vez en el último año
60%	**Posible**	El evento podrá ocurrir en algún momento	Al menos una (1) a vez en los últimos dos (2) años
40%	**Improbable**	El evento podrá ocurrir en algún momento	Al menos una (1) a vez en los últimos cinco (5) años
20%	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos cinco (5) años

2.4.3 Determinar el impacto

El impacto está asociado a la consecuencia económica y/o reputacional que se genera por la materialización del riesgo (ver tabla 5)

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

Tabla 5. Criterios calificación impacto

IMPACTO			
Nivel	**Impacto**	**Descripción Económica o Presupuestal**	**Descripción Reputacional**
100%	**Catastrófico**	Pérdida económica superior a 1500 SMLMV	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional
80%	**Mayor**	Pérdida económica de 319 hasta 1500 SMLMV	Deterioro de imagen con efecto publicitario sostenido a nivel Territorial
60%	**Moderado**	Pérdida económica de 21 hasta 318 SMLMV	Deterioro de imagen con efecto publicitario a nivel Local o Sectores Administrativos
40%	**Menor**	Pérdida económica de 11 hasta 20 SMLMV	De conocimiento general de la entidad a nivel interno, Dirección General, Comités Y Proveedores
20%	**Leve**	Pérdida económica hasta 10 SMLMV	Solo de conocimiento de algunos funcionarios

Nota: Esta tabla es aplicable a todos los tipos de riesgos institucionales, excepto riesgos de corrupción.

2.4.3.1 Determinar el impacto riesgos de corrupción

El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines de la Entidad. Para facilitar la asignación del puntaje es aconsejable diligenciar la siguiente tabla 6.

Tabla 6. Criterios calificación impacto riesgos de corrupción

N	Pregunta Si el riesgo se materializa podria?	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia ?		
3	¿Afectar el cumplimiento de misión de la Entidad ?		
4	¿Afectar el cumplimiento de misión del sector al cual pertenece la Entidad ?		
5	¿Generar perdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar perdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la perdida del bien o servicios o los recursos públicos?		
9	¿Generar perdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar perdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o perdida de vidas humanas ?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

De acuerdo con el número de respuestas afirmativas se determina el nivel de impacto tomando como referencia la tabla 7.

Tabla 7. Nivel impacto riesgos de corrupción

Impacto	Descripción	Nivel	Respuestas Afirmativas
Moderado	Afectación parcial al proceso y a la dependencia Genera medianas consecuencias para la entidad.	60%	1 – 5
Mayor	Impacto negativo de la Entidad Genera altas consecuencias para la entidad.	80%	6 - 11
Catastrófico	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad.	100%	12 - 19

2.4.4 Evaluación del riesgo

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

2.4.4.1 Análisis preliminar (riesgo inherente)

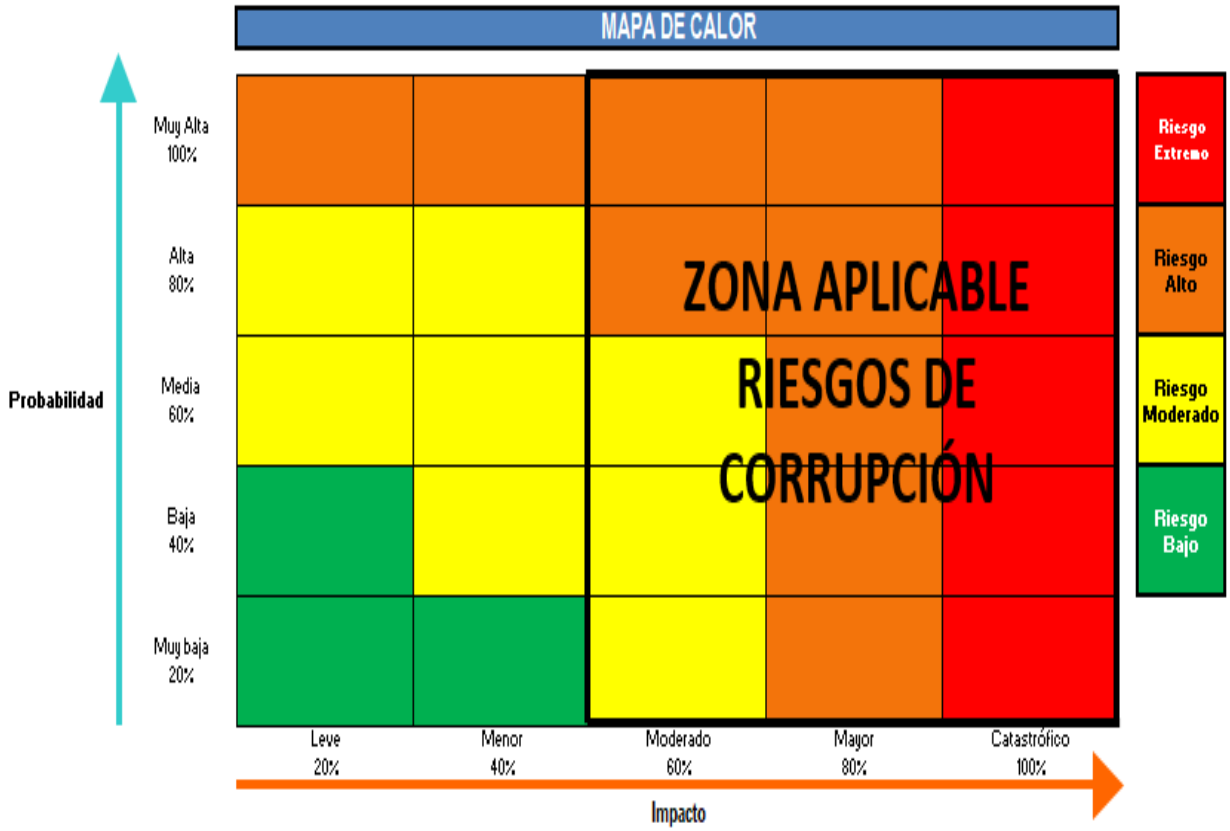
Para estimar el nivel de riesgo inicial o inherente, se cruzan los datos de probabilidad e impacto definidos. Este primer análisis del riesgo se denomina Riesgo Inherente y se define como aquél al que se enfrenta una entidad en ausencia de controles.

El mapa de calor de la Unidad cuenta con 5 niveles de probabilidad y 5 niveles de impacto. Sin embargo, para los riesgos de corrupción el análisis de impacto se realiza teniendo en cuenta solamente tres niveles de impacto "moderado", "Mayor" y "Catastrófico", dado que estos riesgos siempre serán significativos y su impacto no puede catalogarse como menor o insignificante (ver figura 8).

2.4.4.2 Valoración de Controles

Un control se define como la medida que permite reducir o mitigar el riesgo, la identificación de controles se debe realizar para cada riesgo a través de las entrevistas con los funcionarios expertos.

Figura 8. Matriz de Calor riesgos institucionales



- Los responsables de implementar y monitorear los controles son los líderes de proceso.

- Debe diseñarse un control para cada causa. En caso de que la causa no tenga control debe proponerse un Plan de tratamiento que permita mitigar esa causa (sin importar la zona de riesgo residual).

2.4.4.2.1 Estructura para la descripción del control

La descripción del control debe mínimo contener los siguientes elementos (ver figura 9).

Figura 9. Ejemplo redacción del control

- **Responsable**

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 (verifica, valida, concilia, coteja, compara, etc.)

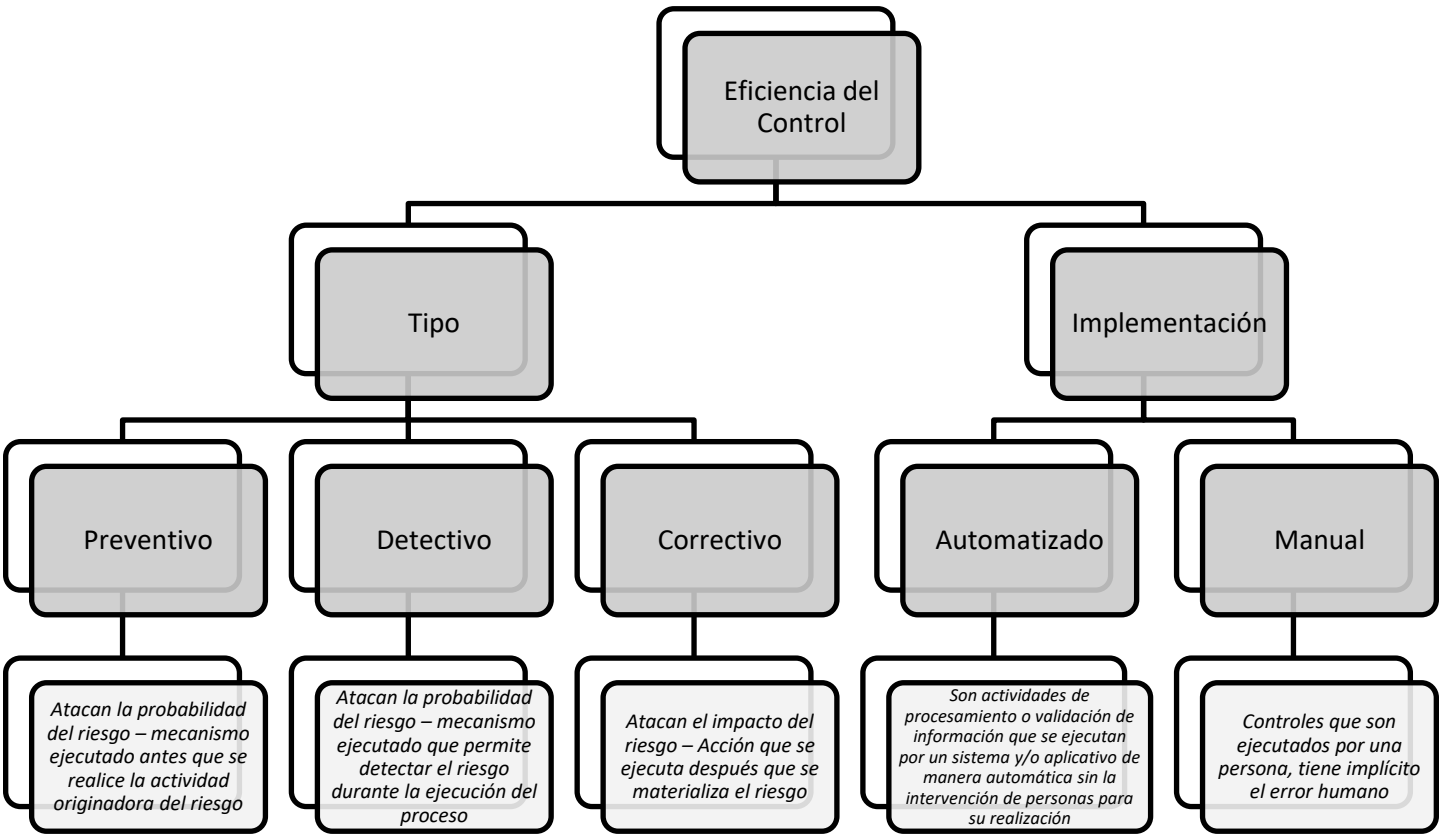
- **Complemento**

Corresponde a los detalles que permiten identificar claramente el objeto del control (periodicidad, evidencia que soporta el control, acción a realizar en caso de desviación encontrada al efectuar el control)

2.4.4.2.2 Tipología del control

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia (ver figura 10) y la formalización (ver figura 10)

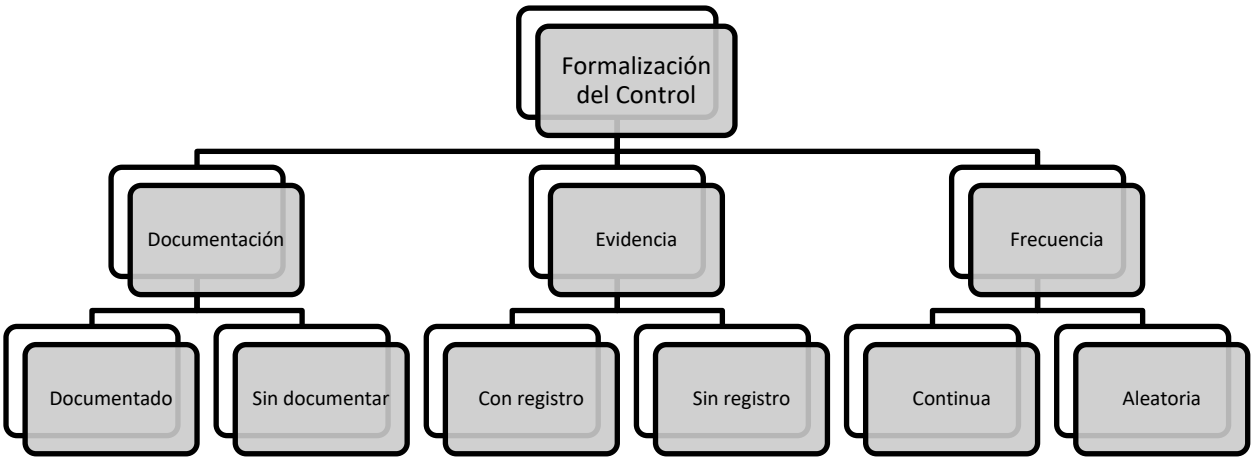
Figura 10. Eficiencia del control



Los atributos de formalización se recogen de manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad (ver figura 11).

NOTA: Controles de tipo correctivo no son aplicables a los riesgos de corrupción

Figura 11. Formalización del control



2.4.4.2.3 Análisis y evaluación del control

Se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 8 se puede observar la descripción y peso asociados a cada uno.

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.

Tabla 8. Atributos para el diseño del control

Características			Peso
Atributos de Eficiencia	Tipo	Preventivo	25%
		Detectivo	15%
		Correctivo	10%
	Implementación	Automático	25%
		Manual	15%
Atributos de Formalización	Documentación	Documentado	-
		Sin Documentar	-
	Frecuencia	Continua	-
		Aleatoria	-
	Evidencia	Registro Sustancial	-
		Registro Material	-
		Sin registro	-

2.4.4.3 Nivel de riesgo (riesgo residual)

Es el resultado de aplicar la efectividad de los controles al riesgo inherente (ver figura 12).

Figura 12. Formulación riesgo residual

Para mayor claridad, se da a continuación un ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles.

Ejemplo:

Riesgo identificado: Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos

- **Probabilidad Inherente**= moderada 60%
- **Impacto Inherente**= mayor 80%
- **Zona de riesgo:** alta
- **Control 1:** el profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación (ver tabla 9)

Tabla 9. Efectividad control 1

Controles y sus características				Peso
Control 1 El profesional del área de contratos, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin Documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con Registro	X	-
		Sin registro		-
Total valoración control 1				40%

- **Control 2:** el jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto (ver tabla 10)

Tabla 10. Efectividad control 2

Controles y sus características				Peso
Control 2 El jefe de Contratos, verifica en el sistema de información de contratación la información registrada por el profesional asignado, y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado.	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin Documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con Registro	X	-
		Sin registro		-
Total valoración control 2				30%

Para la aplicación de los controles se debe tener en cuenta que éstos 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 (ver tabla 11)

Tabla 11. Aplicación de controles para establecer riesgo residual

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

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, y considerando si lo controles ayudan o no a la disminución de impacto o la probabilidad, procedemos a la elaboración del Mapa de Riesgo Residual (después de los controles)

Con la calificación obtenida se realiza un desplazamiento en la matriz así (ver figuras 13 y 14):

- Si el control afecta la **probabilidad** se desplaza hacia **abajo**
- Si afecta el **impacto** se desplaza a la **izquierda**

Figura 13. Movimiento en la matriz de calor de acuerdo con el tipo de control

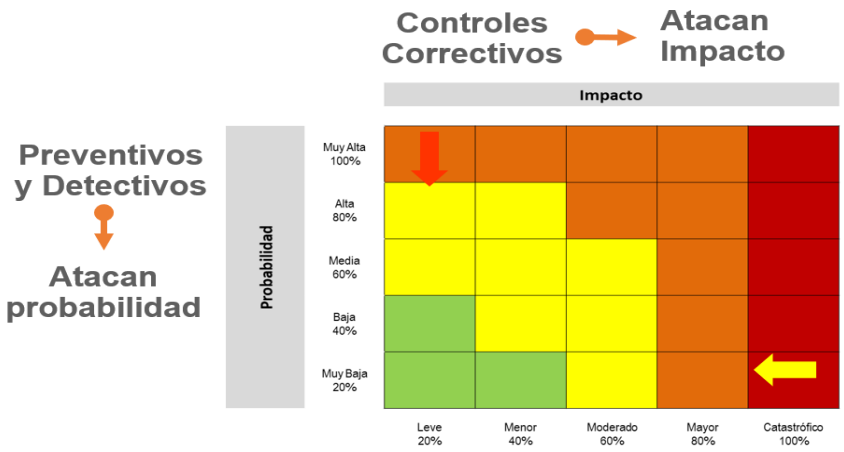
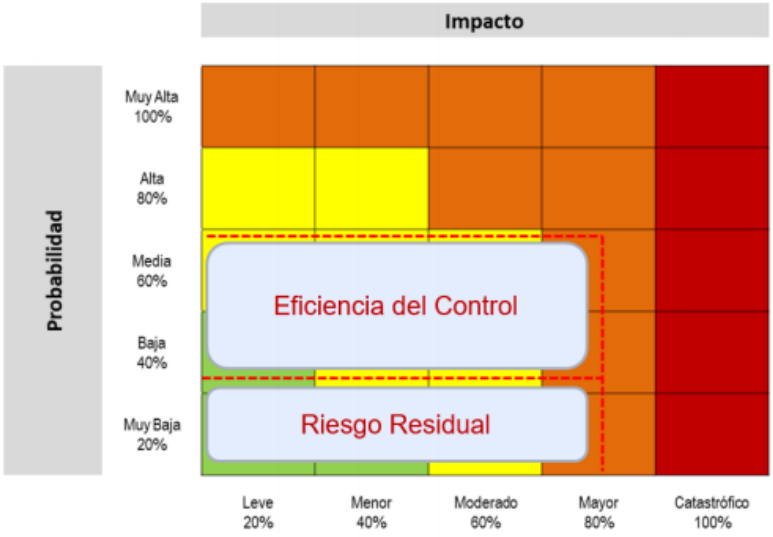


Figura 14. Movimiento en la matriz de calor ejemplo propuesto



2.5 ESTRATEGIA PARA COMBATIR EL RIESGO

Decisión que la Unidad toma frente a un determinado nivel de riesgo, pueden ser aceptar, reducir y evitar. Se analiza frente al Riesgo Residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos se procederá a partir del riesgo inherente (ver tabla 12)

Tabla 12. Estrategias para combatir el riesgo

Zona de Severidad	Estrategia de tratamiento
Bajo	**ACEPTAR** el riesgo y se determina **ASUMIR** el mismo conociendo los efectos de su posible materialización. Frente a los riesgos de corrupción esta medida no es aplicable
Moderado	**REDUCIR** el riesgo, se establece plan de acción o la implementación o ajuste de un control existente que **MITIGUE** nivel de riesgo.
Alto	**REDUCIR** el riesgo, se establece plan de acción o la implementación o ajuste de un control existente que **MITIGUE** el nivel de riesgo. O **REDUCIR** el riesgo y se considera **TRANSFERIR** el riesgo tercerizando el proceso/actividad o trasladar el riesgo a través de seguros o pólizas. La responsabilidad economica recae sobre el tercero, pero no se trasfiere la responsabilidad sobre el tema reputacional.
Extremo	**REDUCIR** el riesgo, se establece plan de acción o la implementación o ajuste de un control existente que **MITIGUE** el nivel de riesgo. O **REDUCIR** el riesgo y se determina **TRANSFERIR** el riesgo tercerizando el proceso/actividad o trasladar el riesgo a través de seguros o pólizas. O **EVITAR** y se determina NO asumir la actividad que genera este riesgo.

Para efectos del plan de acción adicional se debe especificar responsable y fecha de implementación (Inicio y Fin)

2.6 MONITOREO Y REVISIÓN

La revisión y actualización de los mapas de riesgos se validan mínimo una (1) vez en cada vigencia atendiendo la metodología vigente y de manera puntual ante cualquier modificación del proceso, estructura organizacional, objetivos estratégicos, modificación de controles derivados del seguimiento o de los eventos (materialización del riesgo).

Para esta validación se debe tener en cuenta:

- Riesgos materializados (ver Formato monitoreo a la materialización de los riesgos). https://www.unidadvictimas.gov.co/es/NODE/41806
- Observaciones, investigaciones disciplinarias, penales, fiscales, o de entes reguladores
- Hallazgos por parte de la Oficina de Control Interno o de Auditoría externa.
- Cambios importantes en el contexto estratégico que den lugar a nuevos riesgos
- Necesidades identificadas por el proceso o Dirección Territorial

La periodicidad de monitoreo a los controles y plan de acción de cada riesgo está definida en el Mapa de Riesgos Institucional y su tratamiento establecido en el apartado 4.4. de este documento, por sus respectivos líderes y enlaces

El líder o delegado de riesgos en cada Proceso y Dirección Territorial analizan los resultados del seguimiento y pueden determinar establecer un plan de mejoramiento ante cualquier desviación y socializa al interior de su dependencia las acciones a seguir.

El líder o delegado de riesgos en cada Proceso y Dirección Territorial comunica, revisa y actualiza, con el acompañamiento de la OAP, el mapa de riesgo ante cualquier modificación en sus controles o plan de acción, derivados del seguimiento o de los eventos (materialización del riesgo).

2.6.1 Acciones ante la materialización de los riesgos

2.6.1.1 Acciones ante la materialización de riesgos no identificados

- Informar a la segunda línea de defensa (Oficina Asesora de Planeación) con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso o dirección territorial
- Proceder a identificar, valorar y realizar seguimiento según metodología
- Incluir el riesgo en el mapa de riesgos institucional

2.6.1.2 Acciones ante la materialización de riesgos

El líder del proceso o enlaces designados deben:

- Informar a la segunda línea de defensa (Oficina Asesora de Planeación) a través del Formato Monitoreo a la materialización de los riesgos Trimestralmente o una vez se materialice.
  https://www.unidadvictimas.gov.co/es/NODE/41806
- Analizar las causas del evento
- Identificar e implementar las acciones correctivas necesarias, efectuar el análisis de causas y determinar acciones preventivas y de mejora.
- Incluir en aplicativo dispuesto vigente para el seguimiento a su implementación
- Verificar los controles y plan de tratamiento del mapa de riesgos y tomar las acciones a que haya lugar
- Para riesgos de Emergencias, Crisis y Seguridad de las personas, la Oficina Asesora de Planeación debe informar al Proceso de Gestión del Talento Humano a través del correo dispuesto, para su análisis y gestión.

2.6.1.3 Acciones ante la materialización de riesgos de corrupción

El líder del proceso, enlaces designados deben:

- Informar a la segunda línea de defensa (Oficina Asesora de Planeación) sobre el hecho encontrado
- Una vez surtido el conducto regular establecido por la Unidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente
- Identificar e implementar las acciones correctivas necesarias, efectuar el análisis de causas y determinar acciones preventivas y de mejora
- Incluir en aplicativo dispuesto vigente para el seguimiento a su implementación
- Verificar los controles y plan de tratamiento del mapa de riesgos y tomar las acciones a que haya lugar

2.6.1.4 Monitoreo a la materialización de riesgos

En caso de materialización de riesgos se debe registrar en todos los casos la corrección o acción correctiva o acción de mejora correspondiente en el aplicativo dispuesto vigente, teniendo en cuenta lo siguiente:

- Identificación: Se puede seleccionar la opción Acciones correctivas o Corrección o Acción de mejora.
- Origen: En todos los casos se deberá seleccionar la opción "materialización de riesgos".

2.6.1.5 Seguimiento riesgos de corrupción

El seguimiento lo realiza los procesos o direcciones territoriales a través de sus respectivos líderes y enlaces en la periodicidad establecida en sus controles y planes de acción definidos.

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 debe publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

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 por control interno se refieren a:

- Determinar la efectividad de 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.

2.7 SOCIALIZACIÓN, DIVULGACIÓN, CONSULTA Y PUBLICACIÓN

2.7.1 Socialización

Se realizan sesiones de trabajo al interior de cada proceso o dirección territorial, por parte de la Oficina Asesora de Planeación de forma presencial o virtual en la que se da a conocer:

- Procedimiento de administración de riesgos https://www.unidadvictimas.gov.co/es/NODE/41803
- Política y metodología de riesgos definida por la Unidad https://www.unidadvictimas.gov.co/es/NODE/45506

- Herramienta de gestión para la identificación, análisis, valoración, tratamiento y acciones del riesgo

  https://www.unidadvictimas.gov.co/es/NODE/41806

Estas sesiones se llevan a cabo con equipos multidisciplinarios que tengan amplio conocimiento y experiencia en el quehacer de cada proceso y Dirección territorial, con el fin de mantener una comunicación y consulta fluida que enriquezca el ejercicio de la Administración del Riesgo en la Unidad.

2.7.2 Divulgación

La divulgación de los documentos asociados a la metodología, política y procedimiento de administración de riesgos Institucionales se realiza a través de la página web de la Entidad Direccionamiento Estratégico | Unidad para las Víctimas (unidadvictimas.gov.co)

El mapa de riesgos institucional vigente se encuentra en la página web de la Entidad Mapa de Riesgos Institucional (corrupción y gestión) | Unidad para las Víctimas (unidadvictimas.gov.co)

2.7.3 Consulta y Publicación

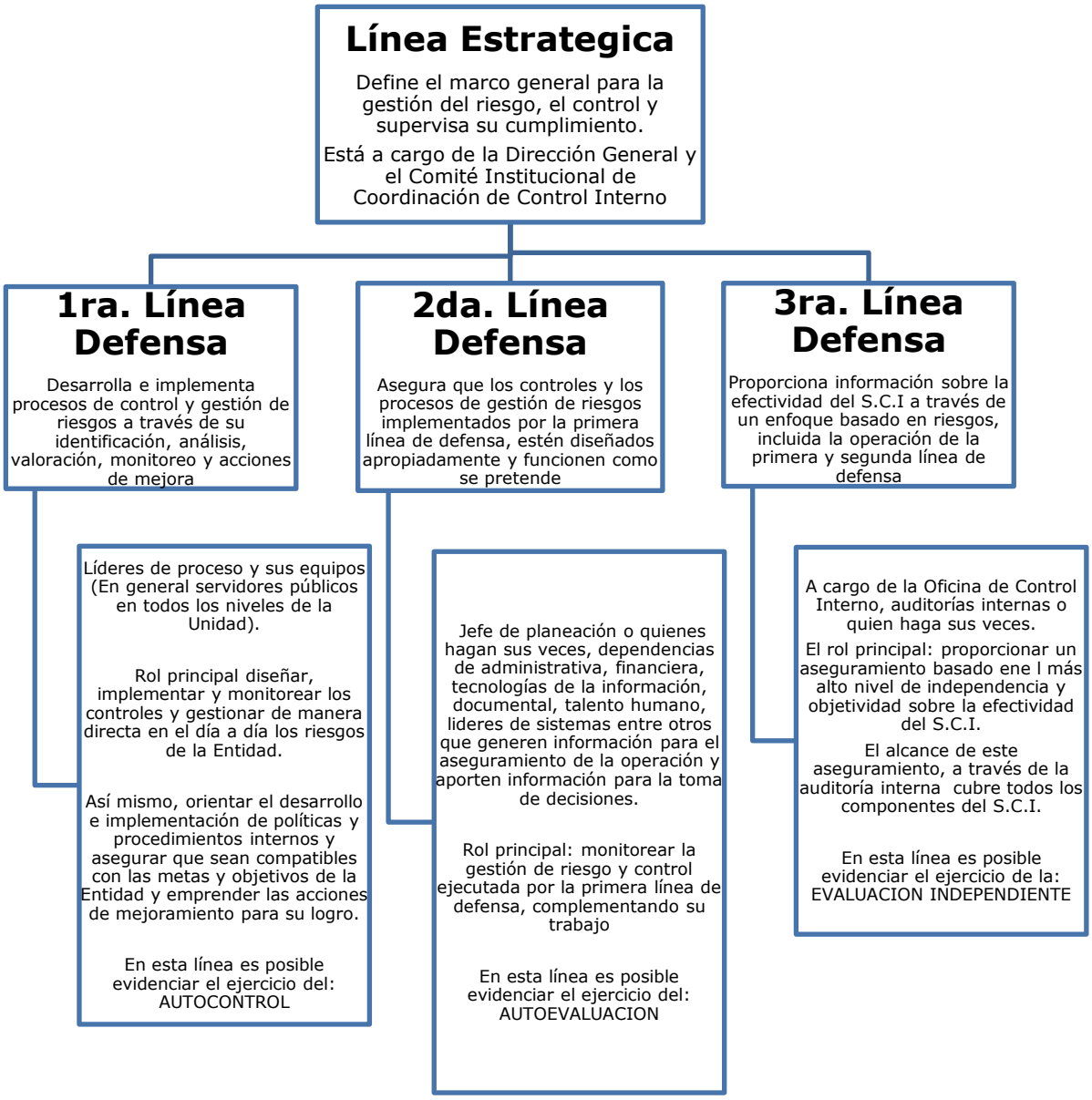
La Oficina Asesora de Planeación consolida el Mapa de riesgos Institucional (incluyendo Corrupción) para someter a consulta y observaciones ante los grupos de interés en el mes de enero de cada vigencia a través de su página web y redes sociales, en caso de que amerite, se realizan los ajustes correspondientes y se somete para aprobación por parte del Comité.

Finalmente, la Unidad realiza su publicación antes del 31 de enero de cada vigencia en el Portal web.

2.8 ESQUEMA DE LINEAS DE DEFENSA

El esquema se encuentra orientado a la asignación de roles y responsabilidades de los funcionarios involucrados en la administración y control del riesgo en la Unidad, con el fin de garantizar el aseguramiento de la gestión y prevenir la materialización de los riesgos en todos sus ámbitos.

Las tres líneas de defensa alineadas con la dimensión del MIPG de "Control interno", que se desarrolla con el MECI están involucradas en el monitoreo y revisión de la gestión de riesgos a través de un esquema de asignación de responsabilidades y roles, así:



De acuerdo con esto la Unidad ha establecido una matriz de roles y responsabilidades donde se establecen cada una de las etapas de la implementación

de la metodología de riesgos y la responsabilidad de cada una de las líneas de defensa frente al cumplimiento las mismas.

Metodología	Línea Estratégica	Primera línea de defensa	Segunda línea de defensa	
	Dirección General y Comité de Control Interno	**Líder del Proceso/Dirección Territorial – Enlaces SIG**	**Oficina Asesora de Planeación**	**Dependencias /Lideres Sistemas**
Política para la administración del riesgo	Aprobar la política institucional de riesgos a lo largo de toda la organización. Garantizar los recursos necesarios para ejercer una óptima gestión del riesgo	Socializar los lineamientos determinados en la política institucional de riesgos con el equipo de trabajo	Conocer, apropiar y dar a conocer la política institucional de riesgos. Determinar los lineamientos para la administración del riesgo en la entidad y los aspectos necesarios para la identificación y mitigación de los riesgos	Conocer y empoderar la política institucional de riesgos.
Establecimiento del Contexto	Analizar el contexto interno y externo de la entidad para facilitar la identificación de riesgos a los procesos	Apoyar el análisis de contexto del proceso en conjunto con su equipo de trabajo.	Participar en el análisis de contexto del proceso para la definición de la política de riesgo, la definición del nivel de impacto y aceptación del riesgo. Orientar a la primera línea de defensa en el análisis del contexto del proceso	Participar en el análisis de contexto del proceso al que pertenece.
Identificación del Riesgo	NA	Impulsar y realizar al interior del proceso/DT la identificación de los riesgos y consolidar la información en el instrumento establecido. Determinar las causas, consecuencias y tipo de riesgo de acuerdo con la metodología de administración de riesgos.	Asesorar a los procesos en la etapa de identificación. Liderar la identificación de los riesgos institucionales en procesos/DT´s Consolidar el mapa de riesgo	Participar en la identificación de riesgos, causas y consecuencias para su sistema de acuerdo con lo establecido en la metodología de administración de riesgos
Análisis y Valoración del Riesgo	Analizar los riesgos y amenazas identificados en la Unidad, con respecto al cumplimiento de planes estratégicos.	Liderar el análisis y valoración del riesgo para el proceso. Impulsar y realizar al interior del proceso el análisis y valoración de los riesgos identificados para el proceso/DT Establecer los controles idóneos que permitan administrar los riesgos identificados. Realizar seguimiento a los controles implementados Detectar las debilidades en los controles y diseñar las acciones correctivas del caso.	Asesorar a los procesos en la etapa de análisis y valoración del riesgo Orientar y capacitar en la identificación, análisis y valoración del riesgo.	Participar en el análisis y valoración de los riesgos identificados para su sistema y en la identificación de los controles idóneos que permitan administrar los riesgos identificados. Asegurar la correcta aplicación de controles definidos en la primera línea de defensa.

Metodología	Línea Estratégica	Primera línea de defensa	Segunda línea de defensa		Tercera Línea de Defensa
	Dirección General y Comité de Control Interno	**Líder del Proceso/Dirección Territorial – Enlaces SIG**	**Oficina Asesora de Planeación**	**Dependencias /Lideres Sistemas**	**Oficina de Control Interno**
Aprobación Mapa de riesgos Institucional	Aprobar el mapa de riesgos institucional	Realizar la aprobación del mapa de riesgos del proceso/DT	Consolidar y validar el mapa de riesgos institucional Someter a consulta de grupos de valor	NA	NA
Planes de Acción	NA	Asegurar la ejecución de los controles y de las acciones del Plan de acción a los riesgos de su proceso/DT Consolidar la evidencia de controles y planes de acción	Acompañar y asesorar en la formulación de los Planes de acción Establecer lineamientos que permitan el cumplimiento de los planes de acción.	Acompañar y asesoría en la formulación de los Planes de acción asociados a su sistema	Realizar seguimiento a los mapas de riesgos y generar alertas al respecto
Revisión y actualización	NA	Atender todos los requerimientos de la oficina de planeación con respecto a los Mapas de riesgos de gestión y de corrupción y Metodología de Administración de riesgos de la unidad. Impulsar y participar en la Mesas de trabajo para la revisión y actualización de los riesgos.	Acompañar y asesorar la revisión y actualización de los mapas de riesgos Realizar las actualizaciones requeridas y consolidar la información en el instrumento establecido.	Participar en las Mesas de trabajo para la revisión y actualización de los riesgos.	NA
Monitoreo a la materialización de los riesgos	NA	Establecer acciones frente a los riesgos materializados. Asegurar el monitoreo a la materialización de los riesgos del proceso/DT y tomar acciones frente a los resultados.	Recibir y consolidar los reportes de los riesgos materializados, su estado de implementación de acciones e informar a la Dirección/Comité para toma de decisiones. Evaluar los controles establecidos por la primera línea de defensa que sean adecuados y efectivos	NA	NA

Metodología	Línea Estratégica	Primera línea de defensa	Segunda línea de defensa		Tercera Línea de Defensa
	Dirección General y Comité de Control Interno	**Líder del Proceso/Dirección Territorial – Enlaces SIG**	**Oficina Asesora de Planeación**	**Dependencias /Lideres Sistemas**	**Oficina de Control Interno**
Seguimiento	Analizar estratégicamente los resultados e informes de seguimiento a los mapas de riesgos de la entidad, de tal manera que se facilite la toma de decisiones requeridas para la mejora de la gestión del riesgo en la entidad o para realizar las actualizaciones necesarias a la política de Administración del Riesgo.	Asegurar que se atiendan todos los requerimientos de la oficina de control Interno con respecto a los Mapas de riesgos de gestión y de corrupción, planes de respuesta y monitoreo a la materialización de riesgo	Atender todos los requerimientos de la oficina de control Interno con respecto a la evidencia relacionada con el Mapa de riesgos institucional, planes de acción y monitoreo a la materialización de riesgo.	Atender todos los requerimientos de la oficina de control Interno con respecto a la evidencia relacionada con los riesgos asociados a los sistemas	Realizar seguimiento al mapa de riesgos institucional. Evaluar las diferentes fases señaladas para la gestión de los riesgos institucionales Determinar si los controles, establecidos en el proceso son adecuados para prevenir o mitigar los riesgos Evaluar las acciones de mejora, su ejecución, al nivel de avance/cumplimiento. Seguimiento a la materialización del riesgo.
Comunicación y Consulta	NA	Conocer y apropiar los riesgos de su proceso. Participar en los procesos de aprendizaje que se programen y facilitar la asistencia de los funcionarios de su equipo de trabajo Como representantes y facilitadores de cada proceso deben apropiar los conocimientos necesarios frente a la metodología de administración del riesgo, con el fin de socializarlos a los miembros de sus equipos o procesos/DT dentro de la entidad.	Coordinar el proceso de divulgación y consulta, generando espacios para la socialización o acompañamiento técnico a los funcionarios sobre la metodología de administración de riesgos y sus documentos asociados	NA	NA

NOTA: Los riesgos operacionales asociados a los Sistemas de Gestión de Seguridad y Salud en el Trabajo y Ambiental se establecen de acuerdo a los lineamientos establecidos por los procesos lideres de estos sistemas.

Sistema de Gestión de Seguridad y Salud en el Trabajo

- Matriz de Identificación de Peligros, Valoración de Riesgos y Determinación de Controles https://www.unidadvictimas.gov.co/es/NODE/39667

Sistema de Gestión Ambiental

- Procedimiento para la Identificación y Evaluación de Aspectos e Impactos Ambientales https://www.unidadvictimas.gov.co/es/NODE/42961

- Matriz de Identificación y Evaluación de Aspectos e Impactos Ambientales – Procesos y Direcciones Territoriales https://www.unidadvictimas.gov.co/es/NODE/65480

- Formato Matriz de Identificación y Evaluación de Aspectos e Impactos Ambientales https://www.unidadvictimas.gov.co/es/NODE/42960

3. DOCUMENTOS DE REFERENCIA

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA, Decreto 0943 del 21 mayo de 2014, Por el cual se actualiza el Modelo Estándar de Control Interno MECI.

SECRETARIA DE TRANSPARENCIA, Guía para la gestión del riesgo de corrupción, 2015

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 6 - noviembre de 2022

4. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
V1	31/10/2013	Creación
V2	18/09/2015	Actualización por cambios en el MECI 1000:2005 y queda vigente el MECI 2014. Expedición del Decreto 0943 de 2014
V3	27/04/2016	Ajustes por la expedición de la Guía para la Administración del Riesgo del DAFP
V4	06/03/2017	Ajustes por la Actualización de la Guía para la Administración del Riesgo del DAFP Ajustes por la expedición de la Guía para la gestión del riesgo de corrupción Inclusión y articulación de riesgos públicos, ambientales, seguridad y salud en el trabajo y seguridad de la información
V5	06/03/2018	Ajustes Análisis de contexto, materialización de riesgos. Ajuste de acuerdo con recomendaciones de auditoría.
V6	14/12/2018	Ajustes anexo 2 Gestión del riesgo de seguridad de la información, de acuerdo con los Lineamientos de MINTIC
V7	30/05/2019	Se ajusta de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018
V8	22/05/2020	Se incluye anexo para la identificación de riesgos y peligros de gestión ambiental. Se ajusta de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018
V9	16/09/2021	Se ajusta de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 5 - diciembre de 2020 Política de Administración de Riesgos Identificación de Riesgos Valoración de Riesgos Estrategia para combatir el riesgo Monitoreo y revisión
V10	26/05/2022	Por la cual se deroga la resolución 1395 de 2020 que adopta la metodología de riesgos institucionales, y se dictan otras disposiciones.
V11	04/12/2023	Se ajusta de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6 - noviembre de 2022, asociado a riesgos de tipología fiscal, se ajustan ítems de enlaces plan indicativo y Manual SIG, objetivos específicos, identificación de riesgos, tablas factores y clasificación de riesgos, se incluye tabla de probabilidad riesgos de corrupción, tratamiento de riesgos y esquema líneas de defensa.