Metodología de Administración de Riesgos

UNIDAD PARA LAS VÍCTIMAS

TABLA DE CONTENIDO

5. DOCUMENTOS DE REFERENCIA

ANEXOS

ANEXO 1. IDENTIFICACIÓN DE PELIGROS Y RIESGOS EN EL DESARROLLO DE LAS ACTIVIDADES LABORALES - SEGURIDAD Y SALUD EN EL TRABAJO

ANEXO 2 . IDENTIFICACIÓN RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La Unidad a partir de agosto de 2013 diseñó e implementó el componente de Administración de Riesgos, fortalecer al Sistema de Control Interno de la Unidad, aplicando una metodología semicuantitativa con el fin de identificar y valorar los riesgos en las actividades o eventos que puedan afectar de forma negativa el cumplimiento de la misión, visión, objetivos institucionales, metas, proyectos de la Unidad para las Víctimas, entre otros; esto permite el fortalecimiento de la cultura del autocontrol y autoevaluación y la identificación de acciones y oportunidades para el mejoramiento continuo y optimización de la gestión institucional.

A partir del 2017, la Unidad pretende integrar a esta metodología los riesgos públicos (de seguridad de las personas), seguridad de la información y seguridad y salud en el trabajo, con el fin de gestionar los riegos a los cuales la Entidad se encuentra expuesta de manera integral.

Para el 2018 la Unidad busca articular esta metodología al MIPG, Plan anticorrupción y atención al ciudadano y al cumplimiento de la ley 1712 del 2014 "ley de transparencia y derecho de acceso a la información pública", con el objetivo de generar una cultura de transparencia y lucha contra la corrupción.

2. OBJETIVO

Establecer la Metodología de Administración de Riesgos Integrales de la Unidad con el fin de identificar, valorar y dar tratamiento a los riesgos de la Unidad.

3. DEFINICIONES

Actividad: Agrupación de tareas que hace parte de un Proceso o Dirección territorial.

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 categoriza en activo crítico.

Amenaza: Las amenazas son todos los elementos o acciones capaces de atentar contra la seguridad de la información y son generadoras de eventos; Las amenazas surgen a partir de la

existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada.

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.

Calificación de Riesgos: cuantificación de los riesgos de acuerdo con la probabilidad de ocurrencia o frecuencia y sus consecuencias.

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

Componente: Agrupación de elementos que hace parte de un subsistema.

Control: los controles son acciones o actividades que deben apuntar a mitigar las causas generadoras del riesgo.

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.

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.

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.

Elemento: Agrupación de factores que hace parte de un componente.

Entorno: Ambiente, contexto. Lo que rodea; territorio o conjunto de lugares que rodean a otro.

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

Evento: Suceso; particularmente suceso posible.

Frecuencia del riesgo: medida estadística del número de veces que se presenta un riesgo en un período de tiempo.

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.

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

Identificación de riesgos: proceso para reconocer si existe un riesgo y definir sus características.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización de un riesgo.

Mapa de Riesgos: Documento con la información resultante de la gestión del riesgo.

Mapa de Riesgos Institucional: Contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, se alimenta con los riesgos residuales de cada uno de los procesos y direcciones territoriales, los cuales pueden afectar el cumplimiento de la misión institucional y objetivos de la entidad. 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.

Mapa de Riesgos por Proceso o Dirección territorial: Recoge los riesgos identificados para cada uno de los procesos o Dirección territorial, los cuales pueden afectar el logro de sus objetivos.

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

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

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.

Peligro: Fuente, situación o acto con un potencial de daño en términos de lesión o enfermedad o una combinación de estas.

Pérdida: consecuencia negativa que puede ocasionar un riesgo, sea financiera o de otro tipo.

Plan: Proyecto, programa de las cosas que se van a hacer y de cómo hacerlas.

Políticas: Principios que sirven de guía y dirigen los esfuerzos de una organización para alcanzar sus objetivos.

Políticas 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.

Posibilidad: condición o característica para que llegue a ocurrir un hecho.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.

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.

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

Responsable: Que es consciente de sus obligaciones y actúa conforme a ellas.

Riesgo: 1. Evento capaz de poner en peligro el cumplimiento de los objetivos de la Entidad Pública con eficiencia, eficacia y calidad. 2. La posibilidad de que ocurra dicho evento.

Riesgo aceptable: aquel que se considera normal para una actividad determinada. Es el riesgo que tiene una probabilidad o frecuencia de ocurrencia muy baja y su impacto leve.

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

Riesgo de 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 seguridad en las personas: El riesgo de seguridad personal 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.

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección (controles) para modificar su probabilidad o impacto; es decir, es la valoración del riesgo sin tener en cuenta los controles establecidos para este.

Riesgo residual: Nivel de riesgo que permanece luego determinar medidas de tratamiento del riesgo.

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.

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

Servidores públicos: Son los miembros de las corporaciones públicas, los empleados y trabajadores del Estado y de sus entidades descentralizadas territorialmente y por servicios.

Socializar: Compartir la información con todos los funcionarios del grupo al que pueda interesar.

Subsistema: Agrupación de Componentes que hace parte de un Sistema.

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: Las vulnerabilidades son las debilidades inherentes al activo que lo hacen susceptible de ser atacado.

4. DESARROLLO

I. MARCO LEGAL

- Constitución Política de Colombia. Artículos 209 y 269.
- Ley 87 de 1993: "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones". (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 objetivos de control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
- Ley 489 de 1998: "Estatuto básico de organización y funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno.
- Decreto 2145 de 1999: "Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones." (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art. 8° de la Ley 1474 de 2011). Decreto 2593 del 2000: Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999.
- Decreto 1537 de 2001: "Por la cual se reglamenta parcialmente la Ley 87 de 1992 en cuanto a elementos técnicos y administrativos que fortalecen el Sistema de control interno de entidades y organismos del estado". El párrafo del Artículo 4° señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (…) y en su Artículo 3° establece el rol que debe desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su Artículo

4° la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…).

- Directiva presidencial 09 de 1999: Lineamientos para la implementación de la política de lucha contra la corrupción.

- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- Decreto 0943 de 2014: "Por medio del cual se actualiza el Modelo Estándar de Control Interno MECI" y se presenta el manual técnico del modelo estándar de control interno para el Estado colombiano MECI 2014. Numeral 1.3 Componente de administración del riesgo.

- Norma Técnica Colombiana de Gestión de Riesgos - NTC 31000 de febrero 16 de 2011.

- Resolución 0479 del 30 de julio de 2014 "por la cual se adopta el Modelo Estándar de Control Interno MECI 2014 en la Unidad para la Atención y Reparación Integral a las Víctimas y se deroga la Resolución 0899 del 03 de septiembre de 2013".

- Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

- Guía de administración de riesgos del Departamento Administrativo de la Función Pública (DAFP).

- Guía de riesgos de corrupción de la Secretaria de Transparencia de la Presidencia de la Republica.

II. Generalidades de la Administración de Riesgos

1. Definición

La Administración de riesgos es necesaria debido a la incertidumbre y la posibilidad que tienen las Entidades de verse enfrentadas a circunstancias, internas y externas, que puedan afectar el logro de sus objetivos[1]

La administración de riesgos es un proceso desarrollado por la Alta Dirección de la Entidad y por todo el personal para proporcionar un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino

[1] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

logrando que la administración del riesgo se convierta en una parte fundamental de la gestión de la entidad.

2. Objetivos

El objetivo primordial de la Administración de riesgos es crear una cultura de **PREVENCIÓN Y CONTROL** para que los eventos inesperados causen el mínimo impacto posible.

Entre los objetivos específicos se tienen:

- Generar conciencia sobre la necesidad de identificar y darle tratamiento a todos los riesgos 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 de gestión y corrupción.
- Prevenir o mitigar cualquier pérdida de recursos que pueda generar la materialización de los riesgos.
- Prevenir de manera permanente la ocurrencia de riesgos de corrupción.
- Proteger a los funcionarios contra accidentes que pueden causar lesiones, daños serios o muerte, mejorando y haciendo más seguras las condiciones de trabajo e implementando medidas preventivas y de protección.
- Buscar la mejora continua y suministrar insumos para la toma de decisiones de la Entidad.

3. Beneficios

La Administración de riesgos contribuye a gestionar los riesgos para alcanzar los objetivos en todos los niveles institucionales.
Los beneficios de la Administración de riesgos son:

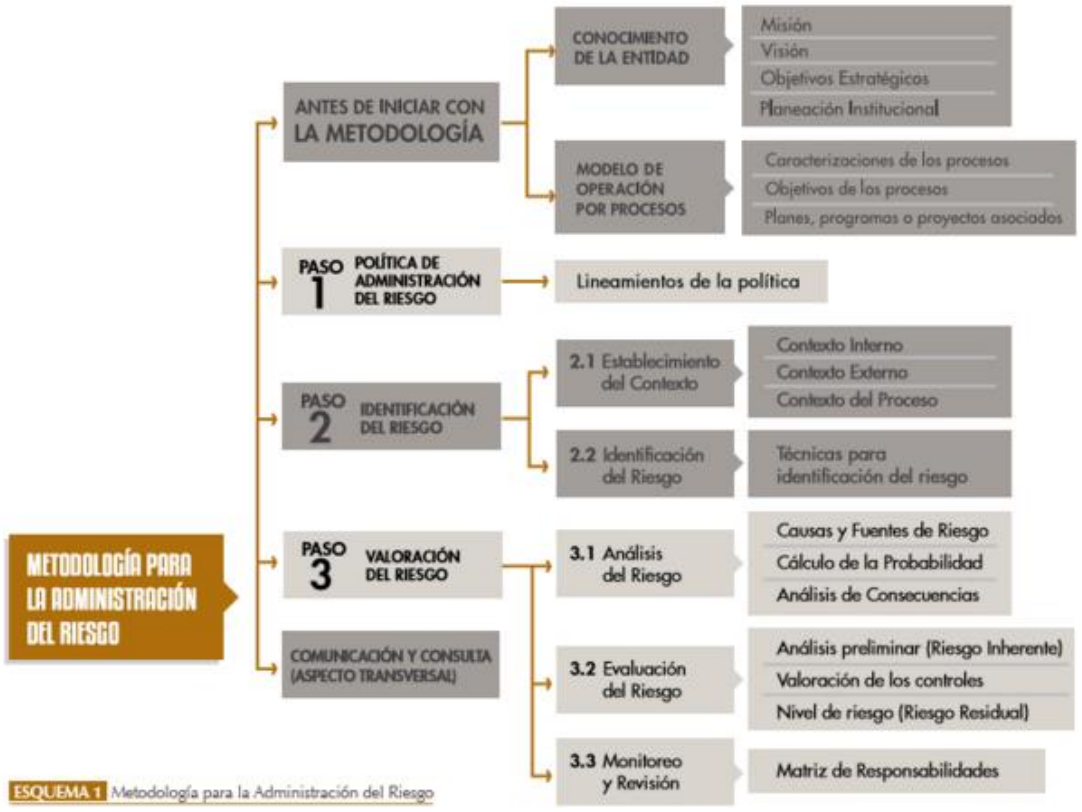
- Contribuir al cumplimiento de los objetivos de la Unidad.
- Consolidar la información de los riesgos para su análisis y mitigación.
- Identificar los riesgos más relevantes en cada proceso y Dirección territorial.
- Saber cómo actuar en situaciones de crisis.
- Mejorar la cultura organizacional propiciando espacios para la participación y discusión sobre los aspectos a mejorar.

- Fortalecer el Sistema Integrado de Gestión de la Unidad.
- Contribuir a una planificación estratégica más efectiva y eficaz.

III. Metodología Administración del Riesgo

La metodología se diseñó teniendo en cuenta los lineamientos del Modelo Estándar de Control Interno - MECI 2014, la Guía para Administración de Riesgos del DAFP. Guía para la gestión del riesgo de corrupción de la Secretaria de Transparencia de la Presidencia de la Republica y la NTC 31000 de Gestión de Riesgos de ICONTEC, GTC 45, NTC 14001: 2015, NTC 27001: 2013.

Metodología de administración de riesgos[2]



ESQUEMA 1 Metodología para la Administración del Riesgo

[2] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

Para construcción de esta metodología se analizó la Metodología de Administración de Riesgos del DAFP y Guía para la gestión del riesgo de corrupción de la Secretaria de Transparencia y a partir de ellas se construyó una Metodología que integró todos los tipos de riesgos y permitió dar cumplimiento a la normatividad aplicable a este tema. Sin embargo, para la etapa de valoración del riesgo fue necesario un capítulo independiente para los riesgos de corrupción y de gestión, ya que tablas de calificación son diferentes. Los demás aspectos y etapas serán tratados de la misma manera para todos los dos tipos de riesgos. La metodología cuenta con *seis capítulos que en su orden son:*

I. Conocimiento previo
II. Política de Administración de Riesgos
III. Etapas de la Administración del Riesgo
IV. Monitoreo y revisión
V. Seguimiento
VI. Divulgación, comunicación y consulta
VII. Roles y responsabilidades.

Para la identificación de los riesgos, se tomará como base toda la documentación disponible de la Entidad, a fin de registrar todos los riesgos existentes y que puedan afectar el cumplimiento de las metas y los objetivos de la entidad (ejemplo: análisis de contexto, informes de Auditorias, informes de seguimiento a los mapas de riesgos, los riesgos materializados, etc.). Los mapas de riesgos se elaboran con la participación de los directivos y servidores públicos de la Unidad con el acompañamiento de los enlaces del Sistema Integrado de Gestión de la Unidad.

La Metodología de Administración de Riesgos de la Unidad está sujeta a ajustes de acuerdo con las orientaciones que sobre la materia determine el Departamento Administrativo de la Función Pública, la secretaria de transparencia de la Presidencia de la Republica, las normas o estándares nacionales que se establezcan sobre el particular y como parte de la mejora continua del Sistema Integrado de Gestión.

Los mapas de riesgos se elaboran con la participación de los directivos y servidores públicos de todos los procesos y direcciones territoriales de la Unidad y con el acompañamiento de la Oficina Asesora de Planeación, particularmente con el apoyo de los enlaces del Sistema Integrado de Gestión de la Unidad, quienes además facilitarán y apoyarán su monitoreo.

El mapa de riesgos institucional se construye consolidando los riesgos que tienen plan de respuesta, es decir, aquellos riesgos residuales que se encuentren en zona moderada, alta o extrema de cada proceso/dirección territorial y los de corrupción, que pueden afectar el cumplimiento de la misión o los objetivos de la Unidad.

Para las Direcciones territoriales se construirá un mapa de riesgos en el cual se identifiquen riesgos propios de la operación de la Dirección territorial y sobre los cuales se identifiquen controles y plan de respuesta que dependan de la gestión de esta.

1. Conocimiento previo

Para implementar a metodología de administración de riesgos es necesario tener conocimiento sobre:

- **La planeación estratégica de la Unidad**: (misión, visión, objetivos estratégicos, indicadores y metas)
- **Modelo de operación por procesos:** (cadena de valor, mapa de procesos, caracterización y objetivos de los procesos y procedimientos)
- **Sistema Integrado de Gestión y sus componentes**.
- **Partes interesadas.** Víctimas del conflicto, Entidades públicas y privadas del orden nacional, Entidades territoriales, Sociedad y Comunidad Internacional, Unidad (cliente interno).
- **Política de Administración de Riesgos.** Alcance, nivel de aceptación etc.
- **Contexto estratégico de la Unidad.** Contexto interno y externo

2. Política de administración del riesgo

"La Unidad administra integralmente los riesgos que pueden afectar el cumplimiento de los objetivos, trabajando para la reparación integral de las víctimas y la implementación de la ley 1448 del 2011, a fin de optimizar su eficacia y eficiencia a través de la identificación, análisis y valoración de riesgos que permita tomar decisiones de manera oportuna con el fin de generar estrategias para su mitigación y aportando al fortalecimiento de la cultura de innovación y confianza para garantizar una atención digna, respetuosa y diferencial a las víctimas."

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.

Nivel de Aceptación del Riesgo: La Unidad para la Atención y Reparación Integral a las Víctimas ha establecido que para los riesgos de gestión el nivel de aceptación es para todos los riesgos que se ubiquen en un nivel bajo, ya que los controles son suficientes y nivel de riesgo sería aceptable. Para los riesgos de corrupción no se establece nivel de aceptación, ya que siempre deben conducir a un tratamiento.

Nivel para calificar el impacto: Según la Metodología de Administración de riesgo en la etapa de valoración del riesgo debe analizarse y evaluarse la probabilidad y el impacto del riesgo. Para la calificación del impacto se tiene establecidas tablas de calificación (Cualitativa y cuantitativa) en las cuales podemos encontrar los niveles 1. Insignificante, 2. Menor, 3. Moderado, 4. Mayor y 5. Catastrófico, esta información se explica de manera más amplia en el apartado 3.3 de este documento.

Tratamiento del riesgo: Culminada la etapa de valoración se establece un plan de tratamiento que requiere establecer una medida de tratamiento, acciones, meta, duración, periodicidad y responsable. Las medidas de tratamiento contempladas son evitar, Reducir, Compartir o transferir y asumir el riesgo esta información se explica de manera más amplia en el apartado 4 de este documento.

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

La Unidad para las Víctimas determina que:

El seguimiento del mapa de riesgos institucional lo realizará la oficina de Control Interno y tendrá una periodicidad cuatrimestral con corte a 30 de abril, 31 de agosto y 31 de diciembre de la vigencia correspondiente.

El monitoreo a la materialización de los riesgos es responsabilidad de los procesos o direcciones territoriales y sus respectivos líderes y se realizará mensualmente de acuerdo con el procedimiento. En caso de materialización de los riesgos es responsabilidad de los servidores informar al enlace del proceso o dirección territorial, quien a su vez debe realizar el reporte correspondiente.

La revisión y actualización de los mapas de riesgos de hará dos veces al año de acuerdo con el cronograma establecido para ello con el acompañamiento del Equipo de riesgos, crisis y comunicaciones estratégicas. Estas etapas de la metodología serán tratadas a mayor detalle en el capítulo 3 de este documento.

3. Etapas de la administración del riesgo

3.1 Establecimiento del contexto

La definición del contexto estratégico se refiere a la identificación de los aspectos o factores internos (contexto interno) y externos (contexto externo), que pueden afectar positiva o negativamente a la entidad. A partir de estos aspectos se establecen las causas de los riesgos a identificar que pueden afectar el cumplimiento de sus objetivos y los posibles planes de tratamiento. Para el desarrollo de este ejercicio la Unidad a establecido la "Guía para la construcción del contexto estratégico".

3.2 Identificación del Riesgo

La identificación de los riesgos se realiza determinando las causas, consecuencias y tipo de riesgo, para esta identificación se tendrán en cuenta distintas fuentes entre ellas: el análisis de contexto del proceso o dirección territorial, procedimientos, caracterizaciones, indicadores entre otros, con el fin de establecer posibles fuentes de riesgo y eventos que pueden afectar el logro de los objetivos.

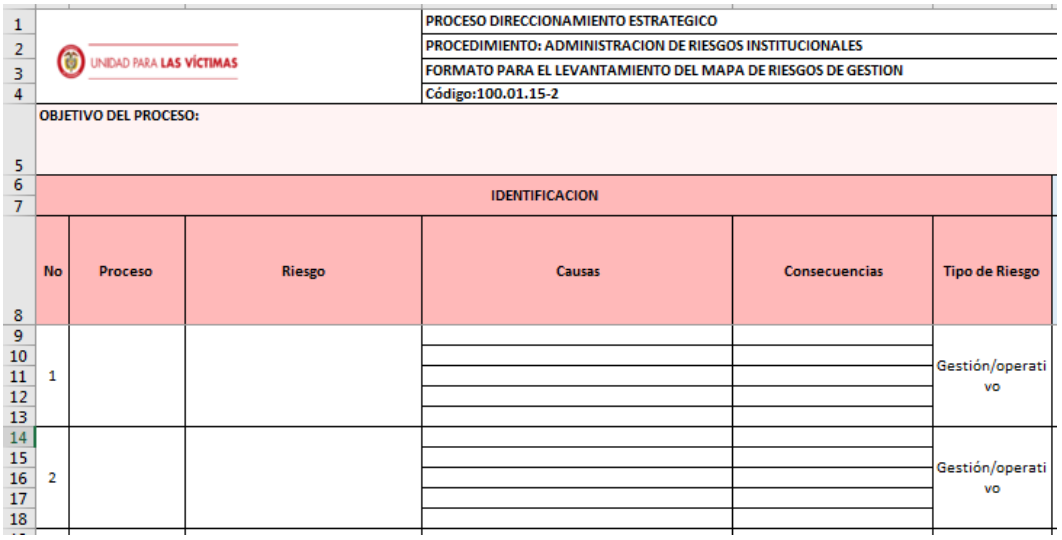
Para realizar la identificación del riesgo es necesario:

1. Entender el proceso o dirección territorial y su funcionamiento
2. Identificar los objetivos o metas
3. Identificar factores críticos de éxito: Un Factor crítico de éxito es algo que debe ocurrir para conseguir un objetivo y se considera crítico si su cumplimiento es absolutamente necesario para cumplir los objetivos de la entidad.
4. Identificar "qué puede fallar" para cada proceso o dirección territorial, Se deben identificar actividades claves.

Para realizar la identificación del riesgo se pueden responder las siguientes preguntas:

1. *¿Qué puede suceder? – Descripción del riesgo*
2. *¿Por qué puede suceder? – Causas*
3. *¿Qué pasaría si sucede? ¿Qué consecuencia tendría tu materialización? – Consecuencias*

En el formato…



1	UNIDAD PARA LAS VÍCTIMAS		PROCESO DIRECCIONAMIENTO ESTRATEGICO			
2			PROCEDIMIENTO: ADMINISTRACION DE RIESGOS INSTITUCIONALES			
3			FORMATO PARA EL LEVANTAMIENTO DEL MAPA DE RIESGOS DE GESTION			
4			Código:100.01.15-2			
5	OBJETIVO DEL PROCESO:					
6	IDENTIFICACION					
7						
8	No	Proceso	Riesgo	Causas	Consecuencias	Tipo de Riesgo
9						
10						
11	1					Gestión/operativo
12						
13						
14						
15						
16	2					Gestión/operativo
17						
18						

***Importante

Para la identificación de los riesgos de corrupción, se deben identificar los procedimientos o tareas que cuenten con los siguientes factores críticos, ya que su presencia puede aumentar la posibilidad de que ocurra un hecho de corrupción:

- Oportunidad: Se refiere a las fallas de diseño del procedimiento donde se abren espacios de discrecionalidad de los servidores que pueden generar espacios de corrupción. Está asociado a la falta de controles internos y externos que sean efectivos.
- Presión: Se refiere al hecho de ejercer influencia/obligar a una persona a tomar una decisión o a realizar una acción. Con respecto a lo hechos de corrupción puede darse por actores criminales o situaciones de presión económica y social para la ejecución de trámites o procedimientos al interior de la entidad. Esto se presenta generalmente por una actitud del individuo que justifica actos por fuera de la integridad pública bajo una valoración de ética por fuera de la finalidad de los principios del servicio público.
- Responsabilidad: Se refiere a las fallas en la ética, integridad, cumplimiento y compromiso con lo público, afectando el cumplimiento del objetivo de la entidad.

Para los riesgos de Seguridad y salud en el trabajo se usará como insumo para la identificación la Matriz de Identificación de Peligros, Valoración del Riesgo y Determinación de Controles la cual se explica a mayor detalle en el anexo 2 del presente documento.

Para los riesgos de Seguridad de la información se como insumo para la identificación de los riesgos a nivel institucional de acuerdo con el anexo 3 del presente documento.

a. Descripción del riesgo

En necesario hacer una corta descripción del riesgo dentro de la identificación. Es importante centrarse en los riesgos más significativos para la entidad relacionados con los objetivos o metas del proceso o dirección territorial y los objetivos estratégicos.

Para la redacción del riesgo se deben tener en cuenta:

- Usar un lenguaje claro y común
- La ausencia de control no es un riesgo
- Evite usar palabras negativas como "No", "Que no", o con palabras que denoten un factor de riesgo "Causa", tales como "Falta de", "Ausencia de", "Falta de", "Poco(a)", "Escaso(a)", "Insuficiente", "Deficiente", "Debilidad en".

b. Determinación de las causas

Las causas son los medios, circunstancias y/o agentes que generan el riesgo identificado o que propician su materialización. Estas causas deben ser identificadas en el análisis del contexto del proceso o como parte del análisis para la identificación del riesgo:

- Internas (Debilidades): Atribuidas a personas, métodos, equipos, materiales e instalaciones, directamente involucradas en el proceso, es decir debilidades de la entidad.

- Externas (Amenazas): Cuando provienen del entorno en el que se desarrolla el proceso, que tiene que ver con agentes externos a la entidad.

*** **Importante** pueden existir causas sobre las cuales no existan controles sin embargo deben ser identificadas.

Una clave para redactar las causas es el uso de las palabras: falta de, ausencia de, fallas de, exceso de, etc. Palabras que conducen a deficiencias que pueden propiciar o permitir la ocurrencia de los riesgos. Un ejemplo de causas puede ser: Falta de recursos físicos y humanos para el desarrollo del proceso, falta de controles al interior del proceso, fallas de los aplicativos, incumplimiento de los protocolos de seguridad.

c. Determinación de las consecuencias

Las consecuencias son los efectos de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente, se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Para el caso de la Unidad, se contemplan algunas categorías como guía para determinar las consecuencias: salud de personas, seguridad en las personas, credibilidad o imagen, operacional, seguridad en la información, legal y otros.

- **Afectación en la integridad de las personas.** En caso de materializarse, podría afectar la salud o la vida de los servidores públicos y/o contratistas que laboran en la Entidad.
- **Afectación en la credibilidad o imagen.** En caso de materializarse, podría afectar la credibilidad y buen nombre de la Entidad frente a las partes interesadas o dentro de la Entidad.
- **Operativa.** En caso de materializarse, podría afectar el desarrollo normal, generando retrasos o incumplimiento en sus actividades, entre otros, fallas en los sistemas de información, desconocimiento de un procedimiento, problemas con la comunidad, etc.
- **Legal.** En caso de materializarse, la Unidad podría enfrentar consecuencias de tipo legal debido al incumplimiento de su función administrativa, ejecución presupuestal y normatividad aplicable.
- **Disciplinaria**: En caso de materializarse, podría generar sanciones disciplinarias

***importante:** Las consecuencias no tienen relación uno a uno con las causas del riesgo, ya que una o varias causa pueden ocasionar un riesgo y la materialización de este a su vez puede ocasionar una o varias consecuencias.

d. Tipos de riesgos

En la identificación del riesgo es necesario establecer el tipo de riesgo al cual nos enfrentamos, la Unidad sugiere algunos tipos de riesgos, los cuales se describen a continuación:

- **Riesgo de Operativos**: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la estructura de la entidad, de la articulación entre dependencias, procesos y/o direcciones territoriales.
- **Riesgos de seguridad de la información**: Son potenciales amenazas que pueden detonar una vulnerabilidad de un activo de información afectando su Integridad, confidencialidad y disponibilidad.

- **Riesgos de seguridad y salud en el trabajo**: Es la probabilidad de que un objeto material, sustancia o fenómeno pueda potencialmente desencadenar perturbaciones en la salud o integridad física del personal, así como en materiales y equipos.

- **Riesgos ambientales**: Es el riesgo que se puede presentar en forma de "perturbación" causada por la actividad (o inactividad) humana que lleva a la degradación o a la pérdida de la sostenibilidad.

- **Riesgos de públicos**. El riesgo de seguridad personal 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. Estos riesgos son una categoría especial de los riesgos de gestión que por su naturaleza estratégica serán trabajados e identificados desde la Alta dirección. Para efectos de la metodología estos riesgos solo se diferencian en la etapa de análisis de riesgo razón por la cual este tema se desarrollará en el anexo 2 del presente documento.

- **Riesgos de corrupción**. Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

3.3. Valoración de los riesgos (Riesgos de Operativos, Seguridad de la información, Seguridad y salud en el trabajo, ambientales, públicos)

La valoración del riesgo consiste en establecer la zona de riesgo inicial (Riesgo Inherente), los controles y su nivel de efectividad y finalmente obtener la zona de riesgo final (Riesgo residual).

En el formato….

RIESGO INHERENTE				CONTROLES			RIESGO RESIDUAL			
Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo	Descripción	Correctivo-Impacto Preventivo-Probab.	Calificación De 0 a 50 = 0 De 51 a 75=1 De 76 a 100 = 2	Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo
		0				0			0	
						0				
						0				
						0				
						0				
		0				0			0	
						0				
						0				
						0				
						0				

3.3.1. Análisis del Riesgo

El análisis de riesgo busca establecer la zona de riesgo inicial probabilidad de ocurrencia del riesgo y su impacto. Con el fin de estimar la zona de riesgo inicial, denominada riesgo inherente; Primero se determina la probabilidad entendida como la posibilidad de ocurrencia del riesgo; segundo se determinan las consecuencias o nivel de impacto que puede ocasionar la materialización del riesgo y finalmente se estima el nivel de riesgo inherente.

a. Calificación de la probabilidad

La probabilidad es la posibilidad de ocurrencia de un evento de riesgo y se mide según su frecuencia, es decir el número de veces en que pudo haberse presentado el evento en un periodo determinado. La frecuencia depende del proceso o dirección territorial y de la disponibilidad de datos históricos sobre el riesgo, en caso de que no exista se evaluará de acuerdo con la experiencia de los servidores.

La probabilidad para los riesgos operativos, riesgos de seguridad de la información, riesgos ambientales y riesgos de seguridad y salud en el trabajo se califica de acuerdo con la siguiente tabla, ubicando el nivel de probabilidad que aplique al riesgo identificado de acuerdo con la descripción y la frecuencia del riesgo:

Tabla calificación de la probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en cualquier momento.	A l menos una vez al mes
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos cada dos meses.
3	Posible	El evento posiblemente ocurra en algún momento	Al menos 1 en el semestre.
2	Improbable	El evento no es probable que ocurra.	Al menos 1 vez en el último año.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (Poco comunes o anormales).	No se ha presentado en el último año.

Fuente: Oficina de Planeación

b. Calificación del impacto

El impacto es el nivel de afectación (efectos) que puede generar la materialización del riesgo y se debe calificar a partir de las consecuencias que genere. Para los riesgos de operativos, riesgos de seguridad de la información, riesgos ambientales y riesgos de seguridad y salud en el trabajo el Impacto se califica de acuerdo con la siguiente tabla ubicando el nivel de impacto que aplique al riesgo identificado de acuerdo con los efectos generados:

Tabla calificación del Impacto[3]

Niveles para calificar el Impacto	Escala	IMPACTO (Efectos)
CATASTRÓFICO	5	1- Interrupción de las operaciones de la Entidad por más de Cinco (5) días. 2- Intervención por parte de un ente de control u otro ente regulador. 3- Pérdida de Información crítica para la entidad que no se puede recuperar. 4- Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. 5- Imagen institucional afectada en el orden nacional o territorial por actos o hechos de corrupción comprobados. 6- Impacto que afecta la ejecución presupuestal en un valor mayor o igual al 50%. 7- Pérdida de cobertura en la prestación de los servicios a las victimas mayor o igual al 20%. 8- Pago de indemnizaciones a terceros por acciones legales.
MAYOR	4	1- Interrupción de las operaciones de la Entidad por más de dos (2) días. 2- Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. 3- Sanción por parte del ente de control u otro ente regulador. 4- Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. 5- Imagen institucional afectada en el orden nacional o territorial por incumplimientos en la prestación del servicio a los usuarios o ciudadanos. 6- Impacto que afecte la ejecución presupuestal en un valor mayor o igual al 10%. 7- Pérdida de cobertura en la prestación de los servicios a las víctimas mayor o igual al 10%. 8- Pago de indemnizaciones a terceros por acciones legales

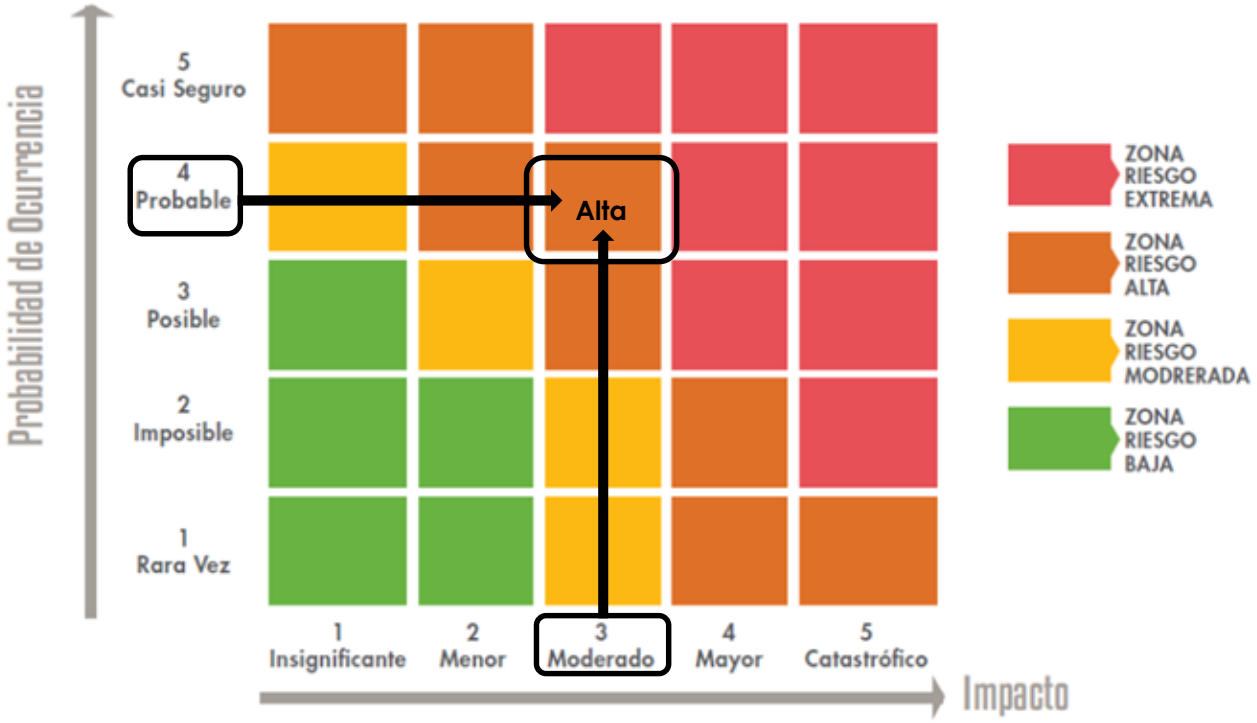
[3] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

MODERADO	3	1- Interrupción de las operaciones de la Entidad por un (1) día. 2- Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. 3- Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. 4- Reproceso de actividades y aumento de carga operativa. 5- Imagen institucional afectada en el orden nacional o territorial por retrasos en la prestación del servicio a los usuarios o ciudadanos. 6- Investigaciones penales, fiscales o disciplinarias. 7- Impacto que afecte la ejecución presupuestal en un valor mayor o igual al 5%. 8- Pérdida de cobertura en la prestación de los servicios a las víctimas mayores o igual al 5%.
Menor	2	1- Interrupción de las operaciones de la Entidad por algunas horas. 2- Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. 3- Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. 4- Impacto que afecte la ejecución presupuestal en un valor menor al 5%. 5- Pérdida de cobertura en la prestación de los servicios a las víctimas menor al 5%.
Insignificante	1	1- No hay interrupción de las operaciones de la entidad. 2- No se generan sanciones económicas o administrativas. 3- No se afecta la imagen institucional de forma significativa. 4- No hay impacto significativo en el presupuesto. 5- Pérdida de cobertura en la prestación de los servicios a las víctimas menor o igual al 1%. 6- No hay pago de indemnizaciones a terceros. 7- No hay Sanciones por incumplimiento

c. Determinación del riesgo inherente

Para estimar el nivel de riesgo inicial, los valores determinados para la probabilidad y el impacto se cruzan en la siguiente matriz de riesgo, con el fin de determinar la zona de riesgo en la cual se ubica el riesgo identificado. Este primer análisis del riesgo se denomina Riesgo Inherente y se define como aquél al que se enfrenta una entidad en ausencia de controles

Tabla calificación riesgos de gestión[4]



3.3.2. Evaluación del riesgo

En esta fase se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final o riesgo residual.

a. Evaluación de controles

Los controles son todas las medidas diseñadas (Procesos, políticas, dispositivos, practicas u otra acción existente) que permita detectar/prevenir la probabilidad y/o minimizar el impacto que pueda generar la materialización del riesgo.

1) Determinar el control: Se debe establecer cuál es el control que se están ejecutando

En la evaluación de los controles se deben Identificar cuáles son los controles existentes, los responsables de ejecutarlos, el objetivo del control, como se llevan a cabo, cual es la evidencia de su ejecución, cuales el tipo de control. Para la descripción del control es necesario incluir las siguientes variables que permiten evaluar el adecuado diseño del control:

[4] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

- **Quien lleva a cabo el control**: Responsable de ejecutarlo (cargo/subproceso al que pertenece o Sistema o aplicativo). Si el control lo ejecuta una persona debe tener autoridad, conocimiento y competencias para ejecutar el control, Si el control es automático por medio de una aplicación o sistema, se debe hacer referencia al mismo.
- **Cada cuanto se lleva a cabo el control:** Periodicidad /frecuencia (mensual, bimensual, trimestral, semestral, anual), esta debe ser suficiente y oportuna para prevenir o detectar el riesgo.
- **Que busca hacer el control**: Objetivo o propósito del control, el cual debe conducir a prevenir las causas que generan el riesgo o a detectar la materialización del riesgo.
- **Como se lleva a cabo**: Como se hace el control.
- **Excepciones y observaciones:** Se debe hacer referencia al procedimiento a seguir en caso de no cumplirse con el control, aclaraciones sobre excepciones en el cumplimiento del control y se debe indicar cualquier tipo de observación a que haya lugar con respecto al control.
- **Cuál es la evidencia de la ejecución del control:** Soporte o evidencia de la ejecución del control.

2) Determinar su naturaleza: Se debe establecer si el control es preventivo o correctivo

Control Preventivo. Se establece para evitar que el evento suceda o minimizar el efecto de su materialización.

Algunos controles preventivos pueden ser:

- Acceso restringido.
- Procedimientos formales aplicados.
- Claves de acceso.
- Condiciones contractuales.
- Distribución de funciones.
- Estandarización - SGC - Sistema documental.
- Firmas autorizadas.
- Gestión de proyectos.
- Inspección y procesos de control.
- Instructivos y guías.
- Investigación y desarrollo, desarrollo tecnológico.
- Mantenimiento preventivo.
- Medicina preventiva.
- Políticas de seguridad.
- Programa de selección de personal.
- Programas de capacitación y entrenamiento.
- Revisión formal de requisitos, especificaciones, diseño, ingeniería y operaciones.
- Rotación de funciones.
- Acuerdos de confidencialidad

Control Correctivo. Está dirigido a identificar el evento o resultado no previsto después de que se haya producido. Busca detectar el evento para corregirlo y se tomen acciones al respecto. Algunos controles correctivos pueden ser:

- Control de calidad
- Supervisión

3) **Determinar si los controles están documentados:** Establecer si el control se encuentra o no documentado, conocer cómo se lleva a cabo el control, quién es el responsable de su ejecución y cuál es la periodicidad para su ejecución, lo cual determinará las evidencias que van a respaldar la ejecución del mismo.

4) **Establecer si el control que se implementa:** Es automático o manual.

- **Controles automáticos**: Son aquellos que utilizan herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación entre otros. Este tipo de controles suelen ser más efectivos en algunos ámbitos, dados su complejidad.

- **Controles manuales:** Procedimientos y políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.

***Importante** para una adecuada mitigación de las causas del riesgo este debe ejecutarse de acuerdo con los establecido, de lo contrario no estaría bien diseñado

En este formato …

Para realizar la evaluación de los controles, se ha determinado el siguiente cuestionario, el cual está incluido en el formato para el levantamiento del mapa de riesgos en la hoja "Controles".

Luego de diligenciar la información del mapa de riesgos se debe continuar con la calificación de los controles de la siguiente manera:

1. Se debe identificar en el formato el riesgo a calificar en la hoja de controles
2. Se deben responder las preguntas determinando si la respuesta es SI o NO

En caso de que la respuesta sea NO se debe colocar 0 "cero" en la casilla correspondiente al control que estamos calificando.
En caso de que la respuesta sea SI se debe colocar el valor que se encuentra en la casilla que se encuentra frente a la pregunta.

Evaluación de los controles

		RIESGO 1	
		Control 1.1	Control 1.2
RIESGO 1		control 1	0
Preguntas	**VALOR**	**CALIFICACIONES**	**CALIFICACIONES**
¿Existen manuales, instructivos o procedimientos para el manejo del control?	15	0	
¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5	NO 0	
¿El control es automático?	15	0	
¿El control es manual?	10	10	
¿La frecuencia de ejecución del control y seguimiento es adecuada?	15	15	
¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10	SI 10	
¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30	30	
TOTAL	100	65	0

Fuente Oficina de Planeación

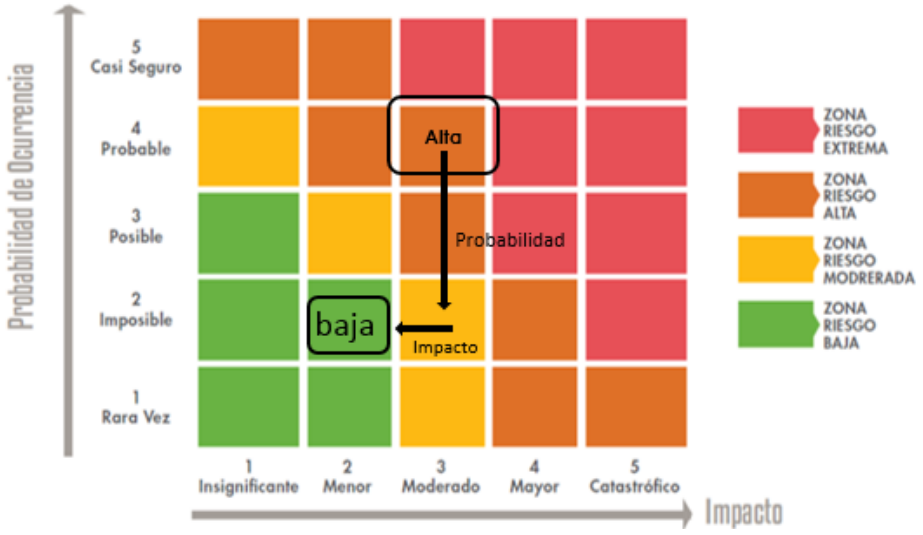
b. Determinación del Riesgo Residual

Aquí se comparan los resultados obtenidos del riesgo inherente con los controles establecidos, para establecer la zona del riesgo final o riesgo residual.

De acuerdo con el resultado obtenido en la calificación de los controles podemos disminuir el nivel de probabilidad(preventivo) o impacto(correctivo), en 1,2,3 niveles en la tabla de calificación de acuerdo con lo siguiente:

Rangos de calificación de los controles	Cuadrantes a disminuir
Entre 0-50	0
Entre 51-75	1
Entre 76-100	2

RIESGO RESIDUAL



- Si el control es preventivo se disminuye únicamente la probabilidad en el número de cuadrantes de acuerdo con la calificación obtenida por el control.

- Si el control es correctivo se disminuye únicamente el Impacto en el número de cuadrantes de acuerdo con la calificación obtenida por el control.

Si el control no genera ningún efecto en la probabilidad o impacto, debe ser eliminado o en su defecto debe generarse una acción en el plan de respuesta que permita en el futuro mejorar su calificación.

*** **importante** Si existen más de dos controles del mismo tipo el valor de la disminución será un promedio de la calificación de los controles.

En el formato ...

RIESGO INHERENTE				CONTROLES			RIESGO RESIDUAL			
Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo	Descripción	Correctivo-Impacto Preventivo-Probab.	Calificación De 0 a 50 = 0 De 51 a 75=1 De 76 a 100 = 2	Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo
4	4	16	Extrema	control 1	Correctivo	65	4	3	12	Alta
						0				
						0				
						0				
						0				
						0				

3.3.3 Construcción del mapa de riesgos de Gestión

La información sobre los resultados de las etapas de Identificación y valoración, así como la información sobre el plan de respuesta, se registran el formato para el levantamiento de mapa de riesgos del proceso o dirección territorial, de la siguiente manera:

Identificación del riesgo:

- Se debe seleccionar el nombre del proceso o dirección territorial (lista desplegable)
- Se debe hacer una descripción breve del riesgo
- Se debe determinar las causas
- Se debe seleccionar las consecuencias (lista desplegable)
- Se debe determinar el tipo de riesgo (lista desplegable)

Riesgo Inherente:

- Se debe seleccionar el valor de la probabilidad (lista desplegable)
- Se debe seleccionar el valor de la Impacto (lista desplegable)
- El nivel de riesgo se calcula automáticamente
- Se debe seleccionar la zona de riesgo (lista desplegable)

Evaluación de controles

- Se debe diligenciar la descripción del control incluyendo: Quien lo hace, cada cuanto lo hace, cuando lo hace, que se hace, como se hace, excepciones y observaciones y la evidencia que queda de la ejecución del control.
- Se debe seleccionar si el control es preventivo o correctivo (lista desplegable)
- Se deben responder las preguntas de la hoja "controles" y esta automáticamente calcula el valor de la calificación.

Riesgo residual

- Se debe seleccionar el valor de la probabilidad (lista desplegable)
- Se debe seleccionar el valor de la Impacto (lista desplegable)
- El nivel de riesgo se calcula automáticamente
- Se debe seleccionar la zona de riesgo (lista desplegable)

Plan de respuesta

- Se debe seleccionar la medida de tratamiento (lista desplegable)
- Se debe establecer la acción o acciones a tomar frente al riesgo cantidad y periodicidad (1 diaria, 3 semanal, 2 mensual, 1 bimensual, 1 trimestral, 1 semestral etc.)
- Se debe establecer una fecha de Inicio de las acciones o actividades (Esta fecha hace referencia a la fecha en la cual se desarrollará por primera vez la actividad)
- Se debe establecer un periodo durante el cual se le dará cumplimiento a las acciones o actividades en meses y preferiblemente dentro de la vigencia actual.
- Se debe establecer un responsable frente a la ejecución de las acciones o actividades

3.4 Valoración del Riesgo de Corrupción

Para los riesgos de corrupción fue necesario desarrollar la etapa de valoración del riesgo en un capítulo independiente, ya que en esta existen algunas diferencias en la metodología entre los riesgos de gestión y los de corrupción.

El riesgo de corrupción es la posibilidad que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado[5]. La posibilidad no implica la materialización del riesgo.

Los componentes básicos de un riesgo de corrupción son:

- La existencia de una acción u omisión
- El uso del Poder
- Desviar la gestión de lo público
- Beneficio particular

Al igual que los riesgos de Gestión, para los riesgos de Corrupción el análisis del riesgo implica una combinación del análisis del impacto y la probabilidad. Sin embargo, para los riesgos de corrupción el impacto se valora de manera diferente, ya que solo contempla 3 niveles de impacto.

3.4.1 Análisis del riesgo de corrupción

Esta etapa tiene como principal objetivo determinar la probabilidad de materialización del riesgo y sus consecuencias o impacto y su medición se realiza de acuerdo con los parámetros establecidos por la Guía de gestión de riesgos de corrupción, con el fin de establecer la zona de riesgo inicial o riesgo inherente.

a. Calificación de la probabilidad

La probabilidad es la posibilidad de ocurrencia de un evento de riesgo y se mide según su frecuencia, es decir el número de veces en que pudo haberse presentado el evento en un periodo determinado. La probabilidad de se califica de acuerdo con los siguientes parámetros:

Calificación del Riesgo de Corrupción - Probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Existe la posibilidad que se haya presentado más de una vez en el Último año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Existe la posibilidad que se haya presentado una vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento	Existe la posibilidad que se haya presentado una vez en los últimos 2 años.

[5] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

2	Improbable	El evento puede ocurrir en algún momento	Existe la posibilidad que se haya presentado una vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (Poco comunes o anormales).	Existe la posibilidad que no se haya presentado en los últimos 5 años.

Fuente Oficina de Planeación

b. Calificación del impacto

El impacto es la consecuencia o efecto que puede generar la materialización del riesgo. Los riesgos de corrupción siempre generan un impacto negativo para las Entidades; por esa razón para este tipo de riesgos no aplican las categorías de calificación (1) insignificante o (2) menor señalados en la Guía de Función Pública para los riesgos de Gestión.

Para los riesgos de corrupción el Impacto se califica de acuerdo con los siguientes parámetros:

- **Moderado:** Genera medianas consecuencias sobre la entidad.
- **Mayor:** Genera altas consecuencias sobre la entidad.
- **Catastrófico:** Genera consecuencias desastrosas para la entidad.

Para determinar la calificación del impacto se debe responder "si = 1" o "no = 0" a las preguntas que se encuentra en el formato para el levantamiento del mapa de riesgos de corrupción de la unidad en la hoja "Impacto".

Riesgo 1		
Nº	Pregunta	Respuesta
	Si el riesgo de corrupción se materializa podría...	SI "1"
1	¿Afectar al grupo de funcionarios del proceso?	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	
3	¿Afectar el cumplimiento de la misión de la Entidad?	
4	¿Afectar el cumplimiento de la misisón del sector al que pertenece la Entidad?	
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	
6	¿Generar pérdida de recursos económicos?	
7	¿Afectar la generación de los productos o la prestación de servicios?	
8	¿Dar lugar al detrimento de la calidad de vida de los comunidad por la pérdida del bien o servicios o los recursos públicos?	
9	¿Generar pérdida de la información de la Entidad?	
10	¿Generar intervención de los órganos de control, de la Fiscalia 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 pérdida de credibilidad del sector?	
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?	
17	¿Afectar la imagen regional?	
18	¿Afectar la imagen nacional?	
	Puntaje	0
	Impacto	**0**
De (1-5)Moderado = 5 (6-11)Mayor = 10 (12-18)Catastrófico = 20		

Fuente Oficina de Planeación

El resultado de las preguntas se evaluará así:

Calificación del Riesgo de Corrupción - Impacto[6]

Calificación de Riesgo de Corrupción Impacto		
Respuestas	**Descripción**	**Nivel**
1-5	Moderado	5
6-11	Mayor	10
12-18	Castrófico	20

c. Determinación del riesgo inherente

Luego de obtenida el resultado de la calificación de la probabilidad y el impacto, se realiza la multiplicación del puntaje de la probabilidad por el puntaje del impacto para obtener el riesgo inherente, este resultado se ubica en una de las cuatro (4) zonas de riesgo que a continuación se describen:

Resultados de la calificación del Riesgo de Corrupción[7]

Resultados de la calificación del Riesgo de Corrupción				
Probabilidad	**Puntaje**	**Zonas de riesgo de corrupción**		
Casi seguro	5	25 Moderada	50 Alta	100 Extrema
Probable	4	20 Moderada	40 Alta	80 Extrema
Posible	3	15 Moderada	30 Alta	60 Extrema
Improbable	2	10 Baja	20 Moderada	40 Alta
Rara vez	1	5 Baja	10 Baja	20 Moderada
Impacto		Moderado	Mayor	Catastrófico
Puntaje		5	10	20

PROBABILIDAD

IMPACTO

Zona de Riesgo Baja: De 5 a 10 puntos.

- Probabilidad: Rara vez o improbable.

[6] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)
[7] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

- Impacto: Moderado y Mayor.
- Tratamiento: Los riesgos de corrupción de las zonas baja se encuentran en un nivel que puede eliminarse o reducirse fácilmente con los controles establecidos en la entidad.

Zona de Riesgo Moderada: De 15 - 25 puntos.

- Probabilidad: Rara vez, Improbable, Posible, Probable y Casi Seguro.
- Impacto: Moderado, Mayor y Catastrófico.
- Tratamiento: Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Baja o eliminarlo.

Zona de Riesgo Alta: De 30 - 50 puntos.

- Probabilidad: Improbable, Posible, Probable y Casi Seguro.
- Impacto: Mayor y Catastrófico.
- Tratamiento: Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Moderada, Baja o eliminarlo.

Zona de Riesgo Extrema: De 60 - 100 puntos.

- Probabilidad: Posible, Probable y Casi Seguro.
- Impacto: Catastrófico.
- Tratamiento: Los riesgos de corrupción de la Zona de Riesgo Extrema requieren de un tratamiento prioritario. Se deben implementar los controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección.

3.4.2 Evaluación del riesgo de corrupción

En esta etapa se evalúan los controles que se encuentran establecidos para cada riesgo y de acuerdo con el puntaje obtenido, se reduce la zona de riesgo en la que se encuentra ubicado el riesgo inherente obteniendo como resultado el riesgo residual.

a. Evaluación de controles

Para la evaluación de los controles se deben determinar los siguientes factores:

- Determinar la naturaleza de los controles: Preventivos o correctivos.
- Determinar si los controles están documentados
- Determinar las clases de controles: Manuales o automáticos

Para la realización de esta evaluación se ha determinado el siguiente cuestionario, el cual está incluido en el formato para el levantamiento del mapa de riesgos de corrupción de la unidad en la hoja “Controles”.

Evaluación controles del Riesgo de Corrupción

De 0 a 50 = 0 De 51 a 75=1 De 76 a 100 = 2						
RIESGO 1						
0		**Control 1.1**	**Control 1.2**	**Control 1.3**	**Control 1.4**	**Control 1.5**
		0	0	0	0	0
¿El control previene la materialización del riesgo (afecta probabilidad- Preventivo), ¿El control permite enfrentar la situación en caso de materialización, (afecta impacto - Correctivo)?		0	0	0	0	0
Calificaciones	**VALOR**	**SI**	**SI**	**SI**	**SI**	**SI**
¿Existen manuales, instructivos o procedimientos para el manejo del control?	15					
¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5					
¿El control es automático?	15					
¿El control es manual?	10					
¿La frecuencia de ejecución del control y seguimiento es adecuada?	15					
¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10					
¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30					
TOTAL	100	0	0	0	0	0

Fuente Oficina de Planeación

b. Determinación del Riesgo Residual

Se comparan los resultados obtenidos del riesgo inherente con los controles establecidos, para Establecer la zona del riesgo final o riesgo residual. Se califica de acuerdo con la siguiente tabla.

Calificación de los Controles[8]

Calificación de los controles	Puntaje a disminuir
De 0 a 50	0
De 51 a 75	1
De 76 a 100	2

Con la calificación obtenida se realiza un desplazamiento en la matriz, así:

- Si el control es correctivo afecta el impacto se disminuye a la izquierda.
- Si el control es preventivo afecta la probabilidad se disminuye hacia abajo.

Si el control no genera ningún efecto en la probabilidad o impacto, debe ser eliminado o en su defecto debe generarse una acción en el plan de respuesta que permita en el futuro mejorar su calificación.

[8] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

Nota:

*Si existen más de dos controles del mismo tipo el valor de la disminución será un promedio de la calificación de los controles.

Resultados de la calificación de los controles[9]

Resultados de la calificación del Riesgo de Corrupción				
Probabilidad	**Nivel**	**Zonas de riesgo de corrupción**		
Casi seguro	5	←		
Probable	4	←		
Posible	3	←		
Improbable	2	←		
Rara vez	1	←		
Impacto		Moderado	Mayor	Catastrófico
Nivel		3	4	5

Si afecta el impacto se desplaza a la izquierda

IMPACTO

PROBABILIDAD

Resultados de la calificación del Riesgo de Corrupción				
Probabilidad	**Nivel**	**Zonas de riesgo de corrupción**		
Casi seguro	5			
Probable	4			
Posible	3			
Improbable	2			
Rara vez	1	↓	↓	↓
Impacto		Moderado	Mayor	Catastrófico
Nivel		3	4	5

Si afecta la probabilidad se desplaza hacia abajo.

3.4.3 Mapa de riesgos de corrupción

La información sobre los resultados de las etapas de Identificación, valoración y seguimiento, así como la información sobre el plan de respuesta, se registran el formato para el levantamiento de mapa de riesgos de corrupción del proceso o dirección territorial de la siguiente manera:

Identificación del riesgo:

- Se debe seleccionar el nombre del proceso o dirección territorial (lista desplegable)
- Se debe hacer una descripción breve del riesgo

[9] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

- Se debe determinar las causas
- Se debe seleccionar las consecuencias (lista desplegable)
- Tipo de riesgo predeterminado como riesgo de corrupción

Riesgo Inherente:

- Se debe registra el valor de la probabilidad
- Se debe registra el valor del impacto de acuerdo con el resultado de la hoja "Impacto".
- El nivel de riesgo se calcula automáticamente
- La zona de riesgo se muestra automáticamente

Evaluación de controles

- Se debe diligenciar la descripción del control incluyendo: Quien lo hace, cada cuanto lo hace, cuando lo hace, que se hace, como se hace y la evidencia que queda de la ejecución del control.
- Se debe seleccionar si el control es preventivo o correctivo (lista desplegable)
- Se deben responder las preguntas de la hoja "controles" y esta automáticamente calcula el valor de la calificación.

Riesgo Residual

- Se debe seleccionar el valor de la probabilidad o Impacto, luego de la disminución.
- El nivel de riesgo se calcula automáticamente
- La zona de riesgo se muestra automáticamente

Plan de respuesta

- Se debe seleccionar la medida de tratamiento (lista desplegable)
- Se debe establecer la acción o acciones a tomar frente al riesgo y la periodicidad con la cual se desarrollarán (diaria, semanal, mensual, bimensual, trimestral, semestral etc.)
- Se debe establecer una fecha de Inicio de las acciones o actividades (Esta fecha hace referencia a la fecha en la cual se desarrollará por primera vez la actividad)
- Se debe establecer un periodo durante el cual se le dará cumplimiento a las acciones o actividades en meses y preferiblemente dentro de la vigencia actual.
- Se debe establecer un responsable frente a la ejecución de las acciones o actividades

Mapa de riesgos de corrupción[10]

FORMATO PARA EL LEVANTAMIENTO DEL MAPA DE RIESGOS DE CORRUPCIÓN DE LA UNIDAD
PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO
Procedimiento de Administración de Riesgos Institucionales y de Proceso

IDENTIFICACION						RIESGO INHERENTE				CONTROLES			RIESGO RESIDUAL				PLAN DE RESPUESTA AL RIESGO (PROCESO)						
No	Proceso	Riesgo	Causas	Consecuencias	Tipo de riesgo	Probabilidad	Impacto	Nivel Riesgo	Zona de Ries	Descripción	Correctivo-Impacto Preventivo-Probab.	Calificación De 0 a 50 = 0 De 51 a 75=1 De 76 a 100 = 2	Probabilidad	Impacto	Nivel Riesgo	Zona de Ries	Medida de Tratamiento	Acción o Actividades	Meta	Fecha de Inicio	Duración	Responsable	P
1					Corrupción			0	0			0			0	0							
												0											
												0											
												0											
			Otros:									0											
												0											

4. PLAN DE TRATAMIENTO

Una vez culminada la etapa de valoración del riesgo es necesario establecer un plan de tratamiento al riesgo que incluye establecer la medida de tratamiento, las acciones para el manejo de riesgos, la meta, la fecha de inicio, la periodicidad y la duración de la acción y el responsable de ejecutarla.

4.1 Medidas de Tratamiento

- Evitar el riesgo: Esta medida se implica tomar las medidas encaminadas a prevenir su materialización. Se logra cuando al interior de los procesos o direcciones territoriales se generan cambios sustanciales de mejoramiento, rediseño o eliminación de actividades que generan riesgo.

- Reducir el riesgo: Esta medida implica tomar medidas encaminadas a disminuir tanto la probabilidad y el impacto por medio de nuevos controles, para generar que el nivel de riesgo residual disminuya a un nivel tolerable para la entidad.

- Compartir o transferir el riesgo: Esta medida implica reducir el efecto del riesgo compartiendo o transfiriendo a otra parte interesada que pueda gestionarlo de manera más eficaz. Por ejemplo: seguros y tercerización. Sin embargo, la responsabilidad sobre el riesgo permanece en donde se identifica

- Aceptar o Asumir el riesgo Luego de implementar medidas para reducir o evitar puede quedar un riesgo residual bajo, en este caso simplemente acepta y se asume la pérdida residual probable

[10] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

4.2 Acciones o actividades

Estas acciones o actividades del plan de tratamiento deben estar encaminadas a reducir o eliminar las causas originadoras del riesgo y deben planearse de tal manera que puedan convertirse en el futuro en controles que puedan reducir el nivel de riesgo.

Deben ser acciones puntuales y concretas, que tengan evidencia y sean de fácil verificación, por ejemplo, capacitaciones, Informes, Alertas, Mesas de trabajo, Mesas de seguimiento, Creación de formatos, Implementación de controles, reuniones, Generación de acuerdos o alianzas. Se debe evitar el uso de palabras que generen ambigüedad o que no sean de fácil verificación como Articular, Gestionar, Velar, etc.

4.3 Meta, Fecha de inicio, periodicidad, periodo y responsable

Se debe establecer una meta y la fecha en que iniciará la acción la periodicidad con que será realizada (diaria, semanal, mensual, bimensual, trimestral, semestral etc.). Adicionalmente se debe establecer el tiempo durante el cual se llevará a cabo la actividad o actividades, este debe ser suficiente para demostrar su efectividad y en lo posible debe establecer dentro de la vigencia en la cual se realice la actualización del mapa. Finalmente se debe establecer un responsable frente cada actividad del plan de respuesta, esta responsabilidad se puede asignar a un cargo; sin embargo, para los riesgos de corrupción si se hace necesario que esta responsabilidad recaiga en el funcionario o contratista que realice la labor.

- **Meta:** debe tener cantidad y periodicidad. Por ejemplo: 1 reunión mensual, 2 acuerdos en el año, 2 Alianzas (una cada semestre del año), 1 control implementado en el semestre, 4 capacitaciones (una cada trimestre).
- **Fecha de inicio:** Es la fecha a partir de la cual se va a iniciar la acción propuesta.
- **Duración:** Se debe establecer una cantidad de meses durante los cuales se va a realizar la acción. Se recomienda que no superen los 12 meses. Por ejemplo: 6 meses, 3 meses, 12 meses.
- **Responsable:** Para riesgos de corrupción debe relacionarse el nombre propio de la persona que va a realizar la acción o de su jefe en su defecto y para riesgos de gestión puede relacionarse el cargo de la persona que va a realizar la acción o de su jefe.

5. Monitoreo Materialización de los riesgos

El líder del proceso o dirección territorial en conjunto con su equipo es el responsable de monitorear mensualmente la materialización de riesgos y repórtala al Equipo Nacional de Riesgos, crisis y

comunicaciones estratégicas. Este monitoreo se registrará en el Formato de monitoreo de riesgos institucionales y se enviará todos los meses COMR (centro de operaciones y monitoreo de riesgos) al correo comr@unidadvictimas.gov.co.

5.1 Formato de monitoreo a la materialización de riesgos

Este formato debe diligenciarse y remitirse por correo al COMR comr@unidadvictimas.gov.co, todos los meses informando si se materializaron o no los riesgos y es la evidencia de la ejecución de dicha actividad, si el formato no es enviado se asume que el proceso o dirección territorial no está cumpliendo con esta actividad.

UNIDAD PARA LAS VÍCTIMAS	PROCESO DIRECCIONAMIENTO ESTRATEGICO			
	PROCEDIMIENTO: ADMINISTRACION DE RIESGOS INSTITUCIONALES			
	FORMATO DE MONITOREO A LA MATERIALIZACION DE LOS RIESGOS			
	Código:100.01.15-15	Versión: 03	Fecha:	Página 1 de ___

PROCESO O DIRECCION TERRITORIAL		

MONITOREO DEL PROCESO O DIRECCION TERRITORIAL

Riesgo	Tipo de riesgo	Fecha de diligenciamiento	Se materializo? SI o NO	Numero de eventos	Analisis de causas	Corrección	Fecha de creación de las accion	Numero de Acción correctiva

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 SISGESTION, en la ruta Acciones correctivas/Formulación/registro NC/Nueva no conformidad, 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".

6. Revisión y actualización

Esta etapa permite determinar la necesidad de modificar, actualizar o mantener en las mismas condiciones los riesgos, así como su identificación, análisis y valoración[11].

[11] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

6.1 Revisión del Mapa de riesgos

Los líderes de los procesos y direcciones territoriales en conjunto con sus equipos deben revisar y actualizar periódicamente el Mapa de riesgos con el acompañamiento Equipo Nacional de Riesgos, crisis y comunicaciones estratégicas y hacer los ajustes pertinentes. Su importancia radica en la necesidad de asegurar la efectividad de los controles establecidos y la identificación de nuevos riesgos.

En esta fase se debe:

- Identificar riesgos nuevos riesgos en el proceso o dirección territorial.
- Obtener información adicional que permita mejorar la valoración del riesgo.
- Analizar y emprender acciones a partir de los eventos (riesgos materializados), los cambios, las tendencias, los éxitos (Mejoras) y los fracasos(Hallazgos).
- Detectar cambios en el contexto interno y externo.

Para esta revisión se deberá tener en cuenta:

- Riesgos materializados (ver Formato de monitoreo de riesgos de gestión y de corrupción).
- Observaciones, investigaciones disciplinarias, penales, fiscales, o de entes reguladores,
- Hallazgos por parte de la Oficina de Control Interno o de Auditoria externa.
- Cambios importantes en el entorno que den lugar a nuevos riesgos.

6.2 Actualización del mapa de riesgo

De acuerdo con el resultado de la revisión realizada, se verificará si los mapas de riesgos deben ser actualizados o si se mantienen bajo las mismas condiciones en cuanto a factores de riesgo, identificación, análisis y valoración del riesgo. Los aspectos analizados en la revisión deben ser considerados para posibles ajustes o cambios sobre los lineamientos establecidos en la metodología y en la política de riesgos institucional, para fortalecer la administración del riesgo de la Unidad.

6.3 Periodicidad

La revisión y actualización del Mapa de Riesgos por parte de los procesos y/o direcciones territoriales

con el acompañamiento Equipo Nacional de Riesgos, crisis y comunicaciones estratégicas se realizará dos (2) veces al año de acuerdo con la programación establecida.

7. Seguimiento

La Oficina de Control Interno debe adelantar seguimiento a Mapa de Riesgos Institucional. En este sentido es necesario que analicen las causas, los riesgos y la efectividad de los controles incorporados en el Mapa de Riesgos de Corrupción.

El Jefe de Control Interno o quien haga sus veces, es el encargado de verificar y evaluar la elaboración, seguimiento y control del Mapa de Riesgos Institucional.

7.1 Aspectos relevantes en la realización del Seguimiento

En la realización del seguimiento se deben evaluar los siguientes aspectos:

- Revisión de las causas
- Revisión de los riesgos y su plan de respuesta (ejecución y evidencia).
- Revisión de los controles (ejecución y evidencia) y su efectividad, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.
- Revisión al cumplimiento de la tarea de monitoreo a la materialización de los riesgos (ejecución y evidencia).

7.2 Periodicidad

El seguimiento del Mapa de Riesgos se realizará tres (3) veces al año en las siguientes fechas:

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

7.3 Resultados del seguimiento

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en lugar de fácil acceso al ciudadano.

El seguimiento adelantado por la Oficina de Control Interno a los mapas de riesgos debe ser retroalimentado a los líderes de los procesos y/o direcciones territoriales, identificando las falencias y puntos a revisar para que estos a su vez tomen acciones y den respuesta a dichas observaciones.

La Alta dirección o su representante debe analizar estratégicamente los resultados e informes de seguimiento a los mapas de riesgos de la entidad, con el fin de tomar las decisiones requeridas para

la mejora de la gestión del riesgo en la entidad o para actualizar la política de administración del Riesgo.

8. Divulgación, comunicación estratégica y consulta

La NTC ISO 31000 define la comunicación y consulta como un proceso continuo y reiterativo que una organización lleva a cabo para suministrar, compartir y obtener información e involucrarse en un diálogo con las partes interesadas con respecto a la Administración del Riesgo.

La comunicación y consulta son necesarias en cada una de las etapas de la Administración del Riesgo, el cual implica un diálogo con las partes interesadas, con esfuerzos centrados más en la consulta que en la forma de flujo de información desde quien toma la decisión hasta otras partes interesadas. Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o partes interesadas, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para mejorar la prestación del servicio[12].

Para el desarrollo de esta etapa, se harán sesiones de trabajo que el equipo operativo del SIG Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas y al interior de cada proceso o dirección territorial, a través de discusiones técnicas en la que identificarán, analizarán, valorarán los riesgos y definirán acciones que conformen el plan de respuesta al riesgo. Estas discusiones técnicas que se llevarán 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.

La divulgación y consulta de los mapas de riesgos se realizará en la Intranet y la página web de la Unidad. Adicionalmente se realizarán socializaciones de los cambios o actualizaciones de los documentos asociados a la Metodología de riesgos, incluyendo la Metodología de administración de riesgos Institucionales, el procedimiento de administración de riesgos y los mapas de riesgos. Finalmente se establecerán unos protocolos y manuales para el manejo de riesgos, crisis y comunicaciones estratégicos los cuales serán gestionados por el Grupo nacional de manejo de crisis.

9. Roles y Responsabilidades

La entidad ha definido la siguiente matriz de roles y responsabilidades para las etapas de la aplicación de la metodología de Administración de riesgos:

[12] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

Matriz de roles y responsabilidades

Metodologia	Línea Estratégica	Primera linea de defensa	Segunda linea de defensa		Tercera linea de defensa
	Direccion General, Equipo directivo, Equipo de riesgos y comunicaciones estrategicas	**Líder del Proceso**	**Enlace SIG**	**Servidores (s) responsable (s) de la actividad o procedimiento**	**Oficina de Control Interno**
Política para la administración del riesgo.	Determinar los lineamientos para la administración del riesgo en la entidad. Dichos lineamientos deben incluir los aspectos necesarios para la identificación y mitigación de los riesgos. Difundir la política institucional de riesgos a lo largo de toda la organización.	Dar a conocer a su equipo de trabajo los lineamientos determinados en la política institucional de riesgos	Conocer, apropiar y dar a conocer la política institucional de riesgos.	Conocer y apropiar la política institucional de riesgos.	NA
Establecimiento del Contexto	Acompañar, analizar y consolidar el análisis de contexto estratégico de la entidad para facilitar la identificación de riesgos a los procesos	Realizar el ejercicio de análisis de contexto del proceso en conjunto con su equipo de trabajo.	Participar en el análisis de contexto del proceso donde interactúa e impulsar la participación de los otros Servidores de su proceso y consolidar la información en el instrumento establecido.	Participar en el análisis de contexto del proceso al que pertenece.	NA
Identificación del Riesgo	Acompañar y asesorar a los procesos en la etapa de identificación.	Liderar el ejercicio de identificación del riesgo, determinación de causas , consecuencias y tipo de riesgo de acuerdo a lo establecido en la metodología de administración de riesgos.	Impulsar y realizar al interior del proceso el ejercicio de identificación de los riesgos para su proceso y consolidar la información en el instrumento establecido.	Participar en la identificación de riesgos, causas y consecuencias para su proceso de acuerdo a lo establecido en la metodología de administración de riesgos	NA
Análisis y Valoración del Riesgo	Acompañar y asesorar a los procesos en la etapa de analisis y valoración del riesgo	Liderar el ejercicio de análisis y valoración riesgos para el proceso. Establecer los controles idóneos que permitan administrar los riesgos identificados.	Impulsar y realizar al interior del proceso el ejercicio de análisis y valoración de los riesgos identificados para el proceso, identificación de los controles e impulsar la participación de los otros Servidores de su proceso y y consolidar la información en el instrumento establecido.	Participar en el análisis y valoración de los riesgos identificados para el proceso y en la identificación de los controles idóneos que permitan administrar los riesgos identificados	NA
Aprobación Mapa de riesgos Institucional	Coordinar la aprobación de los mapas de riesgos de los procesos para su aprobación. Consolidar y remitir a la Dirección general el mapa de riesgos institucional para su aprobación.	Realizar la aprobación del mapa de riesgos de gestión y de riesgos de corrupción del proceso	NA	NA	NA

Metodologia	Línea Estratégica	Primera linea de defensa	Segunda linea de defensa		Tercera linea de defensa
	Direccion General, Equipo directivo, Equipo de riesgos y comunicaciones estrategicas	Líder del Proceso	Enlace SIG	Servidores (s) responsable (s) de la actividad o procedimiento	Oficina de Control Interno
Planes de Respuesta	Acompañar y asesoria en la formulación de los Planes de respuesta	Asegurar la ejecución de los controles y de las acciones del Plan de respuesta a los riesgos de su proceso.	Ejecución de los controles y de las acciones del Plan de respuesta que tenga a su cargo. Consolidación de la evidencia de controles y planes de respuesta en el instrumento establecido.	Ejecución de los controles y actividades del plan de respuesta que tenga a su cargo. Entrega de evidencia de los mismos al enlace del proceso	Realizar seguimiento a los mapas de riesgos y generar alertas al respecto
Revisión y actualización	Acompañar y asesorar la revisión y actualización de los mapas de riesgos	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.	Impulsar y participar en la Mesas de trabajo para la revision y actualización de los riesgos. Realizar la identificación de las actualizaciones requeridas y consolidar la información en el instrumento establecido.	Participar en la Mesas de trabajo para la revision y actualización de los riesgos. Realizar la identificación y reporte al enlace de las actualizaciones requeridas en los mapas de riesgos.	NA
Monitoreo a la materialización de los riesgos	Recibir y consolidar los reporte de todos los riesgos materializados e informarlos a la Dirección para tomar acciones frente a los mismos	Asegurar el monitoreo mensual a la materializacion de los riesgos del proceso y tomar acciones frente a los resultados.	Realizar, consolidar y reportar al COMR* el monitoreo de la materializacion de los riesgos del proceso y tomar acciones frente a los riesgos materializados. * Centro de operaciones y monitoreo de riesgos	Reportaral enlace del proceso los riesgos materializados y cumplir con las acciones establecidas frente a los riesgos materializados.	NA
Seguimiento	Analizar estratégicamente los resultados e informes de seguimiento a los mapas de riesgos de la entidad, con el fin de tomar las decisiones requeridas para la mejora de la gestión del riesgo en la entidad o para actualizar 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 gestion y de corrupcion, planes de respuesta y monitoreo a la materializacion de riesgo.	Atender todos los requerimientos de la oficina de control Interno con respecto a la evidencia relacionada con los Mapas de riesgos de gestion y de corrupcion, planes de respuesta y monitoreo a la materializacion de riesgo.	Atender todos los requerimientos de la oficina de control Interno con respecto a la evidencia relacionada con los Mapas de riesgos de gestion y de corrupcion, planes de respuesta y monitoreo a la materializacion de riesgos que esten a su cargo.	Adelantar seguimiento al mapa de riesgos de corrupción y al mapa de riesgos de gestión. Analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos y determinar la efectividad de los controles. Realizar seguimiento al los planes de respuesta, a la ejecución de las acciones, al nivel de avance/cumplimiento y a monitoreo a la materialización del riesgo.

Metodologia	Línea Estratégica	Primera linea de defensa	Segunda linea de defensa		Tercera linea de defensa
	Direccion General, Equipo directivo, Equipo de riesgos y comunicaciones estrategicas	Líder del Proceso	Enlace SIG	Servidores (s) responsable (s) de la actividad o procedimiento	Oficina de Control Interno
Comunicación y Consulta	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.	Conocer y apropiar los riesgo de su proceso. Participar en los procesos de aprendizaje que se programen y facilitar la asistencia de los funcionarios de su equipo de trabajo.	Conocer y apropiar los riesgo de su proceso. 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 dentro de la entidad.		NA

IV. 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.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA Guía de administración de riesgos, Bogotá: Cuarta edición septiembre de 2015

ICONTEC Gestión de riesgos: Norma técnica colombiana NTC ISO 31000, Bogotá: Febrero 16 de 2011

ICONTEC Guía técnica colombiana: Gestión de riesgos - Vocabulario GTC 137, Bogotá: Febrero 16 2011

ICONTEC Comunicación y consulta acerca del riesgo HB327:2010, Bogotá: Octubre de 2011

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

V. ANEXOS

ANEXO 1

Identificación de peligros y riesgos en el desarrollo de las actividades laborales - Seguridad y salud en el trabajo

Como parte del trabajo de identificación de riesgos el proceso de talento humano realiza la identificación de peligros y evaluación de riesgos en el desarrollo de las actividades laborales de acuerdo a los parámetros establecidos en el presente anexo, cuyos resultados se consignan en la "Matriz de identificación de peligros, valoración de riesgos y determinación de controles", el cual sirve como insumo para identificar los riesgos de Seguridad y salud en el trabajo que harán parte de la Matriz de riesgos institucionales de la Unidad.

a. Levantamiento de información para la identificación de peligros

Para realizar la identificación de peligros y evaluación de riesgos se ha diseñado la "Matriz de identificación de peligros, valoración de riesgos y determinación de controles" aplicable a toda la organización con el fin de asegurar una acción proactiva y no reactiva frente a la ocurrencia de incidentes en los lugares de trabajo. La identificación de peligros se realiza mediante:

- Inspecciones (Formato de inspecciones planeadas Código 770,12,15-3)
- Investigación de accidentes de trabajo (Formato Informe de investigación Código: 770.12.15-15)

b. Identificación de peligros ("Matriz de identificación de peligros, valoración de riesgos y determinación de controles")

El Profesional especialista en SO, será el responsable de identificar los peligros presentes en los diferentes puestos de trabajo y actividades que se realizan. La identificación de peligros presentes en La Unidad para la Atención y Reparación Integral a las Victimas deberá considerar los siguientes aspectos:

- Identificar las actividades rutinarias y no rutinarias.
- Identificar los peligros asociados a las actividades desarrolladas por los funcionarios, contratistas y visitantes.
- Identificar comportamientos, capacidades y condiciones físicas de los funcionarios, contratistas y visitantes como posibles peligros.

- Identificar los peligros que se pueden generar fuera del sitio de trabajo que puedan afectar la salud y seguridad de los funcionarios, contratistas y visitantes.
- Peligros presentes alrededor de las instalaciones de la Unidad y de los lugares de trabajo (en caso de las Direcciones Territoriales).
- Condiciones de equipos, infraestructura y materiales proporcionados por La Unidad para la Atención y Reparación Integral a las Victimas presentes en los sitios de trabajo
- Identificar los peligros que se pueden generar en los cambios propuestos por la Unidad frente a sus actividades, procesos o materiales antes de ponerlos en marcha.
- Modificaciones que se puedan generar dentro del Sistema de Gestión SG SST
- El cumplimiento de requisitos legales aplicables a la Unidad.
- El diseño de puestos de trabajo, procesos, instalaciones, equipos, herramientas, actividades y el talento humano.

Para realizar dicha identificación se tendrá en cuenta la siguiente clasificación de acuerdo a la clasificación descrita en la Guía Técnica Colombiana GTC – 45, de posibles factores de riesgos que pueden afectar la salud y seguridad de los funcionarios, contratistas y visitantes de La Unidad para la Atención y Reparación Integral a las Víctimas.

Tabla de clasificación de factores de riesgo

Factores de Riesgo de Seguridad: Mecánicos, locativos, eléctricos.	• Incendio de sólidos, incendio de líquidos, incendio eléctrico, incendios combinados y explosiones. • Locativo, almacenamiento, trabajos de campo. • Caídas al mismo nivel • Caídas de objetos • Golpes o choques por objetos • Contacto directo • Contacto indirecto • Electricidad estática • Trabajo en alturas
Riesgo Biomecánico	• Posturas inadecuadas. • Movimientos repetitivos. • Manejo de cargas. • Carga postural estática • Diseño del puesto • Carga sensorial
Factores de Riesgo Biológico	• Virus • Bacterias • Hongos

	• Animales • Plantas
Factores de Riesgo Físico	• Ruido • Vibración • Iluminación deficiente o iluminación en exceso. • Radiación (Ionizante o no ionizante) • Disconfort térmico • Ventilación
Riesgo Psicosocial	• Relaciones Jerárquicas • Contenido de la Tarea • Nivel de Responsabilidad • Atención al Público. • Estrés individual • Estrés organizacional
Riesgo de Tránsito	• Colisión • Volcamiento • fallas en el vehículo (varada), obstáculos (condiciones de las vías). • atropellamiento.
Riesgo Público – Seguridad en las personas	• Factores Sociales • Factores Políticos • Seguridad Entorno
Riesgo Natural	• Terremotos • Inundaciones • Vendavales
Riesgo Químico	• Gases • Vapores • Humos • Neblinas
Humanos	• Actos inseguros, desacato de normas de seguridad. • Desconocimiento de prácticas preventivas, características físicas inadecuadas.

Esta información debe ser consignada en la "Matriz de identificación de peligros, valoración de riesgos y determinación de controles" teniendo en cuenta:

- **Factor de riesgo:** elemento que encierra una capacidad potencial de producir lesiones o daños materiales. Seleccione el factor de riesgo presente en el área o actividad en donde se están identificando las condiciones de trabajo teniendo en cuenta la tabla de clasificación de factores de riesgo.

- **Peligro:** Identifica el proceso, objetos, instrumentos y condiciones físicas y psicológicas de las personas que generan el factor de riesgo.

- **Actividad, proceso o tarea:** especifique la actividad, proceso o tarea en donde se están identificando las condiciones de trabajo.

- **Tipo de actividad:** puede ser rutinaria (Procedimientos normales) o No rutinarias (procedimientos periódicos y ocasionales)

- **Cargos:** mencione los cargos o niveles (administrativos, profesionales, directivos) directamente relacionados con los factores de riesgo identificados.

- **Origen:** marque con una X la fuente que identifico el factor de riesgo. Estas fuentes pueden ser (panorama, inspecciones, incidentes, programa PARE, observaciones del comportamiento y gestión del cambio)

c. Análisis del factor de riesgo

Se deberá determinar la descripción de las personas expuestas al factor de riesgo, posibles consecuencias, controles existentes y la valoración del riesgo para clasificar la tarea:

- **Expuestos:** número de personas que se ven afectadas en forma directa o indirecta por el factor de riesgo durante la realización del trabajo. Marque con una X si son visitantes, contratistas y/o trabajadores directos de La Unidad para la Atención y Reparación Integral a las Víctimas.

- **Efectos posibles a la salud:** describa brevemente las posibles consecuencias que pueden generar los peligros identificados sobre las personas expuestas.

- **Control existente:** medidas de eliminación o mitigación de los factores de riesgo que se han puesto en práctica en la fuente de origen, en el medio o en las personas.

- **Probabilidad:** es función de la frecuencia de exposición, la intensidad de la exposición, el número de expuestos y la sensibilidad especial de algunas de las personas al factor de riesgo, entre otras. Se clasifica en: **Baja** (el daño ocurrirá rara vez), **Media** (el daño ocurrirá en algunas ocasiones) y **Alta** (el daño ocurrirá siempre). Marque con una X según corresponda.

- **Consecuencia:** se estiman según el potencial de gravedad de las lesiones. Se clasifican en: Ligeramente **dañino** (lesiones superficiales, de poca gravedad, usualmente no incapacitantes o con incapacidades menores), **Dañino** (todas las EP no mortales, esguinces, torceduras, quemaduras de segundo o tercer grado, golpes severos, fracturas menores en costilla, dedo, mano no dominante, etc.) y **Extremadamente dañino** (lesiones graves: EP graves, progresivas y eventualmente mortales, fracturas de huesos grandes o de cráneo o múltiples, trauma encéfalocraneal, amputaciones, etc). Marque con una X según corresponda.

- **Estimación del riesgo:** está dada de acuerdo con la combinación realizada entre probabilidad y consecuencias, de la siguiente manera:

		CONSECUENCIAS		
		LIGERAMENTE DAÑINO	DAÑINO	EXTREMADAMENTE DAÑINO
PROBABILIDAD	BAJA	RIESGO TRIVIAL	RIESGO TOLERABLE	RIESGO MODERADO
	MEDIA	RIESGO TOLERABLE	RIESGO MODERADO	RIESGO IMPORTANTE
	ALTA	RIESGO MODERADO	RIESGO IMPORTANTE	RIESGO INTOLERABLE

- **Clasificación de la tarea:** determine si la actividad, proceso o tarea es CRITICA o NO CRITICA de acuerdo a los siguientes parámetros:

Estimación del riesgo (Trivial, Tolerable o Moderado) = Clasificación de la tarea NO CRITICA
Estimación del riesgo (Importante o Intolerable) = Clasificación de la tarea CRITICA.

d. Medidas de control

Una vez se determine la estimación del riesgo se debe identificar la intervención a seguir, para esto se deberá tener en cuenta la siguiente tabla:

RIESGO	RECOMENDACIONES
TRIVIAL	No se requiere acción específica si hay riesgos mayores.
TOLERABLE	No se necesita mejorar las medidas de control pero deben considerarse soluciones o mejoras de bajo costo y se deben hacer comprobaciones periódicas para asegurar que el riesgo aún es tolerable.
MODERADO	Se deben hacer esfuerzos por reducir el riesgo y en consecuencia debe diseñarse un proyecto de mitigación o control. Como está asociado a lesiones muy graves debe revisarse la probabilidad y

	debe ser de mayor prioridad que el moderado con menores consecuencias
IMPORTANTE	En presencia de un riesgo así no debe realizarse ningún trabajo. Este es un riesgo en el que se deben establecer estándares de seguridad o listas de verificación para asegurarse que el riesgo está bajo control antes de iniciar cualquier tarea. Si la tarea o la labor ya se han iniciado el control o reducción del riesgo debe hacerse cuanto antes.
INTOLERABLE	Si no es posible controlar este riesgo debe suspenderse cualquier operación o debe prohibirse su iniciación.

Las medidas de control a establecer para mitigar o eliminar el factor de riesgo identificado, tendrá en cuenta la siguiente jerarquización:

- **Eliminar:** consiste en prescindir de la actividad o equipo que genera el peligro. Esta medida de control contempla la eliminación de la tarea, actividad o equipo, con el fin de evitar la ocurrencia de algún incidente asociado.

- **Sustituir**: reemplazar la actividad o equipo por uno menos peligroso. Establece sustituir la actividad, tarea o equipo por otro, con el fin de evitar la ocurrencia de un incidente asociado o reducir la consecuencia del mismo.

- **Controles de ingeniería**: modificar las actividades o equipos de trabajo. Esta medida de control establece la remodelación de alguna actividad, tarea o equipo, con el fin de evitar la ocurrencia de un incidente asociado o reducir la consecuencia del mismo.

- **Señalización y/o gestiones administrativas**: aislar el peligro mediante barreras o su confinamiento. Se debe evitar que los incidentes potenciales de una actividad específica afecten la ejecución de otras actividades, por lo que se debe aislar la actividad, tarea o equipo. Esta medida de control también contempla gestiones administrativas como:

  - Realizar capacitación.
  - Elaborar Procedimientos de trabajo seguros específicos, planes, etc.
  - Elaboración de listas de chequeo, etc.
  - Realizar inspecciones de seguridad

- **En el trabajador, uso de EPP**: en donde el riesgo no es mayor o donde las anteriores medidas de control no se pueden implementar, se deberá desarrollar actividades que involucren al personal como capacitaciones, envió de información sobre el riesgo y dotación e inspección de elementos de protección personal.

- **Controles del comportamiento humano:** es el conjunto de actos exhibidos por el ser humano y determinados por la cultura, las actitudes, las emociones y los valores de la persona que se evidencian en las observaciones del comportamiento.

NOTA: las medidas de control que se determinen para eliminar o mitigar un riesgo debe considerar los posibles peligros que puede generar y el cumplimiento de los requisitos legales aplicables a la organización antes de su implementación.

e. Riesgo Residual

Una vez que los riesgos han sido valorizados se procede a evaluar la "calidad de la gestión", a fin de determinar cuán eficaces son los controles establecidos por la Unidad para mitigar los riesgos identificados. Finalmente, se calcula el "riesgo neto o residual".

El riesgo residual se calcula valorando la efectividad del control a implementar de acuerdo a la siguiente tabla:

EFECTIVIDAD DEL CONTROL

Control implementado	Efectividad
Ninguno	0,1
En el trabajador	0,5
Señalización, gestión administrativa y control de ingeniería	0,8
Eliminación y sustitución	1

Para hallar el riesgo residual (RR) aplicamos la siguiente fórmula:

RR = (Efectividad del control * Valoración del riesgo) – Valoración del riesgo

Una vez se determine el riesgo residual se realizara seguimiento a los riesgos que se encuentren valorados como "IMPORTANTES" e "INTOLERABLES" priorizando las actividades de mayor a menor valor estimado para el riesgo residual. Las medidas de control que se estimen en la "Matriz de identificación de peligros, valoración de riesgos y determinación de controles" se deberán incluir en los programas que desarrolle La Unidad para la Atención y Reparación Integral a las Víctimas, con el fin de realizar seguimiento a dichos controles.

f. Actualización de la matriz de identificación de peligros, valoración de riesgos y determinación de controles

La matriz de identificación de peligros, valoración de riesgos y determinación de controles para La Unidad para la Atención y Reparación Integral a las Víctimas deberá ser actualizada en los siguientes casos:

- Adquisición de máquinas y equipos
- Modificaciones en el acondicionamiento de los lugares de trabajo
- Cambio en las condiciones de trabajo
- La incorporación de un funcionario cuyas características personales o estado biológico conocido lo hagan especialmente sensible a las condiciones del puesto
- Incidentes ocurridos

- Rotación de personal
- Cambio en la normativa aplicable a las actividades de La Unidad para la Atención y Reparación Integral a las Víctimas en temas de seguridad y salud ocupacional.
- Hallazgos no considerados en las inspecciones y observaciones del comportamiento que se realicen
- Reportes de actos y condiciones inseguras no consideradas

NOTA: las modificadas realizadas a la matriz de identificación de peligros, valoración de riesgos y determinación de controles, así como las medidas de control determinadas para eliminar y/o mitigar la ocurrencia de incidentes deberán ser comunicadas a los funcionarios y contratistas por el Profesional Especialista en SO y/o Coordinadores.

ANEXO 2

Identificación riesgos de seguridad de la Información

Para identificar los riesgos de seguridad de la información se debe realizar la identificación de las vulnerabilidades y amenazas que pueden afectar la Integridad, confidencialidad y disponibilidad de la información y los demás activos que la soportan.

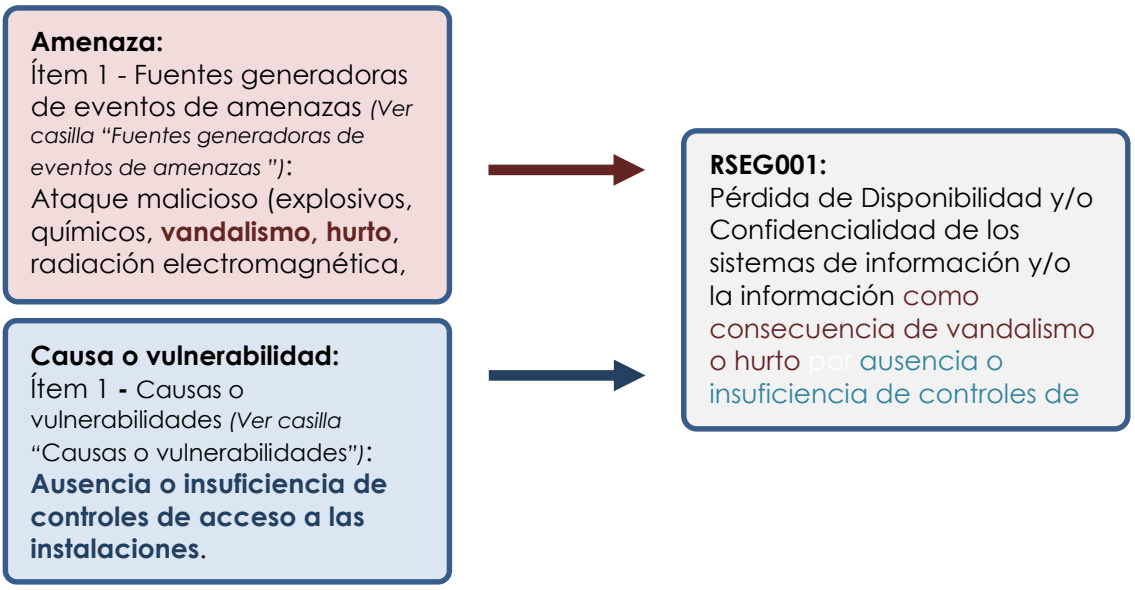
Para la identificación es importante hacer claridad en los siguientes conceptos:

- Las amenazas son todos los elementos o acciones capaces de atentar contra la seguridad de la información y son generadoras de eventos. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada.
- Las vulnerabilidades son las debilidades inherentes al activo que lo hacen susceptible de ser atacado.
- Los activos de información se refieren a la información que tiene valor para la organización y a los elementos relacionados con la misma o que la soportan, como por ejemplo sistemas de información, elementos de hardware, personas e instalaciones.

A modo de ejemplo, a continuación, se selecciona el riesgo tipo **RSEG001:**

R: Riesgo
SEG: Seguridad
xxx: Número de riesgo.

RSEG001: Pérdida de Disponibilidad y/o Confidencialidad de los sistemas de información y/o la información como consecuencia de vandalismo o hurto por ausencia o insuficiencia de controles de acceso a las áreas seguras.



a. Identificación de activos de información

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 v1 el cual es responsabilidad del Proceso de gestión documental, Sin embargo, como parte del proceso de identificación es importante relacionarlos en la descripción del riesgo. Los activos críticos son aquellos se encuentran en la escala del 4 al 5 de la valoración del activo. Los activos que se localicen dentro de este rango se les realizará la correspondiente gestión de riesgos, a partir de la metodología de riesgos definida por la Entidad.

A continuación, ejemplo para el diligenciamiento de la matriz de riesgos:

IDENTIFICACION					
No	**Proceso**	**Riesgo**	**Causas**	**Consecuencias**	**Tipo de Riesgo**
1	Nombre del proceso	**RSEG001***Pérdida de Disponibilidad y/o Confidencialidad de los sistemas de información y/o la información como consecuencia de vandalismo o hurto por ausencia o insuficiencia de controles de acceso a las áreas seguras. - Activo 1 (**ID** activo 1) - Activo 2 (**ID** activo 2)	Ausencia o insuficiencia de controles de acceso a las instalaciones.	Operativo	Seguridad de la Información

b. Insumos para la identificación de Riesgos

La Unidad cuenta con el listado que facilitan esta labor, como son:

- Riesgos seguridad de la información
- Fuentes o generadoras de eventos /Amenazas
- Causas o vulnerabilidades

A continuación, se observa la tabla con los riesgos globales o generales de seguridad de la información donde cada uno de ellos tiene asociado las amenazas y las vulnerabilidades que facilitan al usuario la identificación de riesgos asociados a sus procesos:

Teniendo en cuenta que riesgo es el potencial de que una amenaza pueda explotar una vulnerabilidad de un activo de información afectando la operación o imagen de la Entidad. Para facilitar la identificación de los riesgos de seguridad de la información, se establece el listado de riesgos de seguridad de la información donde se asocian las amenazas y vulnerabilidades:

Riesgos de seguridad de la información			
Listado de Riesgos seguridad de la información		**Fuentes o generadoras de eventos /Amenazas**	**Causas o vulnerabilidades**
RSEG001	Pérdida parcial o total de la Confidencialidad, integridad y/o Disponibilidad de los sistemas de información y/o la información registrada en documento físico o digital.	- Vandalismo o hurto, por ausencia o insuficiencia de controles de acceso a las áreas seguras; - Daño físico (Fuego, agua, humedad, variaciones de temperatura/voltaje, polvo, entre otros) por ausencia o insuficiencia de protección física contra desastres naturales; - Acciones involuntarias y/o deliberadas de usuario por ausencia o insuficiencia en la gestión de eventos de monitoreo o por almacenamiento de información sin protección o por la insuficiencia de personal adecuado para cubrir funciones específicas o desconocimiento de las políticas de seguridad.	Ausencia o insuficiencia de controles de acceso a las instalaciones. Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ej. detección o extinción de incendios, líquidos inflamables, CCTV, entre otros). Ausencia o insuficiencia de procedimientos de Monitoreo de los recursos de procesamiento de información. Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. Falla, daño o degradación de equipos. Ubicación geográfica de las instalaciones en una zona de alto impacto por eventos externos (desastres naturales, orden público, entre otros). Almacenamiento de información sin protección

			Acceso no controlado a información sensible / confidencial. Personal inconforme o molesto. Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. Ausencia de registros de auditoría. Ausencia o insuficiencia de documentación de uso y/o administración. Arquitectura insegura de la red. Puertos o servicios activos no requeridos. Documentación insuficiente o desactualizada.
RSEG002	Pérdida de Confidencialidad y/o Disponibilidad e Integridad por hurto o daño de equipos y/o Unidades de almacenamiento extraíbles en los que se almacene información sensible en texto claro, es decir no cifrado, fuera de las instalaciones de la Entidad.	Ausencia o insuficiencia en el control de los activos que se encuentran fuera de las instalaciones	Ausencia o insuficiencia de procedimientos para el manejo información clasificada. Ausencia o insuficiencia en el control de los activos que se encuentran fuera de las instalaciones Almacenamiento de información sin protección Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. Hurto, fraude o sabotaje de equipos, medios, información o documentos.
RSEG003	Pérdida de confidencialidad, integridad o disponibilidad ocasionada por la infiltración en el servidor, en el dispositivo de red y/o el sistema de información. debido al acceso no autorizado como consecuencia de captura de credenciales	Acceso no autorizado como consecuencia de captura de credenciales transferidas en texto claro, durante el ingreso vía web.	Transferencia y/o almacenamiento de información en texto claro. Espionaje (interceptación, ingeniería social).

	transferidas en texto claro, durante el ingreso vía web.		
RSEG004	Pérdida de disponibilidad de sistemas de información o de los equipos informáticos o de equipos de comunicaciones, debido a fallas en los equipos como resultado de la ausencia o insuficiencia de mantenimiento preventivo / correctivo o falla o degradación de los sistemas de información.	ausencia o insuficiencia de mantenimiento preventivo / correctivo o falla o degradación de los sistemas de información	Incumplimiento de las condiciones técnicas y/o ambientales provistas por el fabricante. Ausencia o insuficiencia de mantenimiento preventivo / correctivo. Arquitectura insegura de la red. Ausencia de planes de continuidad. Ausencia o insuficiencia de control de cambios en la configuración. Fallas conocidas o defectos del software. Ausencia de segmentación de la red.
RSEG005	Interrupción total o parcial de la Disponibilidad debido a falla, daño o degradación de los sistemas (sistema contra incendio, CCTV, control de acceso, Sistema de Aire Acondicionado, Sistema de respaldo eléctrico, etc.) que garantiza la operación de los equipos en el Centro de Datos y centros de cableado,	Falla eléctrica, degradación de equipos, falta de mantenimientos preventivos o por fallas en la administración y gestión de los dispositivos de Red.	Incumplimiento de las condiciones técnicas y/o ambientales provistas por el fabricante. Ausencia o insuficiencia de mantenimiento preventivo / correctivo.
RSEG006	Pérdida de Disponibilidad de los sistemas de información y/o información por insuficiencia o ausencia de planes de continuidad y/o contingencia ante un desastre y/o un evento mayor.	Insuficiencia o ausencia de planes de continuidad y/o contingencia ante un desastre y/o un evento mayor.	Ausencia de planes de continuidad y/o contingencia.

RSEG007	'Pérdida de disponibilidad y/o integridad en el sistema al presentarse errores durante la ejecución de modificaciones debido a la falta definición, aplicación u omisión de alguna de las actividades del procedimiento de gestión de cambios.	falta definición, aplicación u omisión de alguna de las actividades del procedimiento de gestión de cambios.	Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos. Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. Testeo inadecuado o insuficiente.
RSEG008	Pérdida de disponibilidad, integridad y/o confidencialidad en el sistema de información debido a ausencia o insuficiencia de copias de respaldo; o debido a vulnerabilidades no corregidas explotadas y/o falta de protección por código malicioso.	Vulnerabilidades no corregidas explotadas y/o falta de protección por código malicioso.	Ausencia o insuficiencia de copias de respaldo. Ausencia o insuficiencia de mantenimiento. Ausencia o insuficiencia de actualizaciones. Falta de protección contra virus y/o código malicioso. Ausencia o insuficiencia de documentación de uso y/o administración.
RSEG009	Pérdida de la confidencialidad de información física o digital debido a actividades de ingeniería social de un intruso que aproveche el desconocimiento de políticas, procedimientos y directrices de seguridad por parte de un colaborador, proveedor y/o terceras partes.	En caso de presentarse ingeniería social por parte de un intruso que aproveche el desconocimiento de políticas, procedimientos y directrices de seguridad por parte de un colaborador, proveedor y/o terceras partes.	Ausencia o insuficiencia de copias de respaldo. Ausencia o insuficiencia de mantenimiento. Ausencia o insuficiencia de actualizaciones. Falta de protección contra virus y/o código malicioso. Ausencia o insuficiencia de documentación de uso y/o administración.
RSEG010	Pérdida en la integridad de la Imagen y reputación de la entidad o sanciones disciplinarias y/o	Divulgación no autorizada o fuga de información o por el uso de software no legal o plagio. Divulgación de las credenciales de los equipos de cómputo o	Personal inconforme o molesto. Descarga y/o uso no controlado de software.

	penales por incumplimiento de la normatividad y regulaciones ocasionadas por la divulgación no autorizada o fuga de información o por el uso de software no legal o plagio; o por divulgación de las credenciales de los equipos de cómputo o aplicativos o incumplimiento de los términos por la pérdida o daño de la documentación o incumplimiento a los acuerdos de Nivel de Servicio.	aplicativos o incumplimiento de los términos por la pérdida o daño de la documentación. Incumplimiento a los acuerdos de Nivel de Servicio.	Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables. Uso de Software ilegal / No autorizado / Software Malicioso. Ausencia de responsables sobre la gestión en seguridad de la información y/o continuidad de negocio. Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso. Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. Falta de segregación de funciones o incorrecta aplicación de estas.
RSEG011	Pérdida parcial o total de la disponibilidad de los sistemas de información y/o la información por ausencia o insuficiencia de Acuerdo de Nivel de Servicio con terceros.	Ausencia o insuficiencia de Acuerdo de Nivel de Servicio con terceros.	Ausencia o insuficiencia de contratos, acuerdos de niveles de servicio y/o confidencialidad. Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los empleados y/o terceras partes. Dependencia de proveedores. Falla de la red interna

Controles para mitigar Riesgos de seguridad de la información

A continuación, el listado propuesto de controles que los usuarios de cada uno de los procesos pueden ejecutar y asociar en la matriz de riesgo*, siempre y cuando se incluyan cumpliendo con los parámetros establecidos en la metodología (Quien, Cuando, Que busca, Como, Evidencia y excepciones y observaciones):

1. Sincronizar el almacenamiento de la información con ONE -DRIVE.
2. Gestionar la inactivación de credenciales de acceso a sistemas de información o herramientas tecnológicas, cuando el personal del proceso se retira o cambia de rol.
3. Aceptar las actualizaciones del sistema operativo.
4. Actualizar frecuentemente las contraseñas de los sistemas de información.
5. Evitar transportar fuera de la Entidad información física o digital, de carácter confidencial.
6. Colocar guaya de seguridad a equipos portátiles de la Entidad.
7. Portar el carnet de la entidad en un lugar visible, pero al salir de la entidad es recomendable retirarlo.

8. No compartir credenciales de acceso a sistemas de información.
9. Guardar la información física confidencial de la entidad bajo llave.
10. Controlar el préstamo de información física del proceso.
11. Revisar y controlar la información almacenada en (Totoro).
12. Clasificar la información que se encuentra en el servidor de almacenamiento de información - Totoro, donde se identifique la información de gestión y la histórica.
13. Validar los permisos asignados sobre las carpetas del servidor de almacenamiento de información Totoro, asignando permisos de edición, consulta de la información.
14. Solicitar asesoría especializada en caso de ser requerida, en seguridad de la información al iniciar un proyecto.
15. Identificar y Clasificar los activos de información de gestión de su proceso.
16. Mantener y devolver en buen estado los activos tecnológicos que le fueron otorgados por la entidad.
17. Reportar en mesa de servicio tecnológicos los incidentes, en caso de presentarse la pérdida, divulgación o modificación no controlada de la información.
18. Utilizar de manera adecuada los controles físicos instalados en cada una de las sedes como: control dactilar, bitácoras de ingreso, circuito cerrado, alarma contra incendios.
19. Registrar en la bitácora la entrada de los equipos portátiles u otros elementos tecnológicos que requiera reportar.
20. Acompañar a los invitados durante la estadía en la entidad.
21. Informar al guarda de seguridad del piso, cuando se presenten actividades sospechosas al interior del sitio de trabajo.
22. Dar información institucional a los usuarios por los canales adecuados.
23. Evitar abrir archivos sospechosos enviados al correo electrónico.
24. Utilizar los recursos tecnológicos exclusivamente para el uso de la gestión de la entidad.
25. No llevar información confidencial de la entidad en memorias USB, o cd o cualquier otro medio de almacenamiento.
26. Utilizar las herramientas que la Oficina de tecnología de la información ofrece al requerir transportar información sensible de la entidad.
27. No instalar herramientas sin la debida aprobación de la Oficina de tecnología de información.
28. No pegar las credenciales de acceso en papeles adheridas al equipo de cómputo.
29. Utilizar de manera adecuado el correo personal en caso de no estar restringido.
30. Informar a la Red nacional de información en caso de requerir intercambio de información con entidades externas.
31. Avisar a soporte tecnológico en caso de requerir instalación de herramientas tecnológicas recuerde que hay personal idóneo para realizar estos trabajos.
32. Cambiar frecuentemente la contraseña de los sistemas de información a los que se me ha dado permiso.
33. No permitir el ingreso de personal no autorizado al sitio de trabajo.
34. Conocer los lineamientos de seguridad de la información que la entidad tiene establecido.
35. Leer el acuerdo de confidencial que formo con la Entidad.
36. Firmar acuerdos de confidencialidad.
37. Realizar copia de respaldo de información almacenada en equipos de cómputo de manera periódica.
38. Asistir a las charlas que se realicen de seguridad de la información realizadas por la entidad.
39. Socializar al interior del proceso los flash informativos publicados y demás comunicados relacionados con seguridad de la información.
40. Gestionar con la Oficina de Tecnologías de la Información el bloqueo de puertos USB de los equipos de cómputo asignados al personal del proceso.

Control de cambios

Versión	Ítem del cambio	Cambio realizado	Motivo del cambio	Fecha del cambio
V1	Creación	NA	NA	NA
V2	Metodología	Actualización por cambios en el MECI 1000:2005 y queda vigente el MECI 2014. Expedición del Decreto 0943 de 2014	Actualización	
V2	Metodología	Ajustes por la expedición de la Guía para la Administración del Riesgo del DAFP	Actualización	
V3	Metodología	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	Actualización	27/04/2016
V4	Metodología	Inclusión y articulación de riesgos públicos, ambientales, seguridad y salud en el trabajo y seguridad de la información	Actualización	03/03/2017
V5	Metodología	Ajustes Análisis de contexto, materialización de riesgos. Ajuste de acuerdo con recomendaciones de auditoria.	Actualización	06/03/2017