ANEXO 1

GUÍA PARA LA IDENTIFICACIÓN DE LOS PELIGROS Y LA VALORACIÓN DE RIESGOS EN SEGURIDAD Y SALUD EN EL TRABAJO

CAPITULO I

ASPECTOS GENERALES

1.1. INTRODUCCIÓN

El presente capítulo brinda herramientas necesarias para realizar una eficiente gestión de riesgos y peligros, a través de la identificación de peligros, valoración de riesgos e implementación de controles, los cuales permiten satisfacer las necesidades y requisitos de los funcionarios, colaboradores y partes interesadas.

De acuerdo con lo señalado, la identificación se refiere al diagnóstico inicial de las situaciones que pueden causar un peligro o afectación a los funcionarios, colaboradores y/o la Unidad, o generen posibles pérdidas materiales, humanas, etc, determinando puntos críticos, en los que existe una alta probabilidad de ocurrencia respecto de accidentes de trabajo y/o enfermedades laborales.

Teniendo en cuenta lo anterior, la identificación de peligros, valoración de riesgos y determinación de controles es realizada por el proceso de Talento Humano, en el desarrollo de las actividades laborales, siguiendo los parámetros que se establecen en el presente capítulo, 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 para la Atención y Reparación Integral a las Víctimas.

1.2. Objetivos

- Establecer una herramienta que permita la identificación de peligros, valoración de riesgos y determinación de los controles de Seguridad y Salud en el Trabajo asociados a los procesos y actividades propias de la misión de la Unidad para la Atención y Reparación Integral a las Víctimas.

- Analizar la probabilidad de ocurrencia y las consecuencias que puedan originar la materialización de los peligros identificados.

- Implementar los sistemas de control encaminados a la mitigación de peligros y riesgos de Seguridad y Salud en el Trabajo.

1.3. DEFINICIONES

Accidente de trabajo: suceso repentino que sobreviene por causa o con ocasión del trabajo, y que produce en el trabajador una lesión orgánica, una perturbación funcional, una invalidez o la muerte. Es también accidente de trabajo aquel que se produce durante la ejecución de órdenes del empleador o durante la ejecución de una labor bajo su autoridad, incluso fuera del lugar y horas de trabajo.

Actividad rutinaria: Es una actividad que forma parte de un proceso de la organización, se ha planificado y es estandarizable.

Actividad no rutinaria: Es una actividad que no se ha planificado ni estandarizado, dentro de un proceso de la organización o actividad que la organización determine como no rutinaria por su baja frecuencia de ejecución.

Análisis del riesgo: Es un proceso para comprender la naturaleza del riesgo y para determinar el nivel del mismo.

Consecuencia: Es un resultado, en términos de lesión o enfermedad, de la materialización de un riesgo, expresado cualitativa o cuantitativamente.

Competencia: corresponde a los atributos personales y aptitud demostrada para aplicar conocimientos y habilidades.

Diagnóstico de condiciones de trabajo: Es el resultado del procedimiento sistemático para identificar, localizar y valorar “aquellos elementos, peligros o factores que tienen influencia significativa en la generación de riesgos para la seguridad y la salud de los trabajadores”.

Diagnóstico de condiciones de salud: Es el resultado del procedimiento sistemático para determinar “el conjunto de variables objetivas de orden fisiológico, psicológico y sociocultural que determinan el perfil sociodemográfico y de morbilidad de la población trabajadora”.

Elemento de Protección Personal (EPP): Es un dispositivo que sirve como barrera entre un peligro y alguna parte del cuerpo de una persona.

Enfermedad: Es una condición física o mental adversa identificable, que surge, empeora o ambas, a causa de una actividad laboral, una situación relacionada con el trabajo o ambas.

Enfermedad profesional: Es todo estado patológico que sobreviene como consecuencia obligada de la clase de trabajo que desempeña el trabajador o del medio en que se ha visto obligado a trabajar, bien sea determinado por agentes físicos, químicos o biológicos.

Equipo de protección personal: Es un dispositivo que sirve como medio de protección ante un peligro y que para su funcionamiento requiere de la interacción con otros elementos. Ejemplo: sistema de detección contra caídas.

Evaluación higiénica: Es una medición de los peligros ambientales presentes en el lugar de trabajo para determinar la exposición ocupacional y riesgo para la salud, en comparación con los valores fijados por la autoridad competente.

Evaluación del riesgo: Es un proceso para determinar el nivel de riesgo asociado al nivel de probabilidad y el nivel de consecuencia.

Exposición: Es una situación en la cual las personas se encuentran en contacto con los peligros.

Identificación del peligro: proceso para reconocer si existe un peligro y definir sus características.

Incidente: evento(s) relacionado(s) con el trabajo, en el (los) que ocurrió o pudo haber ocurrido lesión o enfermedad (independiente de su severidad) o víctima mortal.

Lugar de trabajo: espacio físico en el que se realizan actividades relacionadas con el trabajo, bajo el control de la organización.

Medida(s) de control: medida(s) implementada(s) con el fin de minimizar la ocurrencia de incidentes.

Nivel de consecuencia: medida de la severidad de las consecuencias

Nivel de deficiencia: Magnitud de la relación esperable entre el conjunto de peligros detectados y su relación causal directa con posibles incidentes y con la eficacia de las medidas preventivas existentes en un lugar de trabajo.

Nivel de exposición: situación de exposición a un peligro que se presenta en un tiempo determinado durante la jornada laboral.

Nivel de probabilidad: Es un producto del nivel de deficiencia por el nivel de exposición.

Nivel de riesgo: magnitud de un riesgo resultante del producto del nivel de probabilidad por el nivel de consecuencia

Partes Interesadas: persona o grupo dentro o fuera del lugar de trabajo involucrado o afectado por el desempeño de seguridad y salud ocupacional de una organización

Peligro: fuente, situación o acto con potencial de daño en términos de enfermedad o lesión a las personas, o una combinación de éstos.

Personal expuesto: número de personas que están en contacto con peligros.

Probabilidad: grado de posibilidad de que ocurra un evento no deseado y pueda producir consecuencias

Proceso: conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Riesgo: combinación de la probabilidad de que ocurra(n) un(os) evento(s) o exposición(es) peligroso(s), y la severidad de lesión o enfermedad, que puede ser causado por el (los) evento(s) o la(s) exposición(es).

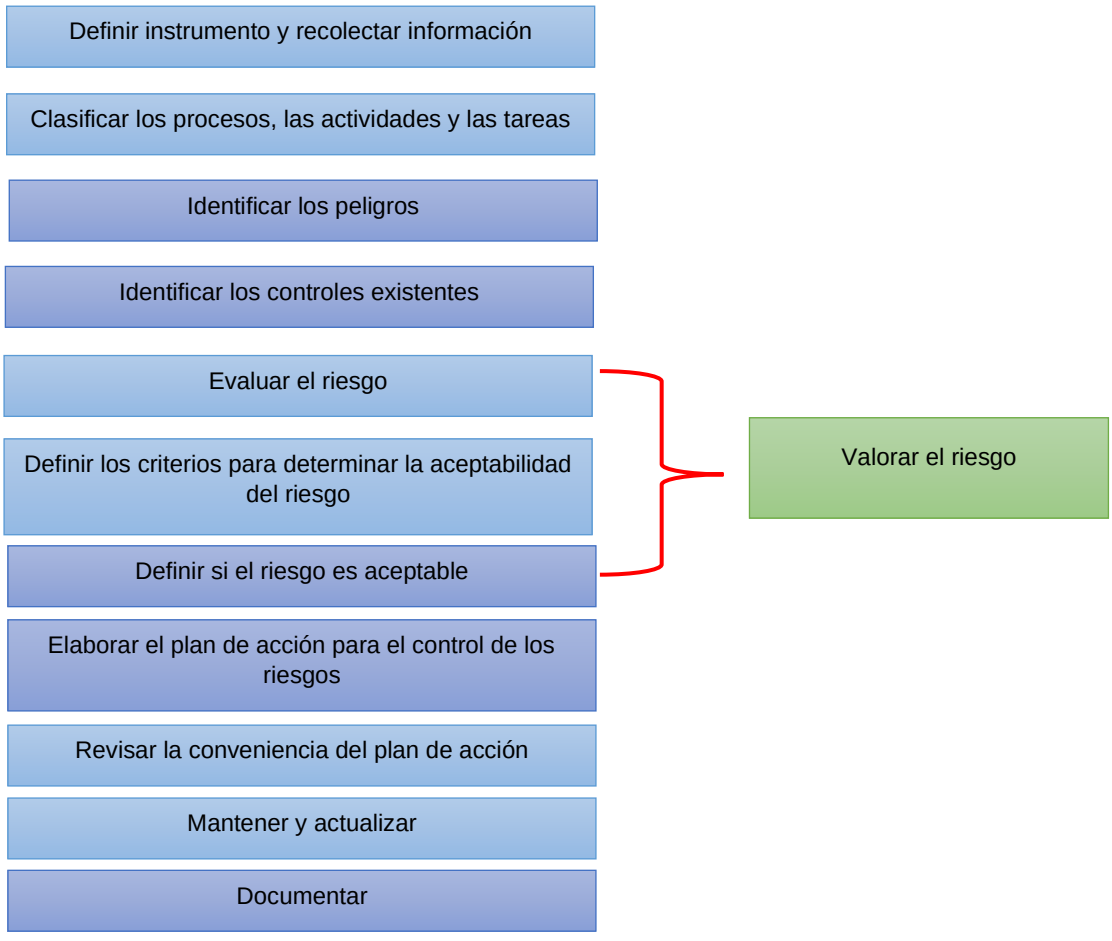
CAPITULO II

GESTIÓN DE LOS PELIGROS Y RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO

2.1. Identificación de los riesgos:

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 y evaluación de los riesgos debe ser desarrollada por la Unidad con la participación y compromiso de todos los niveles de la entidad, teniendo en cuenta las siguientes actividades:



Fuente: GUÍA TÉCNICA GTC COLOMBIANA 45

2.1.1. Actividades necesarias para la identificación del riesgo

Las siguientes actividades son necesarias para que la Unidad, realice la identificación de los peligros y la valoración de los riesgos:

a) Definir el instrumento para recolectar la información: una herramienta donde se registre la información que permita la identificación de los peligros y valoración de los riesgos, para lo cual, la entidad cuenta con la Matriz de identificación de peligros, valoración de riesgos y determinación de controles asociada al proceso de Gestión del Talento Humano.

b) Clasificar los procesos, las actividades y las tareas: preparar una lista de los procesos de trabajo y de cada una de las actividades que lo componen y clasificarlas; esta lista debería incluir instalaciones, planta, personas y procedimientos.

c) Identificar los peligros: incluir todos aquellos relacionados con cada actividad laboral. Considerar quién, cuándo y cómo puede resultar afectado.

d) Identificar los controles existentes: relacionar todos los controles que la organización ha implementado para reducir el riesgo asociado a cada peligro.

e) Evaluar el riesgo: calificar el riesgo asociado a cada peligro, incluyendo los controles existentes que están implementados. Se debería considerar la eficacia de dichos controles, así como la probabilidad y las consecuencias si éstos fallan.

f) Definir los criterios para determinar la aceptabilidad del riesgo.

g) Definir si el riesgo es aceptable: determinar la aceptabilidad de los riesgos y decidir si los controles de SST existentes o planificados son suficientes para mantener los riesgos bajo control y cumplir los requisitos legales.

h) Elaborar el plan de acción para el control de los riesgos: diseñar acciones que permitan mejorar y mantener los controles implementados para la prevención y mitigación de los riesgos.

i) Revisar la conveniencia del plan de acción: El plan de acción debe ser objeto de revisión con el fin de garantizar que el proceso de valoración de los riesgos y de establecimiento de criterios sea adecuado y la ejecución del proceso es eficaz.

j) Mantenimiento y actualización: se debe establecer la necesidad de identificar si los controles para el riesgo existentes resultan ser eficaces y suficientes con relación a nuevos peligros, responder a los cambios que la Unidad lleve a cabo, así como también a la retroalimentación de las actividades de seguimiento, investigación de incidentes, situaciones de emergencia o los resultados de las pruebas respecto a procedimientos de emergencia, cambios en la legislación y factores externos que afectan la salud ocupacional de los funcionarios y colaboradores de la Unidad para la Atención y Reparación Integral a las Víctimas- UARIV-

2.2. Metodología

Para la gestión de los riesgos de Seguridad y Salud en el trabajo se empleará la metodología que facilitará la administración, prevención y mitigación de los eventos que materialicen riesgos, los cuales afecten la seguridad y salud de los funcionarios y colaboradores de la Unidad, teniendo en cuenta los siguientes aspectos:

a) Identificación de actividades realizadas en la entidad: en el marco de las actividades misionales de la Unidad, se requiere identificar las áreas, lugares de trabajo, puestos de trabajo, áreas externas entre otros, y las actividades que se realizan tanto rutinarias como no rutinarias; para ello se debe tomar como punto de referencia las labores ejecutadas por el personal de planta, contratista y/o visitantes de la Unidad para la Atención y Reparación Integral a las Víctimas- UARIV-

b) Identificación de Peligros y Valoración de Riesgos de Seguridad y Salud en el Trabajo: para esta identificación se utilizará la matriz de Identificación de peligros, valoración de riesgos y determinación de los controles.

c) Datos de Identificación de la Matriz: para realizar la matriz de identificación de peligros, valoración de riesgos y determinación de controles se tendrá en cuenta los parámetros aplicables de clasificación descritos en la Guía Técnica Colombiana GTC – 45 y procurará de acuerdo con el Decreto 1072 de 2015 que la metodología sea sistemática y que tenga alcance sobre todos los procesos y actividades rutinarias y no rutinarias internas o externas.

Tabla de clasificación de factores de riesgo según guía técnica colombiana GTC 45

	CLASIFICACIÓN						
DESCRIPCIÓN	Biológico	físico	Químico	Psicosocial	Biomecánicos	Condiciones de seguridad	Fenómenos naturales
	Virus	Ruido (de impacto, intermitente, continuo)	Polvos orgánicos, inorgánicos	Gestión organizacional (estilo mando, pago, contratación, participación, inducción y capacitación, bienestar social, evaluación del desempeño, manejo de cambios)	Postura (prolongada, mantenida, forzada, anti gravitacional)	Mecánico (elementos o partes de máquinas, herramientas, equipos, piezas a trabajar, materiales proyectados, solidos o fluidos)	Sismo
	Bacterias	Iluminación (luz visible por exceso o deficiencia)	Fibras	Características de la organización del trabajo (comunicación, tecnología, organización del trabajo, demandas cualitativas y cuantitativas de la labor)	Esfuerzo	Eléctrico (alta y baja tensión, estática)	Terremoto

	Hongos	Vibración (cuerpo entero, segmentaria)	Líquidos (niebla y rocío)	Características del grupo social de trabajo (relaciones, cohesión, calidad de interacciones, trabajo en equipo)	Movimiento repetitivo	Locativo (sistemas y medios de almacenamiento), superficies de trabajo (irregularidades, deslizantes, con diferencia de nivel), condiciones de orden y aseo, (caídas de objeto)	
	Ricketsia	temperaturas extremas (calor y frio)	Gases y vapor	Condiciones de la tarea (carga mental, contenido de la tarea, demandas emocionales, sistemas de control, definición de roles, monotonía, etc.)	Manipulación manual de cargas	Tecnológico (explosión, fuga, derrame, incendio)	Inundación
	Parásitos	Presión atmosférica (normal y ajustada)	Humos metálicos, no metálicos	Interface personal - tarea (conocimientos, habilidades en relación con la demanda de la tarea, iniciativa, autonomía y reconocimiento, identificación de la persona con la tarea y la organización)		Accidentes de tránsito	Derrumbes
	Picaduras	Radiaciones ionizantes (rayos X, gama, beta y alfa)	Material articulado	Jornada de trabajo (pausas, trabajo nocturno, rotación, horas extras, descansos)		Públicos (robos, atracos, asaltos, atentados, de orden público, etc.)	Precipitaciones, (lluvias, granizadas, heladas)
	Mordeduras	Radiaciones no ionizantes (láser, ultravioleta, infrarroja, radiofrecuencia, microondas)				Trabajo en alturas	
	Fluidos o excrementos					Espacios confinados	
Tener en cuenta únicamente los peligros de fenómenos naturales que afectan las seguridad y bienestar de las personas en el desarrollo de una actividad. Enn el plan de emergencia de cada empresa, se consideran todos los fenómenos naturales que pudieran afectarla							

2.3. Evaluación del 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:

2.3.1. Grado de peligrosidad

Es un indicador de la gravedad de un riesgo reconocido y se valora de la siguiente manera:

Probabilidad (P): la posibilidad que se presenten las consecuencias identificadas si se materializa el peligro. Se evalúa con base en la escala establecida en la Tabla para cada situación específica.

MUY BAJA	1	Cuando es casi imposible que ocurra
BAJA	3	Cuando es remota pero posible (poco común)
MEDIA	6	Cuando es muy posible (nada extraño que ocurra)
ALTA	10	Cuando es inminente (ocurre con frecuencia)

Consecuencia (C): El resultado del riesgo que se evalúa, incluyendo los daños personales y los materiales. La calificación numérica se asigna de acuerdo con los valores numéricos establecidos para cada situación específica.

LEVE	1	Pequeñas heridas, lesiones no incapacitantes o daños menores
MEDIO	4	Lesiones con incapacidad no permanente o daños superiores al 20%
GRAVE	6	Lesiones incapacitantes permanentes o daños superiores al 60%
CATASTRÓFICA	10	Muerte o daños superiores al 90% del capital de la compañía

Exposición (E): frecuencia con que las personas o la infraestructura entran en contacto con el peligro. Se valora conforme a la escala identificada para cada situación específica

REMOTA	1	La persona está expuesta al peligro una vez al mes o pocas veces al año
OCASIONAL	3	Expuesta algunas veces a la semana
FRECUENTE	6	Algunas veces al día
CONTINUA	10	Continuamente o muchas veces al día

Estimación del riesgo: está dada de acuerdo con la combinación realizada entre probabilidad, las consecuencias y el grado de exposición, definiendo el Grado de Peligrosidad de la siguiente manera:

GP = C x P x E

			CONSECUENCIA				EXPOSICIÓN				
			LEVE	MEDIO	GRAVE	CATASTROFICO					
			1	4	6	10					
PROBABILIDAD	MUY BAJA	1	1	4	6	10	REMOTA	1	1	6	10
	BAJA	3	3	12	18	30	OCASIONAL	3	9	54	90
	MEDIA	6	6	24	36	60	FRECUENTE	6	36	216	360
	ALTA	10	10	40	60	100	CONTIUNUA	10	100	600	1000

Interpretación del grado de peligrosidad (g.p.)

Escala de valoración del GP	1	**301**	601
	300	600	1000
Clasificación	**BAJO**	**MEDIO**	ALTO
Medida de intervención o control	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.	Se deben hacer esfuerzo por reducir el riesgo y en consecuencias debe diseñar un proyecto de mitigación o control. Cómo está asociado a lesiones muy graves debe revisarse la probabilidad y debe ser de mayor prioridad y debe ser de mayor prioridad que el moderado con menores consecuencias.	En presencia de un riesgo, no debe realizarse ningún tipo de 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.

Clasificación de la tarea: determine si la actividad, proceso o tarea es ACEPTABLE o NO ACEPTABLE de acuerdo con los siguientes parámetros:

Estimación del riesgo (Bajo) = Clasificación de la tarea ACEPTABLE.
Estimación del riesgo (Medio o Alto) = Clasificación de la tarea NO ACEPTABLE.

Una vez realizada la clasificación de las tareas determinado el nivel de riesgo de la Entidad, se procede a decidir si el riesgo es aceptable o no se determina de acuerdo con la tabla mostrada a continuación.

ACEPTABILIDAD DEL RIESGO		
NIVEL DEL RIESGO	**INTERPRETACIÓN**	
IV	Aceptable	No es necesario intervenir, salvo que un análisis más preciso lo justifique
III	Mejorable (Aceptable)	Mejorar el control existente
II	No aceptable o Aceptable con control específico	Corregir o adoptar medidas de control
I	No aceptable	Situación crítica, corrección urgente

En el evento que el riesgo resulte No aceptable, se analizará como una acción de mejora y se seguirá lo establecido en los Procedimientos sobre Acciones Correctivas y Acciones Preventivas. Adicionalmente, se generará un documento asociado para su mitigación, el cual deberá estar avalado por el proceso Gestión de Talento Humano.

2.3.2. Medidas de control

Una vez se determine la estimación del riesgo y verifique la aceptabilidad, téngase en cuenta lo siguientes criterios:

- **Número de expuestos:** determinar el número de funcionarios, colaboradores y visitantes de la Unidad expuestos a este peligro para establecer el alcance del control que se va a implementar.
- **Consecuencia:** identificar las consecuencias más graves y con mayor impacto que pueda originar el peligro asociado, con el fin de determinar un control eficaz que pueda mitigar dicha consecuencia.
- **Existencia de requisito legal y otros específicos o asociados (si/no):** Determinar si existe o no un requisito legal específico asociado que establezca parámetros de priorización en la implementación de las medidas de intervención.

2.3.2. Medidas de Intervención

Se debe establecer para cada uno de los riesgos medidas de intervención, las cuales permiten eliminar, sustituir o minimizar un riesgo:

- **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 de este.

- **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 de este.

- **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 Elementos de Protección Personal - 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 deben considerar los posibles peligros que puede generar y el cumplimiento de los requisitos legales aplicables a la organización antes de su implementación.

Una vez se determine la estimación del riesgo, es necesario identificar la intervención a seguir, para ello, téngase en cuenta la siguiente tabla:

RIESGO	RECOMENDACIONES
BAJO	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.
MEDIO	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.
ALTO	En presencia de un riesgo, 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.

2.4. Riesgo residual

Una vez que los riesgos han sido valorados 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 de los controles implementados y se realiza nuevamente la evaluación del grado de peligrosidad de la misma manera que en el literal C Evaluación del factor del riesgo.

Una vez se determine el riesgo residual se realizará seguimiento a los riesgos que se encuentren valorados como "NO ACEPTABLES" 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 de promoción y prevención que desarrolle la Unidad para la Atención y Reparación Integral a las Víctimas, con el fin de realizar seguimiento a dichos controles.

2.5. 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- UARIV- 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 modificaciones 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 COPASST de las diferentes Direcciones Territoriales, quienes a su vez la socializarán a funcionarios y operadores.

2.6. Roles de las líneas de defensa frente a la gestión del riesgo de seguridad y salud en el trabajo

LÍNEA ESTRATÉGICA	Definir un instrumento para la gestión del riesgo y el control Conocer los informes sobre la materialización de riesgos de seguridad y salud en el trabajo en la entidad, así como las causas que los originaron. Realizar seguimiento a los resultados de las evaluaciones realizadas por la Oficina de Control Interno.
PRIMERA LÍNEA DE DEFENSA	Definir los objetivos de SST, metas, responsables, frecuencia e indicadores cualitativos y cuantitativos, consistentes con la política de SST y programas establecidos por la Entidad. Revisar los cambios en las condiciones de trabajo, ambiente laboral y entorno que puedan generar nuevos riesgos o modificar los riegos ya identificados por la entidad. Revisar las medidas de control y actividades de intervención para cada causa que pueda derivar la materialización de un riesgo Revisar y hacer seguimiento al cumplimiento de las medidas de control, diseñados para la mitigación del riesgo Revisar las actualizaciones de la matriz de identificación de peligros, valoración de riesgos
SEGUNDA LÍNEA DE DEFENSA	Establecer directrices y apoyo en la identificación, análisis, evaluación de controles y tratamiento de los riesgos. Revisar el diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones para su fortalecimiento. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo.
TERCERA LÍNEA DE DEFENSA	Revisar la efectividad y la aplicación de las medidas de control y actividades de monitoreo vinculadas a la gestión de riesgos de la entidad. Realizar seguimiento a la materialización de riesgos en la Entidad, así como al cumplimiento de las acciones mejora definidas por cada proceso. Evaluar la matriz de identificación de peligros, valoración de riesgos y verificar las actualizaciones realizadas

CAPITULO III

SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO – SGSST.

El Sistema de Gestión de Seguridad y Salud en el Trabajo SGSST busca evaluar los riesgos y oportunidades que pueden afectar la capacidad de la Unidad, para mejorar el desempeño en la Salud y la Seguridad de sus funcionarios y colaboradores, así como de las demás partes interesadas.

La Unidad para la Atención y Reparación Integral a las Víctimas, en el marco de la línea estratégica y la primera línea de defensa dimensión 7 MIPG, ha establecido los lineamientos relacionados con el Sistema de Gestión de Seguridad y Salud en el Trabajo a nivel de la Dirección general y Direcciones territoriales en la actualización de su contexto interno y externo, así como, la actualización de las necesidades y expectativas de sus funcionarios, colaboradores y partes interesadas.

3.1. Políticas operativas para el Sistema de Gestión de la Seguridad y Salud en el Trabajo

En el marco de la primera línea de defensa, se establecen las siguientes políticas:

a) La identificación y actualización de los riesgos para el Sistema de Gestión de Seguridad y Salud en el Trabajo, se realizará anualmente desde la Dirección General, bajo los siguientes criterios:

- Expedición y/o modificación de los requisitos legales.
- Modificaciones en los procesos que incidan en la Seguridad y Salud en el Trabajo.
- Resultados del análisis y cambios en el contexto interno y externo
- Resultados de la identificación de peligros, valoración de riesgos y determinación de medidas de controles.
- Resultados de las necesidades y expectativas de las partes interesadas
- Resultados y decisiones de la Revisión por la Dirección General

b) La gestión de riesgos estará basada en la identificación y análisis de los riesgos para el Sistema de Gestión de SST, así como también, la implementación de controles para su prevención y mitigación las actividades que puedan generarlos, y cumplimiento de las acciones incluidas en el plan de tratamiento.

c) La identificación de riesgos del Sistema de Gestión de SST será realizada por el equipo de SST.

d) La recopilación de la información de las actividades de SST y el diligenciamiento de los avances en la Matriz de objetivos de seguridad y salud en el trabajo, Matriz plan de implementación SIG y Matriz plan de acción está a cargo del equipo de SST.

e) Reportar mensualmente, el resultado de seguimiento de indicadores del Sistema de Gestión de Seguridad y Salud en el Trabajo a la Oficina Asesora de Planeación.

f) Se realizarán inspecciones planeadas de seguridad anualmente y cuando se requiera en todas oficinas a nivel central y territorial, de acuerdo con el procedimiento para la realización de inspecciones de seguridad.

g) Se realizará seguimiento semestral al cierre de hallazgos reportados en las inspecciones de seguridad mediante reunión de seguimiento con los procesos de Gestión Administrativa y Documental y con la Oficina de Tecnología de la Información.

h) Todos los accidentes de trabajo sin excepción deberán registrase en la Matriz de accidentalidad, de acuerdo con el procedimiento de reporte e investigación de incidentes y accidentes de trabajo.

i) Se realizará un seguimiento trimestralmente de acciones correctivas derivadas de los accidentes de trabajo reportados.

j) La actualización de la Matriz de identificación de peligros, valoración de riesgos y determinación de controles será actualizada de manera permanente, para lo cual se deberá tener en cuenta las inspecciones de seguridad y los incidentes y accidentes de trabajo reportados.

k) Se realizará una reunión mensual del Equipo de Seguridad y Salud en el Trabajo con el fin de verificar el cumplimiento de objetivos de SST, cumplimiento del cronograma anual del Sistema de Gestión de Seguridad y Salud en el Trabajo y del cierre de acciones correctivas derivadas de las inspecciones e investigaciones de incidentes y accidentes de trabajo reportados

3.2. Formulación de los planes de tratamiento

Al momento de formular los planes de tratamiento, se deberá definir una acción como mínimo por cada etapa del ciclo PHVA (planear, hacer, verificar y actuar), así mismo las fechas de ejecución de las actividades.

Las acciones de mejora, preventivas o correctivas formuladas en los planes de tratamiento, deberán tener relación directa con los riesgos identificados y se establecerán de acuerdo con el seguimiento que se realice al desempeño del Sistema de Gestión de Seguridad y Salud en el Trabajo de conformidad con el procedimiento de acciones correctivas, preventivas y de mejora.

ANEXO 2

GUÍA PARA LA GESTIÓN DE RIESGOS DE EMERGENCIA, CRISIS Y SEGURIDAD PÚBLICA EN LA UNIDAD PARA LA ATENCIÓN A LAS VÍCTIMAS

CAPITULO I
ASPECTOS GENERALES

1.1. INTRODUCCIÓN

La Unidad para la Atención y Reparación Integral a las Víctimas en cumplimiento de las actividades propias de su misión desde la Dirección Nacional y Direcciones Territoriales, para atender de manera oportuna las situaciones de calamidad, desastre, emergencia y crisis según sea el caso, considera necesario identificar las diversas amenazas y vulnerabilidades que acorde con el origen (natural o antrópico) generan algún tipo de impacto en su operación.

Por lo anterior, se debe analizar el riesgo como el daño potencial que, puede ocurrir a la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada, por la materialización de amenazas. Así mismo debe definirlo como el producto entre Probabilidad (P) y Severidad (S), en función de condiciones amenazantes y hechos particulares de vulnerabilidad.

De acuerdo con lo expuesto, la gestión para este tipo de riesgos debe contemplar:

- Una planeación para la implementación de controles que permitan la prevención, mitigación o reducción del riesgo.

- Una adecuada y eficiente evaluación que permita establecer la naturaleza del riesgo, su facilidad de acceso (posibilidad de exposición), las características del sector y/o población expuesta (receptor), la posibilidad de que ocurra y la magnitud de exposición y sus consecuencias, con el fin de tomar las medidas necesarias que permitan minimizar los impactos que ocasión de los riesgos se puedan generar.

- Un análisis que permita identificar los peligros asociados con cada uno de los riesgos, entendiendo a estos peligros como el potencial de causar algún tipo de daño.

1.2. Objetivo

Establecer un instrumento en virtud del cual, se definan los procedimientos para dar una respuesta oportuna ante cualquier amenaza de origen natural, social y antrópicas que ponga en riesgo a los funcionarios, colaboradores y demás personas involucradas, en las instalaciones de la Unidad para las víctimas o cumpliendo sus actividades en el territorio.

1.3. Políticas de gestión de riesgo de emergencia, crisis y seguridad pública

Para garantizar la efectiva gestión de los riesgos de emergencia, crisis y seguridad pública, en el marco de la primera línea defensa dimensión 7 de MIPG, se establecen las siguientes políticas:

- El riesgo debe ser valorado y evaluado frente a las amenazas identificadas, mediante la metodología de valoración preliminar del riesgo establecida por la Unidad.

- Las actividades establecidas para la prevención, preparación y respuesta ante emergencias o crisis, deben contar con recursos de tipo físicos, humanos y tecnológicos necesarios.

- Se debe evaluar periódicamente la situación de vulnerabilidad de las sedes de la Unidad para la Atención a Víctimas frente a las amenazas identificadas.

- Establecer acciones que permitan prevenir, mitigar, controlar y superar los impactos ambientales adversos provocados por situaciones de emergencia o crisis.

- Se debe contar con un Comité de Manejo de Crisis y Comunicaciones Estratégicas para la atención eficiente y eficaz, de la emergencia o crisis a nivel central o territorial.

- Se debe diseñar e implementar planes de acción y contingencia para la prevención y atención de emergencias o crisis.

- Realizar capacitaciones periódicas a los funcionarios del nivel central y territorial con relación a los planes de emergencias y contingencias diseñados por la Unidad para las Víctimas.

- Definir protocolos y acciones orientadas a generar en los brigadistas, y colaboradores con los conocimientos y la información necesaria para responder de manera oportuna, segura y efectiva frente a condiciones de riesgo y amenazas que puedan convertirse en una emergencia o crisis, y que pongan en peligro su vida o integridad, así como también la de sus compañeros, visitantes o partes interesadas, o la afectación al medio ambiente.

- Los eventos y situaciones que puedan materializar los riesgos que generen crisis a nivel central y territorial de la Unidad, serán gestionados de acuerdo con lo señalado en el manual de manejo de crisis y comunicaciones estratégicas, el cual será parte integral de la metodología de riesgos de la Entidad.

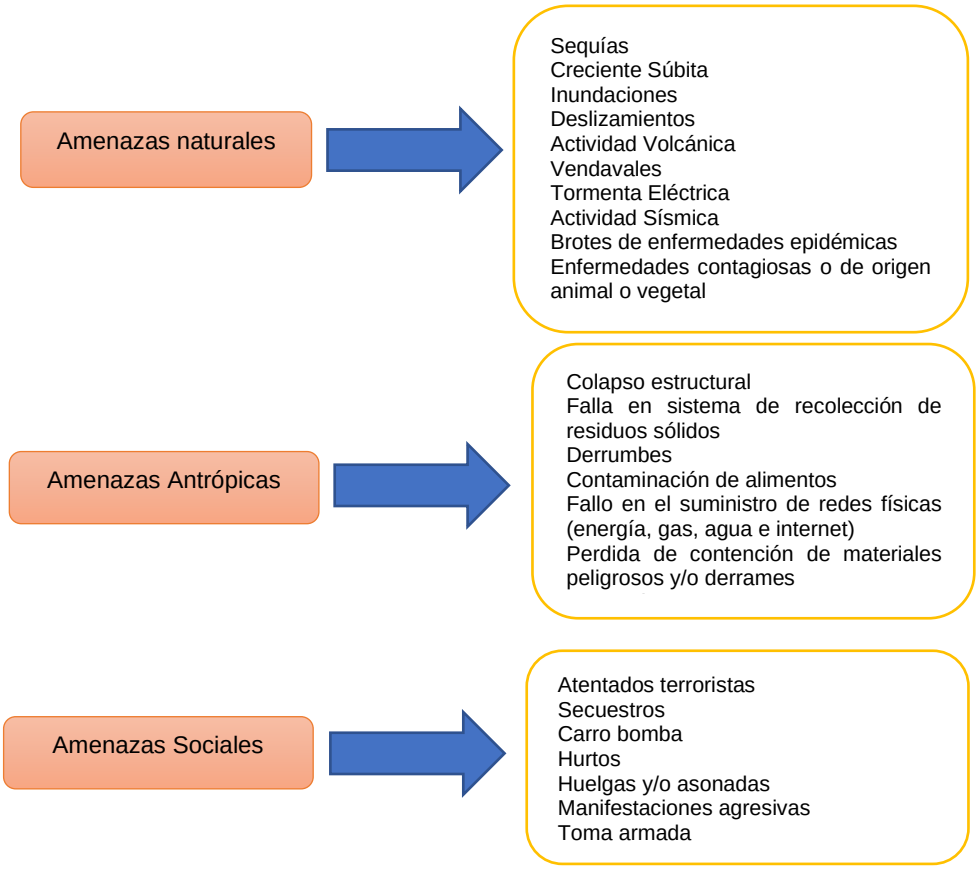
CAPITULO II

GESTION DE RIESGOS DE EMERGENCIA, CRISIS Y SEGURIDAD PÚBLICA

2.1. Identificación de Amenazas

Es de gran importancia conocer las amenazas, derivadas de situaciones que se puedan presentar con ocasión de fenómenos físicos de origen natural, socio-natural o antrópico no intencional, las cuales pueden causar daño a la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada, funcionarios y colaboradores de la Unidad. Por consiguiente, es necesario identificar las amenazas.

De acuerdo con ello, se deben tener en cuenta los siguientes aspectos:



2.2. Factores que afectan la amenaza y el riesgo

Al momento de analizar las amenazas y elementos vulnerables, se debe considerar los factores que pueden generar situaciones que pueden aumentar o disminuir el riesgo.

Adicionalmente, se establecerá una metodología presentada que involucra los siguientes aspectos:

- Análisis de las amenazas que generen situaciones de emergencias o crisis
- Identificar las fuentes de riesgo y amenazas
- Clasificar las consecuencias de la emergencia o crisis
- Determinación de la probabilidad y asignación de rangos de acuerdo con la probabilidad
- Informar los resultados del análisis

2.3. Valorización de las consecuencias

Una vez identificadas las amenazas, se determinará el nivel de riesgo, los cuales deben ser ajustados según el análisis efectuado teniendo en cuenta la particularidad de cada uno de ellos.

2.4. Elementos de Gestión en Seguridad y Salud en el Trabajo.

Se tendrán en cuenta los siguientes aspectos orientados a la prevención, mitigación y superación del riesgo con base en el resultado del siguiente cuestionario el cual se clasificará de la siguiente manera:

RANGO	CALIFICACIÓN
De 20 a 25 puntos	20%
De 13 a 19 puntos	15%
De 7 a 12 puntos	10%
De 1 a 6 puntos	5%
0 puntos	0%

	SEGURIDAD	SI (0)	PARCIALMENTE (0.5)	NO (1)
1	Se tiene un Sistema de Gestión de Seguridad y Salud en el Trabajo implementado, socializado y documentado			
2	La Política de Seguridad, Salud en el Trabajo se encuentra documentada y socializada entre los funcionarios, colaboradores, proveedores y otras partes interesadas			
3	Se encuentran identificados los requisitos legales aplicables a Seguridad y Salud en el trabajo.			
4	Se aplica el procedimiento de evaluación de la Implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo			

5	Se tienen canales de recolección de inquietudes y aportes de los funcionarios y colaboradores en materia de seguridad y salud en el trabajo.			
6	Se tienen cartillas de prevención de desastres			
7	Para la identificación y valoración de los peligros que pueden ocurrir en la sede central y las sedes territoriales se utiliza la metodología diseñada para tal efecto.			
8	Se tiene un mecanismo de reporte de los accidentes de trabajo			
9	Se tiene diseñado y aprobado un plan de emergencias y contingencias para responder de manera oportuna a las situaciones que afecten el desarrollo normal de las actividades de la Unidad originadas por amenazas naturales, social y antrópicas no intencionales.			
10	Se cuenta con brigadas de emergencia.			
11	El Comité de Manejo de Crisis y Comunicaciones Estratégicas – COMR, cuenta con los lineamientos específicos para actuar oportunamente en situaciones de crisis.			
12	Se cuenta con programas de capacitación especiales para los integrantes de las brigadas de emergencias e integrantes del COMR			
13	La Unidad ha establecidos los requisitos necesarios para desempeñar cada trabajo y proporcionar a los funcionarios y colaboradores la inducción y reducción necesaria para el cumplimiento de sus funciones u obligaciones según sea el caso.			
14	Se realizan capacitaciones periódicas en materia de Seguridad y Salud en el Trabajo.			
15	Se tienen plenamente identificadas las actividades de alto riesgo en las que se podrían generar accidentes o sucesos debido a fallas humanas.			
16	Dentro de las obligaciones de los contratistas se incluye el cumplimiento de las normas de seguridad y salud en el trabajo.			
17	Se garantiza la dotación de equipos de protección y otras medidas de seguridad, a los funcionarios y colaboradores teniendo cuenta las actividades a realizar.			
18	Las instalaciones de la Unida a nivel central y territorial, cuenta con alarmas, extintores, botiquines, detectores de humo, etc.			
19	Las rutas de evacuación se encuentran debidamente señalizadas.			
20	La unidad realiza simulacros al menos una vez al año con la participación de todos los funcionarios y colaboradores			
	SALUD	**SI (0)**	**PARCIALMENTE (0.5)**	**NO (1)**
21	En el diseño de los procedimientos relacionados con un ambiente laboral sano y seguro participan los funcionarios de la Unidad			
22	Las amenazas identificadas que puedan generar emergencias o crisis son de conocimiento de los funcionarios y colaboradores.			
23	Se realiza la evaluación de aptitudes físicas del personal según sea la tarea asignada.			
24	Se cumple con el protocolo de exámenes de salud ocupacional para el ingreso de funcionarios y colaboradores			
25	Se clasifican los equipos de seguridad y de protección personal de acuerdo con los riesgos y amenazas a las cuales pueden estar expuestos los funcionarios y colaboradores en virtud del cumplimiento de sus funciones u obligaciones según sea el caso.			

2.5. Elementos Ambientales

Para realizar la calificación de los elementos ambientales, se considerarán los siguientes aspectos donde un puntaje alto significa un riesgo ambiental alto de acuerdo con los siguientes porcentajes:

RANGO	CALIFICACIÓN
De 10 a 8 puntos	20%
De 7 a 5 puntos	15%
De 5 a 3 puntos	10%
De 1 a 2 puntos	5%
0 puntos	0%

	AMBIENTE	VERDADERO (1)	FALSO (0)
1	La Política Ambiental no se encuentra documentada y socializada a los funcionarios, colaboradores, proveedores y otras partes interesadas.		
2	A nivel central y territorial no se tiene un Plan de Gestión Ambiental		
3	Los requisitos legales aplicables a los aspectos ambientales, no se encuentran identificados		
4	No se realizan campañas de sensibilización para el manejo de residuos y materiales		
5	No se cuentan con mecanismos que permita reducir el uso de materiales no recicles.		
6	No se realizan campañas de sensibilización de uso del papel		
7	No se utilizan las herramientas tecnológicas para realizar campañas de ahorro de energía y agua		
8	No se cuenta con una metodología de gestión de riesgos ambientales		
9	No se cuenta con una matriz donde se identifiquen las circunstancias o hechos que se puedan configurar en riesgos ambientales		
10	No se tiene plena identificación de las zonas ambientales sensibles y de alto riesgo en las cuales se deba realizar actividades propias de la misión de la entidad		

2.6. roles de las líneas de defensa frente a la gestión del riesgo de riesgos de emergencia, crisis y seguridad pública

LÍNEA ESTRATÉGICA	Definir un instrumento para la gestión del riesgo y el control. Conocer los informes sobre la materialización de riesgos que generen emergencia o crisis y las causas que los originaron. Realizar seguimiento a los resultados de las evaluaciones realizadas por la Oficina de Control Interno.

PRIMERA LÍNEA DE DEFENSA

Definir los lineamientos para garantizar la efectiva administración de los riesgos que generen emergencia o crisis.

Impartir las directrices sobre las cuales funcionará el COMR

Revisar las medidas de control y actividades de intervención implementadas para cada causa que pueda derivar la materialización de un riesgo

Revisar y hacer seguimiento al cumplimiento de las medidas de control, diseñados para la mitigación del riesgo propuestas por el COMR

Revisar las actualizaciones de la matriz de identificación de peligros, valoración de riesgos

Emitir lineamientos encaminados al cumplimiento de las funciones del Comité de Nacional y Territorial de Manejo de Crisis y Comunicaciones

Establecer directrices y apoyo en la identificación, análisis, evaluación de controles y tratamiento de los riesgos.

Revisar el diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones para su fortalecimiento.

Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo.

Verificar el cumplimiento de los protocolos de seguridad diseñados

ANEXO 3

GUÍA PARA LA GESTIÓN DE RIESGOS AMBIENTALES EN LA UNIDAD PARA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS

CAPITULO I
ASPECTOS GENERALES

1.1. INTRODUCCIÓN

La gestión del riesgo ambiental busca garantizar el cumplimiento de los objetivos y metas trazados por la Unidad para prevenir y reducir los efectos no deseados, incluyendo las condiciones adversas no deseadas en materia ambiental.

Lo anterior tomando como insumo el análisis del contexto interno y externo tanto a nivel central como territorial; así como, los resultados de la identificación y evaluación de los aspectos e impactos, requisitos legales y otros requisitos aplicables para el logro de los objetivos y el desempeño ambiental.

En consecuencia, se han establecido en el marco de la primera línea de defensa de la dimensión 7 de MIPG, los lineamientos que permitan la identificación y gestión de los riesgos del sistema de gestión ambiental, con el fin de prevenir la probabilidad de ocurrencia y el impacto de estos, a través de la formulación e implementación de controles efectivos.

1.2. Objetivos

Identificar y analizar los riesgos que pueden afectar el desempeño del sistema de gestión ambiental de la unidad y que deban ser considerados en los procesos de planeación estratégica y toma de decisiones de la Entidad.

Establecer los controles efectivos que garanticen el cumplimiento de los lineamientos para la gestión de riesgos ambientales.

1.3. Políticas para la gestión de riesgo ambiental

- La identificación y actualización de riesgo ambiental se realizará anualmente en los niveles central y territorial de la Unidad, cuando identifiquen:

  - ✓ Modificaciones en los requisitos legales y otros requisitos relacionados con el eje ambiental.
  - ✓ Modificaciones en los procesos que involucren el sistema ambiental
  - ✓ Cambios en el contexto interno y externo del eje ambiental.
  - ✓ Situaciones que tengan impactos ambientales
  - ✓ Cambios de las partes interesadas y sus necesidades y expectativas
  - ✓ Variaciones en los resultados de los indicadores del eje ambiental

- ✓ Aspectos relevantes en el resultado de la Revisión por la Dirección General

- Para la formulación de los planes de tratamiento se deberá definir una acción como mínimo por cada etapa del ciclo PHVA, así mismo, las acciones de los planes de tratamiento deberán tener relación directa con los riesgos identificados.

- Para la formulación de los planes de tratamiento se deberá contar con los recursos de talento humano, financieros, tecnológicos y demás que se requieran para la gestión de los riesgos identificados.

- Se deberá socializar la matriz de riesgos identificados y los planes de tratamiento con las actividades para su mitigación a todos los funcionarios y colaboradores de la Unidad para las Víctimas.

- Cuando se presente incumplimientos reiterativos de los planes de tratamiento o cuando se materialicen riesgos, se deberá determinar la pertinencia de generar una acción correctiva teniendo en cuenta la necesidad de recursos para su ejecución.

CAPITULO II
GESTION DEL RIESGO AMBIENTAL

2.1. Actividades para la Gestión de Riesgos

Para la identificación de los riesgos ambientales y la determinación de sus controles, el Grupo de Gestión administrativa y documental realiza la identificación y evaluación de aspectos e impactos ambientales acorde a lo establecido en la ISO 14001 cuyos resultados se encuentran documentados en la “Matriz de identificación de aspectos e impactos ambientales”, la cual sirve como instrumento de valoración de impactos ambientes asociados a las actividades, productos y servicios de la unidad.

2.2. Identificación de aspectos e impactos ambientales

La identificación de aspectos ambientales parte del ejercicio de análisis interpretativo de la situación ambiental y la revisión a los procedimientos asociados a los procesos de la entidad, identificando las actividades y productos (bienes y/o servicios) que interactúan con el ambiente en diferentes escenarios.

A partir de la identificación de los aspectos ambientales asociados a los diferentes procesos, productos, servicios o actividades que desarrolla la Entidad, se identifica el impacto ambiental asociado (Contaminación al recurso aire, Contaminación al recurso agua, Agotamiento de los recursos naturales, Contaminación del recurso suelo, Consumo excesivo de energía y agua, Afectación a la fauna, afectación a la flora, afectación a la salud humana). Dichos impactos pueden ser positivos o negativos.

Para el análisis de los riesgos identificados y sus consecuencias, se requiere hacer una breve descripción de cómo se presenta o manifiesta el riesgo propuesto.

Posteriormente se deberá establecer las causas, es decir, los elementos o actividades que pueden propiciar o desencadenar la ocurrencia del riesgo por factores internos o externos del entorno.

2.3. Parámetros de evaluación de impacto ambiental.

La evaluación de los impactos ambientales identificados consiste en estimar el impacto ambiental a través de una interpretación cuantitativa, identificando sus atributos, así como el cumplimiento normativo en relación con el aspecto y/o el impacto ambiental identificado. La importancia del impacto se cuantifica de acuerdo con los criterios legales, partes interesadas e Impacto ambiental (Frecuencia, severidad y alcance). Esta valoración se debe realizar en el formato "Matriz de identificación y evaluación de aspectos e impactos ambientales" por el ingeniero ambiental del proceso de Gestión Administrativa encargado del Subsistema de Gestión Ambiental.

Criterio Legal - CL

Este parámetro considera la existencia de un requisito legal (ley, decreto, resolución, ordenanza), de un requerimiento contractual o de un compromiso adquirido a nivel institucional relacionado con el Aspecto Ambiental que se está valorando; así como el grado de cumplimiento del mismo.

Existencia de un requisito	Valor
No existe requisito legal, contractual o institucional	1
Existe requisito legal, contractual o institucional	10

Cumplimiento del requisito	Valor
No aplica	1
Si cumple	5
No cumple	10

Se valora en la matriz de aspectos ambientales mediante la siguiente fórmula:

$$CL = Existencia * Cumplimiento$$

Se identifica a normatividad ambiental relacionada con cada uno de los impactos ambientales generados, estos pueden ser leyes, decretos y resoluciones.

Criterio Partes Interesadas - CPI

Este parámetro tiene en cuenta que la principal parte interesada en un Sistema de Gestión Ambiental es la comunidad, aunque también tiene en cuenta clientes, proveedores, contratistas, entidades financieras entre otros; se evalúa si existen reclamaciones, solicitudes, quejas o reclamos relacionados con el aspecto ambiental evaluado y si a estos se les hace la gestión correspondiente.

Exigencia	Valor
No se han presentado ni existen peticiones, quejas, solicitudes o reclamos relacionado con el aspecto ambiental evaluado	1
No se han presentado ni existen peticiones, quejas, solicitudes o reclamos relacionados sin implicaciones legales	5
Se presenta, existe o se ha presentado queja, reclamo solicitud con implicaciones legales	10

Cumplimiento del requisito	Valor
Se realizó la gestión correspondiente y se solucionó el tema	1
Se ha realizado la gestión, aunque la petición sigue vigente	5
No se ha hecho gestión o esta no ha sido efectiva	10

Este criterio se valora en la matriz de aspectos ambientales mediante la siguiente fórmula:

$$CPI = Exigencia * Gestión$$

Criterio Impacto Ambiental - CIA

Un impacto ambiental tiene diversos atributos, para la valoración de estos se utilizarán los parámetros correspondientes a: Frecuencia: hace referencia al número de veces que se presenta el impacto ambiental en un lapso, este puede ser diario, mensual o anual y se valora de acuerdo con la siguiente tabla:

FRECUENCIA	VALOR
Anual o semestral	1
Trimestral, bimensual o mensual	5
Semanal o diario	10

Severidad: se refiere a la cantidad de daño o beneficio1 - cambio, que hace el impacto ambiental en el recurso natural y se valora mediante la siguiente tabla:

SEVERIDAD	VALOR
Leve, no es perceptible el daño o el beneficio en el ambiente	1
Moderado, el cambio es notorio de alguna forma	5
Considerable, el cambio en el medio ambiente es fácilmente notable	10

Alcance: denota el área o extensión geográfica en la que se presenta el impacto ambiental valorándose de acuerdo con la siguiente tabla:

ALCANCE	VALOR
Puntual, el impacto ambiental se manifiesta	1
Local, el impacto ambiental se presenta en un área mayor, aunque no sobrepasa los límites del ente territorial	5
Extenso, impacto ambiental puede presentarse en varias regiones del país	10

El criterio de impacto ambiental se evalúa en la matriz de aspectos ambientales, por medio de la siguiente fórmula:

$$CIA = Frecuencia * 3.5 + Severidad * 3.5 + Alcance * 3$$

Luego, la Significancia Total – ST - del impacto ambiental se valora cuantitativamente mediante la siguiente ecuación que relaciona los criterios anteriormente expuestos:

$$ST = 0.5 * CL + 0.35 * CIA + 0.15 * CP$$

Debido a que los Impactos Ambientales pueden ser adversos o beneficiosos, el carácter de cada impacto ambiental se tiene en cuenta afectando la Significancia Total con un signo (-) para los impactos adversos.

Es necesario tener en cuenta que no todos los impactos ambientales los causa la Entidad directamente, por ejemplo, el papel se fabrica a partir de la madera de los árboles, sin embargo, la Entidad no tala esos árboles, por lo tanto, este es un Impacto Ambiental Indirecto que por principio la Organización debe gestionar.

Posteriormente, los resultados cuantitativos se interpretan cualitativamente de acuerdo con los siguientes intervalos en el valor de la Significancia Total:

SIGNIFICANCIA TOTAL	VALORACIÓN CUALITATIVA	CONTROLES
ST ≤ -75	SIGNIFICANCIA ALTA	Objetivos, Programas y Metas
-55 ≤ ST < -75	SIGNIFICANCIA MEDIA	Objetivos, Programas y Metas
-39 ≤ ST < -55	SIGNIFICANCIA BAJA	Controles Operacionales
-4 ≤ ST < -39	SIN SIGNIFICANCIA	Sin control hasta manejar los anteriores
ST > 4	SIGIFICANCIA POSITIVA	Se comunica y promueve

Se tiene en consideración el impacto ambiental que se genera por las actividades de la Entidad en todo el ciclo de vida de servicio prestado, englobando todas las necesidades de análisis y evaluación de cuestiones ambientales en cada una de las etapas que se encuentran bajo control o influencia de la Unidad, donde incluimos desde adquisición de productos y servicios necesarios para la prestación del servicio hasta el uso y tratamiento al finalizar la vida del servicio, pasando por los diferentes procesos de la Entidad.

Finalmente, se identifica la etapa del ciclo de vida de los servicios que presta la unidad, con la cual está relacionado el impacto ambiental generado.

2.3.1. Ciclo de vida

El ciclo de vida se refiere a las diferentes etapas que tienen los productos o servicios que termina con la disposición final de los aspectos ambientales con el fin de disminuir en cantidad y significancia los impactos ambientales que se puedan causar. Para el caso de la Unidad para las Victimas, se identificaron cuatro etapas del ciclo de vida de los servicios que se prestan, estos son:

- Adquisición de productos y/o servicios: son los productos o servicios necesarios para que la Unidad pueda funcionar y prestar sus servicios a las partes interesadas, entre ellos se pueden encontrar los insumos de papelería, equipos eléctricos y electrónicos, infraestructura física y elementos para su mantenimiento, servicios de transporte, aseo y cafetería, acueducto, alcantarillado y energía eléctrica.

- Diseño y operación del servicio: en esta etapa se da uso a los diferentes servicios y productos adquiridos, por lo que es donde se generan los aspectos ambientales de forma directa.

- Productos generados: hace referencia a todos los productos obtenidos mediante el desarrollo de las actividades de los diferentes procesos de la Unidad, estos productos en su mayoría es información documentada tanto de manera física como digital.

Disposición final: en la etapa final se disponen todos los residuos generados durante la etapa de operación, en donde la mayoría de los residuos que se producen corresponden a residuos sólidos (residuos ordinarios y material reciclable), residuos peligroso y vertimientos.

Cada aspecto ambiental será clasificado en una de las etapas anteriores y se tendrá en cuenta la tabla anexa del formato “Matriz de identificación y evaluación de aspectos e impactos ambientales” en donde se relacionan las etapas del ciclo de vida, las actividades realizadas en las etapas, los aspectos ambientales asociados, los controles mediante los cuales se establecen actividades que permitan mantener en niveles bajos o reducir la magnitud de los impactos ambientales, y las evidencias que permitan la verificación del control.

2.4. Determinación de controles.

Se evalúan las actividades asociadas con los aspectos significativos identificados, debe asegurarse la realización de tal forma que permita el control o la reducción de los impactos adversos asociados con ellos, para dar cumplimiento a la política ambiental, objetivos y metas ambientales definidas en los programas de gestión ambiental.

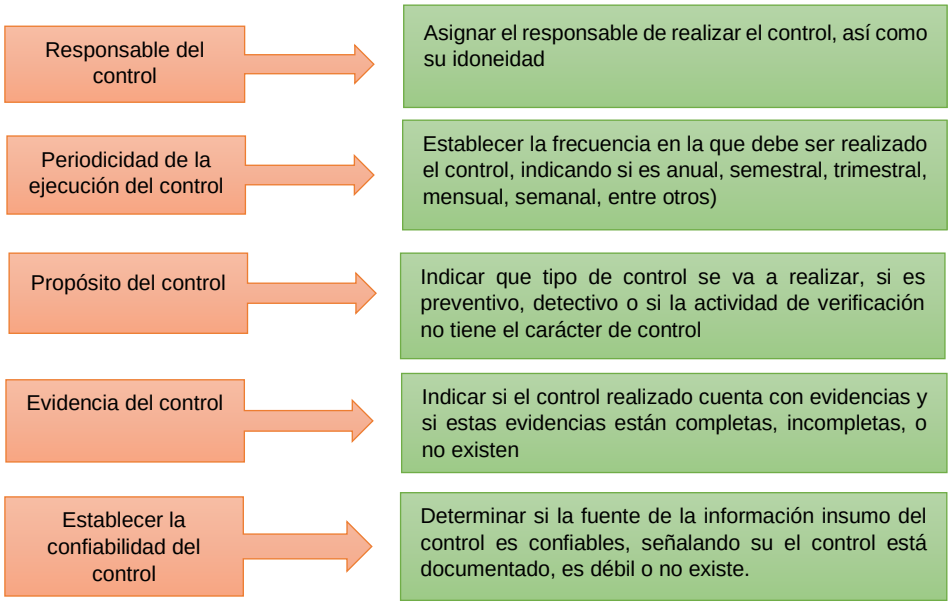
El Control operacional hace referencia a los procedimientos, prácticas o actividades que aseguran y mantienen un nivel permitido, disminuyen o evitan los impactos originados por los aspectos ambientales.

Teniendo en cuenta lo anterior, y cuando un impacto ambiental sea generado por un hecho considerado de significancia “ALTA” y “MEDIA”, se requiere definir un control operacional, para lo cual debe atenderse a lo siguiente:

- Procedimientos
- Programas de gestión ambiental
- Objetivos ambientales
- Metas y se asignará el proceso responsable para definir el control y realizar seguimiento.

En el evento que un impacto ambiental sea considerado con significancia “BAJA” y “NO SIGNIFICATIVA”, se deberá manejar sin control, hasta manejar los anteriores.

Al realizar la descripción del control, es necesario determinar la responsabilidad frente a las actividades o mecanismos que impliquen el cumplimiento de estos:

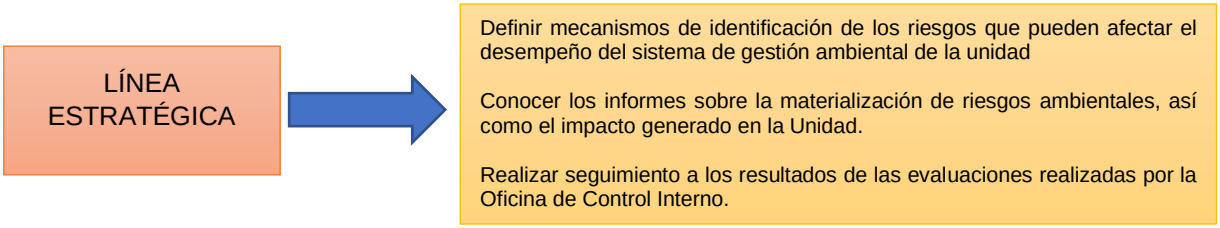


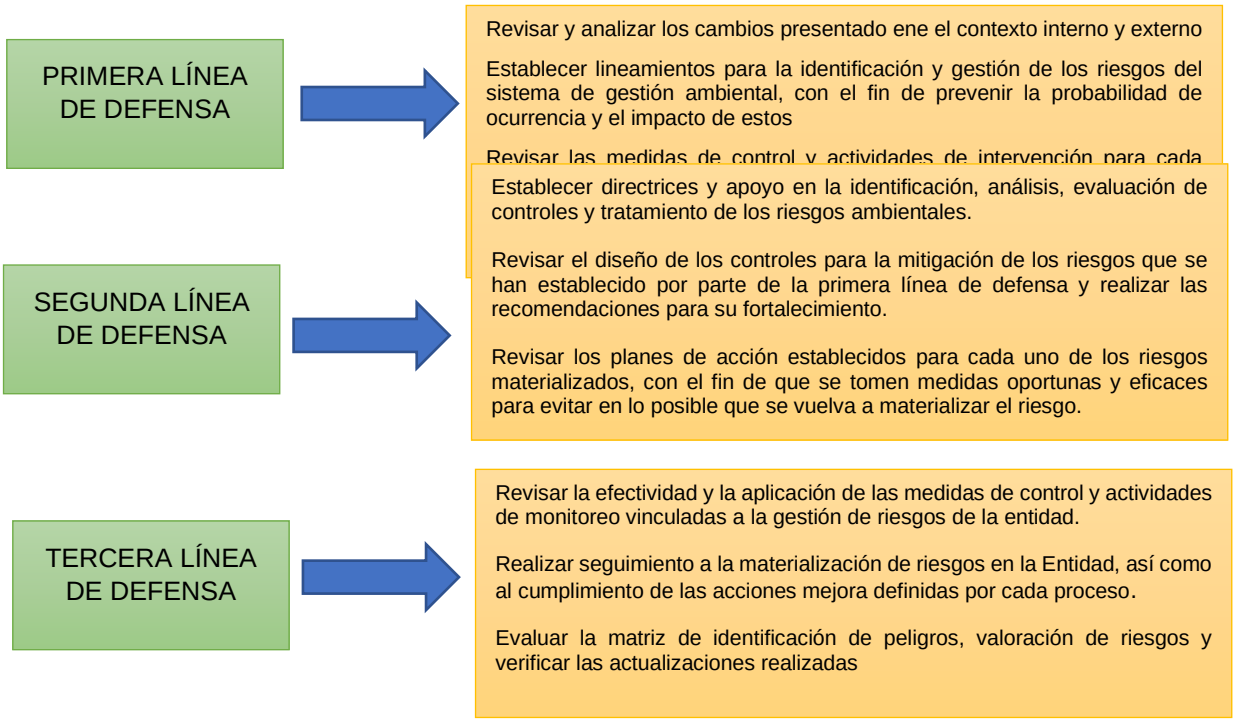
2.5. Seguimiento y reporte

El monitoreo y revisión de los riesgos ambientales y los controles establecidos en la Unidad para las Víctimas, deberán realizarse de manera mensual, registrando los resultados de cada una de las actividades desarrolladas en las Matriz de Riesgos, así como las evidencias correspondientes a los controles realizados.

Una vez realizado el monitoreo, es necesario elaborar los informes o reportes que den cuenta del resultado de la verificación efectuada, se procederá a la revisión y validación de esta información con el fin de efectuar la correspondiente medición de la gestión del Riesgo.

2.6. Roles de las líneas de defensa frente a la gestión del riesgo gestión de riesgos ambientales




PRIMERA LÍNEA DE DEFENSA
Revisar y analizar los cambios presentado ene el contexto interno y externo
Establecer lineamientos para la identificación y gestión de los riesgos del sistema de gestión ambiental, con el fin de prevenir la probabilidad de ocurrencia y el impacto de estos
Revisar las medidas de control y actividades de intervención para cada
SEGUNDA LÍNEA DE DEFENSA
Establecer directrices y apoyo en la identificación, análisis, evaluación de controles y tratamiento de los riesgos ambientales.
Revisar el diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones para su fortalecimiento.
Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo.
TERCERA LÍNEA DE DEFENSA
Revisar la efectividad y la aplicación de las medidas de control y actividades de monitoreo vinculadas a la gestión de riesgos de la entidad.
Realizar seguimiento a la materialización de riesgos en la Entidad, así como al cumplimiento de las acciones mejora definidas por cada proceso.
Evaluar la matriz de identificación de peligros, valoración de riesgos y verificar las actualizaciones realizadas

ANEXO 4

GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL
UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS

CAPITULO I
ASPECTOS GENERALES

1.1. INTRODUCCIÓN

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital, tienen como propósito brindar los lineamientos para la identificación, análisis y tratamiento de los riesgos que puedan generar afectación en el cumplimiento de los objetivos en los diferentes procesos de la entidad, facilitando de esta manera la toma de decisiones en la prevención, mitigación y control respecto a la materialización de los mismos.

De acuerdo con lo expuesto, se tiene como marco de referencia el siguiente:

- Estándar Internacional **ISO 31000:2018**
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital – **DAFP**,
- Conpes 3854 de 2016
- Modelo de Seguridad y Privacidad de la Información del MinTIC
- Norma Técnica Colombiana NTC-ISO/IEC 27005
- Ley 1448 de 2011, “por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno en Colombia”
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y el Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
- Ley Estatutaria 1581 de 2012, “por la cual se dictan disposiciones generales para la protección de datos personales”.

1.2. Objetivo:

Establecer los lineamientos que garanticen la óptima gestión de riesgos de seguridad de la información y seguridad digital de la Unidad para la Atención y Reparación Integral a las Víctimas- UARIV-

1.3. Políticas para la gestión de riesgos de seguridad de la información y seguridad digital

- Para garantizar la adecuada gestión de los riesgos será necesario realizar un análisis previo de la entidad considerando aspectos generales como la Misión, Visión, objetivos y Planeación Institucional. Adicionalmente, se deberá tener un claro conocimiento del modelo de operación por procesos considerando sus caracterizaciones y actividades principales.

- Deberá establecerse una matriz de riesgos para la gestión de riesgos de seguridad de la información y seguridad digital, la cual considerará el análisis del contexto, la identificación, análisis, valoración, tratamiento y evaluación del riesgo y la oportunidad de mejora con base en lo anterior.

- En el evento de no identificarse los riesgos, es necesario soportarlo a través de un memorando emitido a la Oficina de Tecnologías de la Información - OTI.

CAPITULO II

GESTIÓN DEL RIESGO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL

2.1. Identificación de 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, teniendo en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual es necesario identificar:

a) Los 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 v2, del Proceso de gestión documental.

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.

b) Identificación de Amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar

todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas) (MINTIC, 2016, p.19).

Para la metodología de gestión de riesgos de seguridad de la información, se adopta el listado de amenazas comunes plantado por la norma ISO/IEC 27005:2008:
Dónde: A = Accidentales; D= Deliberadas; y E= Ambientales.

Tipo	Amenazas	Origen
Daño físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Tabla 2. Amenazas comunes (ICONTEC, 2009, p.49).

Según la guía 7 de gestión de riesgos del MinTIC, se recomienda tener especial atención a las fuentes de amenazas humanas, que se listan a continuación:

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso	Reto Ego Rebelión Estatus Dinero	Piratería Ingeniería social Intrusión, accesos forzados al sistema Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador (por ejemplo: espionaje cibernético) Acto fraudulento (repetición, personificación, interceptación)

		Soborno de la información Suplantación de identidad Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/terrorismo Guerra de la información (warfare) Ataques contra el sistema (negación distribuida del servicio) Penetración del sistema Manipulación del sistema
Fuente de amenaza	**Motivación**	**Acciones amenazantes**
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja política Explotación económica Hurto de información Intrusión en la privacidad personal Ingeniería social Penetración en el sistema Acceso no autorizado al sistema (acceso a información clasificada de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencias Ganancia monetaria Venganza Errores y omisiones no intencionales (error en el ingreso de los datos, error de programación)	Asalto a empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingresos de datos falsos o corruptos Interceptación Código malicioso (virus, bomba lógica, troyano) Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema

Tabla 3. Amenazas humanas (ICONTEC, 2009, p.50).

2.2. Identificación de Vulnerabilidades

Según la Norma ISO/IEC 27005:2008 y la guía 7 para la gestión de riesgos del MinTIC, se pueden identificar vulnerabilidades en las siguientes áreas:

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
1	Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
2		Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
3		Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
4		Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
5		Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
6		Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
7		Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
8		Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
9		Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
10		Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
11		Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
12		Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
13		Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
14		Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
15		Ausencia de planes de continuidad	Falla del equipo
16		Ausencia de políticas sobre el uso del correo electrónico	Falla del equipo
17		Ausencia de procedimientos para la introducción del software en los sistemas operativos	Falla del equipo
18		Ausencia de registros en las bitácoras (logs) de administrador y operario	Falla del equipo
19		Ausencia de procedimientos para el manejo de información clasificada	Falla del equipo
20		Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Falla del equipo
21		Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
22		Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
23		Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
24		Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
25		Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
26		Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
27		Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
28		Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
29		Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
30		Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado
31	Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
32		Ubicación en un área susceptible de inundación	Inundación
33		Red energética inestable	Pérdida del suministro de energía
34		Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
35	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
36		Procedimientos inadecuados de contratación	Destrucción de equipos o medios
37		Entrenamiento insuficiente en seguridad	Error en el uso
38		Uso incorrecto de software y hardware	Error en el uso
39		Falta de conciencia acerca de la seguridad	Error en el uso
40		Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
41		Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
42		Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
43	Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
44		Líneas de comunicación sin protección	Escucha encubierta
45		Tráfico sensible sin protección	Escucha encubierta
46		Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
47		Punto único de falla	Falla del equipo de telecomunicaciones
48		Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
49		Arquitectura insegura de la red	Espionaje remoto
50		Transferencia de contraseñas en claro	Espionaje remoto
51		Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
52	Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
53		Defectos bien conocidos en el software	Abuso de los derechos

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
54		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
55		Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
56		Ausencia de pistas de auditoria	Abuso de los derechos
57		Asignación errada de los derechos de acceso	Abuso de los derechos
58		Software ampliamente distribuido	Corrupción de datos
59		En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
60		Interfaz de usuario compleja	Error en el uso
61		Ausencia de documentación	Error en el uso
62		Configuración incorrecta de parámetros	Error en el uso
63		Fechas incorrectas	Error en el uso
64		Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
65		Tablas de contraseñas sin protección	Falsificación de derechos
66		Gestión deficiente de las contraseñas	Falsificación de derechos
67		Habilitación de servicios innecesarios	Procesamiento ilegal de datos
68		Software nuevo o inmaduro	Mal funcionamiento del software
69		Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
70		Ausencia de control de cambios eficaz	Mal funcionamiento del software
71		Descarga y uso no controlados de software	Manipulación con software
72		Ausencia de copias de respaldo	Manipulación con software
73		Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
74		Falla en la producción de informes de gestión	Uso no autorizado del equipo
75	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
76		Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o de medios.
77		Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
78		Sensibilidad a la radiación electromagnética	Radiación electromagnética
79		Ausencia de un eficiente control de cambios en la configuración	Error en el uso
80		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
81		Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos

No	Tipo / Área	Ejemplos de vulnerabilidades	Ejemplos de amenazas
82		Almacenamiento sin protección	Hurto de medios o documentos
83		Falta de cuidado en la disposición final	Hurto de medios o documentos
84		Copia no controlada	Hurto de medios o documentos

Tabla 4. Vulnerabilidades (ICONTEC, 2009, p.51).

2.3. Definición de riesgos de seguridad de la información

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad (MINTIC, 2016, p.19).

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

R: Riesgo

SEG: Seguridad

001: 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.

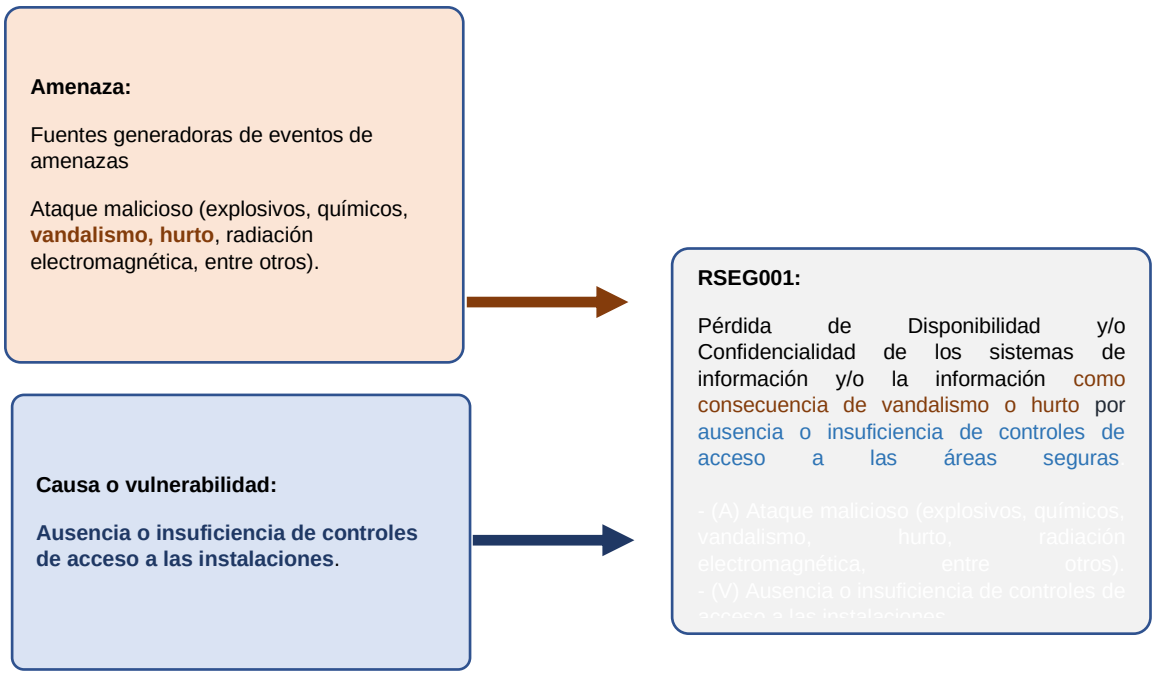


Figura 5. Ejemplo de riesgo

Para facilitar la identificación de los riesgos de seguridad de la información, se establece el listado de ejemplos de riesgos de seguridad de la información donde se asocian las amenazas y vulnerabilidades de manera global:

Listado de Riesgos seguridad de la información		Fuentes o generadoras de eventos /Amenazas	Causas o vulnerabilidades
	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.
	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.
	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	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).

	como consecuencia de captura de credenciales transferidas en texto claro, durante el ingreso vía web.		
	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.
	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.
	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.
	'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.
	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.
	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.
	Pérdida en la integridad de la Imagen y reputación de la entidad o sanciones disciplinarias y/o penales por incumplimiento de la normatividad y regulaciones ocasionadas por la divulgación no autorizada o fuga de información	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 aplicativos o incumplimiento de los términos por	Personal inconforme o molesto. Descarga y/o uso no controlado de software. Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables.

	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.	la pérdida o daño de la documentación. Incumplimiento a los acuerdos de Nivel de Servicio.	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.
	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

Una vez identificados el riesgo se debe tener en cuenta los siguientes aspectos:

- Deben redactarse en términos cualitativos
- Debe Incluir las causas y vulnerabilidades.
- Debe indicar qué atributos afectado (Confidencialidad, Integridad, Disponibilidad).

Adicionalmente, al momento de identificar el riesgo es pertinente plantear los siguientes interrogantes:

¿QUÉ PUEDE SUCEDER?

Para lo cual es necesario Identificar la afectación que conlleve la materialización del riesgo con relación al cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER?

Este interrogante nos permite establecer las causas riesgo identificadas en el contexto.

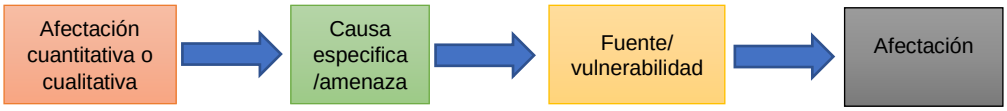
¿CUÁNDO PUEDE SUCEDER?

De acuerdo con el desarrollo del proceso la probabilidad de ocurrencia.

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

Ayuda a establecer los posibles efectos por la materialización del riesgo

Para la redacción de un riesgo, se debe tener en cuenta la siguiente estructura:



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

IDENTIFICACION					
No	**Proceso**	**Riesgo**	**Causas**	**Consecuencias**	**Tipo de Riesgo**
1	Nombre del proceso	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.	Operativas	Seguridad de la Información

Tabla 5. Ejemplo diligenciamiento matriz de riesgos

2.4. Análisis de riesgo, Evaluación del riesgo, plan de respuesta, seguimiento, monitoreo y revisión, comunicación y consulta

Para el análisis de riesgos, se tomará como referencia el aspecto cuantitativo y cualitativo, de tal manera que sea posible determinar la probabilidad en la ocurrencia de una eventualidad y el impacto generado en la materialización del riesgo.

La Probabilidad representa el número de veces que el riesgo se ha presentado o puede presentarse en un determinado tiempo.

El impacto hace referencia a magnitud de sus efectos en caso de materialización.

Para la gestión de riesgos de seguridad de la información, se adoptan los lineamientos definidos por la Oficina asesora de planeación en la metodología para la administración de riesgos de la Unidad para la Atención y reparación Integral a las Víctimas, específicamente para:

- Análisis de riesgos
- Evaluación del riesgo
- Plan de respuesta
- Seguimiento
- Monitoreo y revisión
- Comunicación y consulta

Sin embargo, a continuación, se listan los controles de seguridad de la información disponibles para los procesos de la Entidad:

- Sincronizar el almacenamiento de la información con ONE -DRIVE

- 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.
- Aceptar las actualizaciones del sistema operativo.
- Actualizar frecuentemente las contraseñas de los sistemas de información
- Validar los resultados arrojados por los buscadores web
- Evitar ingresar información personal en formularios dudosos
- Registrar el ingreso y la salida de los elementos tecnológicos, en las instalaciones de la Entidad
- Evitar transportar fuera de la Entidad información física o digital, de carácter confidencial
- Usar guaya de seguridad a equipos portátiles de la Entidad
- Portar el carné de la entidad en un lugar visible, pero al salir de la entidad es recomendable retirarlo
- No compartir credenciales de acceso a sistemas de información
- No ingresar a sitios web o enlaces sospechosos
- Borrar los tableros de las oficinas, una vez se termine la reunión
- Guardar la información física confidencial de la entidad bajo llave
- Controlar el préstamo de información física del proceso
- Revisar y controlar la información almacenada en (Totoro)
- Clasificar la información que se encuentra en el servidor de almacenamiento de información - Totoro, donde se identifique la información de gestión y la histórica
- Validar los permisos asignados sobre las carpetas del servidor de almacenamiento de información Totoro, asignando permisos de edición, consulta de la información
- Solicitar asesoría especializada en caso de ser requerida, en seguridad de la información al iniciar un proyecto.
- Identificar y clasificar los activos de información de gestión de su proceso
- Manipular la información física de manera adecuada, donde evite el deterioro de esta
- Mantener y devolver en buen estado los activos tecnológicos que le fueron otorgados por la entidad
- Reportar en mesa de servicio tecnológicos los incidentes, en caso de presentarse la pérdida, divulgación o modificación no controlada del activo de información
- Dar buen uso de los privilegios que le son otorgados en las herramientas tecnológicas de la entidad
- 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
- Registrar en una bitácora, la entrada de los equipos portátiles u otros elementos tecnológicos que requiera reportar
- Acompañar a los invitados durante la estadía en la entidad y hacerlos colocar el carnét de visitantes para su respectiva identificación
- Informar al guarda de seguridad del piso, cuando se presenten actividades sospechosas al interior del sitio de trabajo.
- Dar información institucional a los usuarios por los canales adecuados
- Evitar abrir archivos sospechosos enviados al correo electrónico
- Dar buen uso de los recursos tecnológicos que la entidad le proporciona al iniciar el contrato.

- Utilizar los recursos tecnológicos exclusivamente para el uso de la gestión de la entidad.
- Registrar por mesa de servicio la materialización de un incidente de seguridad.
- No llevar información confidencial de la entidad en memorias USB, o cd o cualquier otro medio de almacenamiento
- En caso de presentarse fuga de información por la pérdida y/o hurto del medio de almacenamiento dar aviso inmediato del incidente a la mesa de servicio
- Utilizar las herramientas que la Oficina de Tecnología de la información ofrece al requerir transportar información sensible de la entidad
- No instalar herramientas sin la debida aprobación de la Oficina de tecnología de información.
- Citar la información en documentos de manera correcta, en caso de ser utilizada en documentos públicos.
- No pegar las credenciales de acceso en papeles adheridas al equipo de cómputo
- Utilizar de manera controlada la red Wifi de la Entidad.
- Utilizar de manera adecuado el correo personal en caso de no estar restringido
- Informar a la Red nacional de información, en caso de requerir intercambio de información con entidades externas.
- No Compartir contraseñas de internet con personas ajenas a la entidad.
- Avisar a soporte tecnológico en caso de requerir instalación de herramientas tecnológicas recuerde que hay personal idóneo para realizar estos trabajos
- Dejar bajo llave, las oficinas a su cargo en el tiempo que se encuentre en ausencia
- Cambiar frecuentemente la contraseña de los sistemas de información a los que se ha dado el permiso a los funcionarios o colaboradores de la entidad.
- Llevar el adecuado control de cambios de los documentos para el debido control
- No permitir el ingreso de personal no autorizado al sitio de trabajo
- Mantener cerrado el cuarto de comunicación y/o de repositorio de información, permitir únicamente acceso al personal autorizado por la entidad
- Revisar y validar los permisos de mantenimiento que se lleven a cabo en las diferentes sedes de la entidad, en caso de ser el encargado del ingreso del personal
- No realizar pruebas a los sistemas de información con datos reales, para esos casos se requiere de la creación de datos de prueba
- Conocer los lineamientos de seguridad de la información que la entidad tiene establecido
- Leer el acuerdo de confidencialidad que se haya firmado con entidad
- Firmar acuerdos de confidencialidad
- Permitir al personal especializado, la recolección de evidencia en caso de ser requerida.
- No imprimir documentos confidenciales de la entidad, de no ser requerido.
- Recoger los documentos con información confidencial del centro de copiado del lugar de trabajo.
- Destruir la información de forma correcta en caso de no ser requerida.
- Realizar copia de respaldo de información almacenada en equipos de cómputo de manera periódica
- Asistir a las charlas que se realicen de seguridad de la información, realizadas por la entidad.

- Socializar al interior del proceso, los flashes informativos publicados y demás comunicados relacionados con seguridad de la información por la entidad de seguridad de la información.
- Gestionar con la Oficina de Tecnologías de la Información el bloqueo de puertos USB de los equipos de cómputo asignados al personal del proceso.

2.5. Roles de las líneas de defensa frente a la gestión del riesgo de seguridad de la información y seguridad digital

LÍNEA ESTRATÉGICA	Definir un instrumento para la gestión del riesgo y el control. Conocer los informes sobre la materialización de riesgos de seguridad de la información y seguridad digital, así como las causas que los originaron. Realizar seguimiento a los resultados de las evaluaciones realizadas por la Oficina de Control Interno.
PRIMERA LÍNEA DE DEFENSA	Definir los objetivos de SST, metas, responsables, frecuencia e indicadores cualitativos y cuantitativos, consistentes con la política de SST y programas establecidos por la Entidad. Impartir directrices que permitan garantizar la efectiva gestión de riegos de seguridad de la información y seguridad digital. Revisar las medidas de control y actividades de intervención para cada causa que pueda derivar la materialización de un riesgo Revisar y hacer seguimiento al cumplimiento de las medidas de control, diseñados para la mitigación del riesgo Revisar las actualizaciones de la matriz de identificación de peligros, valoración de riesgos
SEGUNDA LÍNEA DE DEFENSA	Monitorear la implementación de prácticas efectivas de gestión de riesgos de seguridad de la información y seguridad digital por parte de la primera línea de defensa. Revisar el diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones para su fortalecimiento. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo.
TERCERA LÍNEA DE DEFENSA	Revisar la efectividad y la aplicación de las medidas de control y actividades de monitoreo vinculadas a la gestión de riesgos de la entidad. Realizar seguimiento a la materialización de riesgos en la Entidad, así como al cumplimiento de las acciones mejora definidas por cada proceso. Evaluar la matriz de identificación de peligros, valoración de riesgos y verificar las actualizaciones realizadas

MANUAL PARA EL MANEJO DE CRISIS Y COMUNICACIONES ESTRATÉGICAS DE LA UNIDAD PARA LA ATENCIÓN INTEGRAL DE LAS VÍCTIMAS

1. INTRODUCCION

La Unidad para la Atención y Reparación Integral a las Víctimas cuenta para su funcionamiento con un grupo interdisciplinario y equipo técnico, que, por la naturaleza de su trabajo en la mayoría de los casos, presentan amenazas[1], vulnerabilidades[2] y riesgos[3], los cuales pueden alterar el funcionamiento y operatividad de la entidad, llevando a traumatismos en la ejecución de las actividades propias de su misionalidad.

Teniendo en cuenta lo anterior, los eventos que originan las contingencias pueden ser cambiantes, por cuanto se presentan como situaciones inesperadas, las cuales irrumpen en el curso normal de las operaciones afectando de manera integral a los individuos, colectivos instituciones o sistemas[4]; que si no se les da el manejo adecuado podrían derivar en una crisis[5], ocasionando un impacto negativo tanto en la imagen y como en la credibilidad de la entidad ante los Grupos de Interés y partes interesadas.

De acuerdo con lo expuesto, el presente manual acorde con lo señalado en la primera línea de defensa de la dimensión 7 de MIPG, se orienta al establecimiento de los lineamientos que deben seguirse para facilitar las actividades de los actores directamente involucrados en el manejo de una situación de crisis.

---

[1] Representa un peligro latente asociado con un fenómeno físico de origen natural o antrópico que puede presentarse en un sitio específico y en un tiempo determinado, produciendo efectos adversos en las personas, los bienes y/o el medio ambiente.

[2] Predisposición intrínseca de un sujeto o elemento a sufrir daño, debido a posibles acciones externas.

[3] Destrucción o pérdida esperada obtenida del producto de la probabilidad de ocurrencia de eventos peligrosos y de la vulnerabilidad de los elementos expuestos a tales amenazas, matemáticamente expresado como la probabilidad de exceder un nivel de consecuencias económicas y sociales en un cierto sitio y en un cierto período de tiempo (Spence, R.J.S. 1990."Seismic Risk Modelling - A review of Methods", 1990).

[4] Documento Universidad Nacional (2001) Qué hacer ante situaciones de riesgo. Bogotá Pág. 5.

[5] La crisis es definida como: “una situación conflictiva que entra en la esfera pública, es decir, cuando un asunto pasa a los medios de comunicación. Por lo tanto, mientras el problema se mantiene en el ámbito privado no se puede hablar de crisis”. Cavadas Gormaz María José. experta en temas de seguridad de la ciudad de Madrid, España.

“Cualquier evento que amenaza la imagen y reputación de una institución, compañía o persona, que tiene el potencial de generar publicidad negativa” y “situación que puede amenazar la reputación de una institución y/o lesionar sus atributos”.Rossignoli Oscar, ¿Qué es el manejo de crisis?

De igual manera y en lo que respecta a la Segunda Línea de Defensa dimensión 7 MIPG, se realizará la verificación por parte de la Oficina Asesora de Planeación de la aplicación y efectividad de los lineamientos y controles establecidos por la Alta Dirección para la prevención, manejo y retroalimentación de la crisis.

Lo anterior con el fin que, en cumplimiento de su roll en la Tercera Línea de Defensa dimensión 7 MIPG, la Oficina Asesora de Control Interno realice la evaluación efectiva del resultado de la estrategia para el manejo de crisis.

2. OBJETIVO:

Establecer la metodología en virtud de la cual, la Unidad para las Víctimas en el desarrollo de sus funciones y en el marco del autocontrol pueda evitar hechos que se materialicen en riesgos, que afecten la integridad, seguridad y bioseguridad de los servidores públicos como de los colaboradores de la entidad.

3. ALCANCE:

Señalar los aspectos relevantes respecto al manejo institucional a nivel central y territorial de la crisis, los eventos que dan lugar a ella y comunicaciones estratégicas.

DEFINICIONES:

Amenaza: representa un peligro latente asociado con un fenómeno físico de origen natural o antrópico que puede presentarse en un sitio específico y en un tiempo determinado, produciendo efectos adversos en las personas, los bienes y/o el medio ambiente.

Colaboradores:

COMR: Centro de Operaciones y Monitoreo de Riesgos

Comunidad: definida como aquellos grupos humanos que habilitan en territorios de interés para la Unidad.

Crisis: situación inesperada o evento extraordinario que puede afectar la imagen, integridad y credibilidad de la UARIV, así como también la salud, integridad o bienestar de los funcionarios y colaboradores.

Contratistas: hace referencia a las personas naturales o jurídicas, que suscribe un contrato para la prestación de un servicio.

Desastre: alteración en forma súbita a las personas, su medio ambiente o sus bienes causado por factores externos de origen antrópico o natural que demandan la inmediata acción de las autoridades a fin de mitigar los efectos adversos de estos sobre la salud de las personas. Excede la capacidad de respuesta y demanda ayuda externa de orden nacional o internacional.

Emergencia: alteración en forma súbita de las personas, el medio ambiente que lo rodea o sus bienes por causas naturales o antrópicas y que demandan la inmediata acción de las entidades de salud, tendiente a disminuir las consecuencias de este. Se caracteriza por no exceder la capacidad de respuesta.

Estado: constituido por las instituciones del Estado, en sus diferentes ramas del poder público, que tienen relación con la Unidad.

Funcionarios: Definido por su relación laboral; está constituido por personas naturales que tienen una relación laboral y reciben un salario por parte de la Unidad.

Medio de comunicación: medios de comunicación en general.

Organismos Institucionales: constituidos por la comunidad internacional en general y en particular por los organismos de cooperación internacional que tienen que ver con la labor de la Unidad.

Riesgo: daño, destrucción o perdida esperada obtenido del producto de la probabilidad de ocurrencia de eventos peligrosos y de la vulnerabilidad de los elementos expuestos a tales amenazas, matemáticamente expresado como la probabilidad de exceder un nivel de consecuencias económicas y sociales en un cierto sitio y en un cierto período de tiempo (Spence 1990).

Sociedad: definida como la totalidad de la población colombiana, entendida en sus dimensiones societaria, económica, política y cultural.

Víctimas: Se consideran víctimas, para los efectos de esta ley, aquellas personas que individual o colectivamente hayan sufrido un daño por hechos ocurridos a partir del 1º de enero de 1985, como consecuencia de infracciones al Derecho Internacional Humanitario o de violaciones graves y manifiestas a las normas internacionales de Derechos Humanos, ocurridas con ocasión del conflicto armado interno

Vulnerabilidad: predisposición intrínseca de un sujeto o elemento a sufrir daño debido a posibles acciones externas.

4. DESARROLLO

5.1. Comunicaciones y Reportes

Con base en la información derivada de los eventos o sucesos generadores de crisis, se deberán emitir de manera oportuna informes de monitoreo que permitan brindar el soporte en caso de crisis o emergencias en cualquier lugar del país.

5. LINEAMIENTOS DE LA ALTA DIRECCIÓN PARA EL MANEJO DE CRISIS

En el contexto de la primera línea de defensa, se establecen los siguientes lineamientos para prevenir la ocurrencia de eventos que ocasionen crisis, para abordar el manejo de la misma y la determinación de roll del Equipo Nacional de Manejo de Crisis, el Equipo de Manejo de Crisis Territorial, el Comité de Manejo de Crisis y se establecerán los lineamientos aplicables por el Centro de Operaciones y Monitoreo de Seguridad – COMR**,** quien será el encargado de intervenir en los momentos de crisis generados por eventos o riesgos de seguridad.

6.1. Prevención y mitigación de crisis

Con el fin fortalecer la gestión del riesgo, para poder prevenir o mitigar los hechos que puedan generar crisis será necesario:

- Identificar el personal y colaboradores de la UARIV que puedan ser objeto de una crisis
- Analizar el entorno y el nivel de seguridad, en el cual los funcionarios y colaboradores desempeñan sus actividades
- Mantener un inventario de recursos disponibles de apoyo dentro y fuera de la institución para enfrentar la crisis
- Realizar jornadas de formación y capacitación de los funcionarios y colaboradores de la Unidad donde se pueden presentar crisis.
- Incluir en el programa de inducción y reinducción el manejo de crisis
- Gestionar el riesgo de acuerdo con el protocolo establecido en la metodología de administración del riesgo

6.2. Manejo de Crisis

Las crisis derivadas de la ocurrencia o materialización de los riesgos de seguridad serán abordadas por las estructuras identificadas en el presente manual, trabajarán de manera coordinada y articulada:

5.2.1. Centro de Operaciones y Monitoreo de Seguridad – COMR

En el momento que se genere la crisis, el Centro de Operaciones y Monitoreo de Seguridad – COMR operará como primera instancia. En este sentido, recibirá, procesará, escalará y difundirá los reportes a los diferentes grupos de interés, y así mismo dará las recomendaciones necesarias sobre la ocurrencia de los hechos a los Directores Territoriales y líderes de proceso, las cuales servirán como insumo para la toma de decisiones.

Adicionalmente, será el administrador de la herramienta tecnológica COMR, que permite la comunicación permanente con funcionarios vía celular y demás instrumentos tecnológicos necesarias, para el desarrollo de la gestión de seguridad preventiva y mitigación de los riesgos.

También, contará con un equipo para el análisis de los distintos riesgos de seguridad que pueden generar crisis, tanto en el campo de la prevención y atención de emergencias, como en el área de análisis de contingencias que afecten la gestión de la Unidad.

Dado que las contingencias y las crisis, en la mayoría de los casos, no son previsibles, los profesionales que hacen parte del Centro de Operaciones, deben tener disponibilidad las 24 horas del día y los 365 días del año, estando en comunicación permanente con el delegado de la Dirección General en la Unidad, con fin de informar cualquier eventualidad presentada.

Lo anterior requiere de sistemas de comunicaciones especiales e información sobre cada uno de los miembros (nombre completo, puesto o cargo dentro de la entidad, teléfono, dirección de residencia, números de teléfono oficina, teléfono de residencia, celulares, correo electrónico, etc.,).

En cada una de las veinte (20) Direcciones Territoriales de la Unidad, el respectivo Director y su enlace en materia de manejo de crisis, reportarán al COMR la información sobre eventos, contingencias y crisis que se presenten en la territorial.

El Centro de Operación funcionará los siete (7) días de la semana y veinticuatro (24) horas al día, con las siguientes funciones:

- Detectar los eventos y riesgos, así como también generar respuestas oportunas para su inmediata solución
- Monitorear continuamente los riesg os de seguridad
- Generar las alertas tempranas sobre problemas particulares, relacionados con un conjunto de problemas y sobre la eventualidad de un conflicto de mayores proporciones, a nivel local, territorial y nacional
- Recolectar, sistematizar, analizar y reportar información especializada en materia de contingencias y manejo de crisis.
- Generar y difundir conocimiento sobre el manejo de crisis
- Recomendar, que se escalen los hechos a los Equipos de Manejo de Crisis y Comunicaciones Estratégicas, y se convoque el Comité de Crisis cuando a ello haya lugar

para prevenir que la contingencia afecte de manera grave la continuidad del servicio y sus consecuencias sean públicas.
- Brindar las recomendaciones necesarias como insumo para la toma de decisiones

Como resultado de su gestión, el COMR deberá presentar los siguientes informes:

- Informe de proyección diaria con relación a las actividades en terreno
- Informe de vías y aeropuertos y pronóstico meteorológico.
- Proceso de monitoreo y registro de reportes a comisiones jornada A.M.
- Boletín diario de noticias
- Informe diario sobre la situación del personal en terreno y desarrollo de las actividades en el territorio nacional e Internacional.
- Proceso de monitoreo y registro de reportes a comisiones jornada P.M.
- Recepción y manejo inicial de incidentes
- Guía para el desarrollo del curso básico de seguridad virtual y su respectivo registro en el sistema COMR.
- Actualización de los directorios relacionados con las entidades del Estado y organismos de seguridad y apoyo.
- Estadística de Actividades en terreno: Objetivo, dependencias comprometidas, ubicación geográfica de su ejecución, personal participante.

5.2.2. Equipo Nacional de Riesgos, Manejo de Crisis y Comunicaciones Estratégicas

a) Alcance:

Operará como segunda instancia en el manejo de la crisis y su función estará orientada al monitoreo y análisis de eventos y contingencias que por sus efectos puedan perturbar la continuidad de la gestión de la Unidad**.**

b) Integración del Equipo Nacional de Manejo de Crisis y Comunicaciones Estratégicas.

Este Equipo será dirigido desde y por la Dirección General de la Unidad, a través de un Coordinador, y estará conformado así:

- El coordinador Técnico.
- Los líderes según la tipología de riesgos:
- Un delegado de la Oficina Asesora de Comunicaciones.
- Un delegado de la Subdirección de Prevención y Atención de Emergencias.

5.2.3. Equipo Territorial Riesgos, Manejo de Crisis y Comunicaciones Estratégicas

a) Alcance

Operará como segunda instancia a nivel territorial en el manejo de la crisis y su función estará orientada al monitoreo y análisis de eventos y contingencias que por sus efectos puedan perturbar la continuidad de la gestión de la Unidad en territorio**.**

b) Integración del Equipo Territorial Riesgos, Manejo de Crisis y Comunicaciones Estratégicas. Nacional de Manejo de Crisis y Comunicaciones Estratégicas.

Este Equipo será dirigido desde y por la Dirección Territorial de la Unidad, y estará conformado así:

- Director territorial
- Los líderes según la tipología de riesgos a nivel territorial
- Un delegado de la Oficina Asesora de Comunicaciones en territorio.
- Un delegado de la Subdirección de Prevención y Atención de Emergencias en territorio.

c) Funciones

Estos Equipos tendrán las siguientes funciones orientadas a la gestión del riesgo de seguridad pública, teniendo en cuenta que el campo de acción del Equipo Territorial como su nombre lo indica, se encuentra en la atención de la crisis a nivel de territorio:

- Recopilar de manera ágil información sobre la contingencia que genera la crisis
- Brindar recomendaciones sobre la implementación de los lineamientos o de la metodología para la administración de riesgos de seguridad.
- Emitir alertas sobre los riesgos materializados.
- Realizar periódicamente informes sobre el comportamiento de los riesgos
- Coordinar la implementación de acciones o posibles soluciones frente a los riesgos de seguridad que se pueden llegar a materializar a nivel general y territorial.
- Analizar los resultados de las acciones implementadas sobre los riesgos de seguridad materializados y su efectividad.
- Analizar el impacto de los riesgos materializados y que deriven siniestro
- Analizar en el marco del fortalecimiento del autocontrol, los resultados del monitoreo y seguimiento de los riesgos identificados en el mapa de riesgo, con el fin de que se tomen acciones para la optimización de la gestión de los mismos.
- Implementar oportunamente las acciones de prevención de eventos que generen situaciones de crisis
- Establecer escenarios y definir las estrategias y ejes de acción, para reestablecer la operación de la Unidad afectada por la crisis.
- Estar en permanente contacto con los medios de comunicación, a través del vocero designado.

- Coordinar acciones con el Equipo Nacional de Riesgos, Manejo de Crisis y Comunicaciones Estratégicas, cuando se requiera.
- Revisar las acciones de contingencia que se puedan presentar
- Determinar la probabilidad de materialización del riesgo y sus consecuencias o impacto
- Presentar informes de gestión del riesgo

e) Sesiones del Equipo

Los equipos se reunirán por lo menos una (1) vez al mes para hacer monitoreo de los hechos que puedan generar crisis y manejo de crisis materializadas. Las reuniones serán convocadas por el Coordinador Técnico o el Director Territorial según sea el caso por lo menos con tres (03) días hábiles de anticipación.

De igual manera podrán reunirse cuando las circunstancias así lo exijan.

A las convocatorias se adjuntará la documentación pertinente de acuerdo con la agenda propuesta.

f) Convocatoria.

La convocatoria a las reuniones se realizará vía correo electrónico a todos los integrantes.

Adicionalmente, se invitarán Instituciones públicas y/o privadas cuando a ello haya lugar.

5.2.4. Comité de Manejo de Crisis.

a) Objeto

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

b) Alcance

Intervendrá cuando por la complejidad y naturaleza de los hechos que originan la crisis requieren el análisis de la Alta Dirección para la toma decisiones.

c) Integración del Comité de Crisis.

El comité estará conformado así:

- El Director (a) General quien presidirá el Comité Nacional o su delegado.
- El Secretario técnico designado por los integrantes del comité nacional.

- El Subdirector (a) General o su delegado
- El Secretario (a) General
- El jefe de la Oficina Asesora Jurídica
- El jefe de la Oficina Asesora de Comunicaciones
- El Subdirector de Prevención y Atención de Emergencias
- El Coordinador Técnico del Equipo de Gestión de Riesgos, Manejo de Crisis y Comunicación Estratégicas.
- De acuerdo con la crisis, el o los Directores de dependencias o directores territoriales directamente afectados por la misma.

d) Funciones

El Comité de Crisis tendrá las siguientes funciones:

- Verificar la eficacia de la gestión del Riesgo
- Determinar la asignación de los recursos para la mitigación y control de la crisis.
- Identificar los riesgos en situación extrema y critica con alta probabilidad de materialización.
- Analizar las consecuencias y el impacto generado por la crisis.
- Definir estrategias y ejes de acción para reestablecer la operación
- Mantener contacto permanente con los medios de comunicación cuando las circunstancias de la situación lo ameriten.

e) Sesiones.

Este comité se reunirá trimestralmente con el fin de analizar los informes de materialización de riesgos. De igual manera podrán reunirse de manera extraordinaria cuando las circunstancias así lo exijan.

f) Quórum.

El quórum para sesionar el Comité estará constituido por la mitad más uno de sus miembros. Pasados los primeros treinta (30) minutos de la hora señalada para empezar la reunión del Comité sesionará con los miembros presentes y sus decisiones tendrán plena validez.

6. Herramienta tecnológica COMR

Permitirá realizar el análisis y monitoreo de eventos y contingencias que generen crisis, para el almacenamiento y consulta de datos con el fin de generar valor a la información que facilite la toma de decisiones.

Esta herramienta permitirá:

- Sistematizar y clasificar información sobre las distintas contingencias y generar alertar tempranas.

- Recolectar y sistematizar la información relacionada con datos sensibles de los funcionaros y colaboradores de la UARIV.
- Identificar generadores de la crisis y sus potenciales causas
- Mantener monitoreo sobre los medios de comunicación y sus actores
- Controlar la improvisación en el manejo de las contingencias y crisis.
- Generación de estadísticas y resultados a tiempo y en tiempo real frente a la ocurrencia de incidentes en las misiones desarrolladas en territorio

La administración de la herramienta la realiza de manera autónoma el Centro de Operaciones, contando con el soporte de la Oficina de Tecnologías de la Información – OTI.

7. Vocero

El Director General será el vocero de la UARIV. El Director General será la única persona con la facultad de conceder las declaraciones oficiales o dar entrevistas de acciones adelantadas por la entidad.

Para el caso de las Direcciones Territoriales, serán los directores, los voceros de las actuaciones misionales, a menos que la temática requiera un manejo especifico, en caso de la línea de mensaje y la divulgación será acordada con la Oficina Asesora de Comunicaciones.

Los voceros deberán:

- Reunir toda la información posible, contando con el acompañamiento de oficina Asesora de Comunicaciones
- Determinar la estrategia de comunicación a través de los canales habilitados
- Determinar los mecanismos de monitoreo inmediato en todos los medios para comprobar el alcance de la crisis.
- Determinar la secuencia y la coherencia de la comunicación, en caso de que se trate de una crisis con extensión en el tiempo.
- Neutralizar la ventaja de los medios que trabajan a tiempo real
- Brindar información en tiempo real a la comunidad, para mantenerlos informados sobre la situación de la crisis
- Mantener el control de la situación frente al manejo de la información
- Mantener una comunicación directa y fluida con los medios de comunicación para informar sobre hechos ocurridos

- Diseñar la comunicación interna
- Preparar información de reserva para llenar los vacíos informativos
- Elaborar un discurso mediante el cual se informe las acciones tomadas para controlar la crisis.

Adicionalmente, el vocero en el cumplimiento de sus funciones deberá tener en cuenta lo establecido en el plan estratégico de comunicaciones específico del proceso de comunicación estratégica y el mensaje transmitido deberá ajustarse en lo contenido en la matriz de comunicaciones de la UARIV, en cuanto a la forma del mensaje y los canales de comunicación, a quien va dirigido y el responsable del mensaje, entre otros.

Con posterioridad a la crisis

Una vez ocurrido y manejado el evento, es importante:

- Restablecer la normalidad lo antes posible, asegurando primero la integridad de las personas.
- Activar el apoyo de los recursos de comunicación, para informar a la ciudadanía el retorno a la normalidad.
- Recoger la mayor cantidad de información que sirva de experiencia para futuras crisis (crear un archivo de crisis y experiencias positivas y negativas).
- Los Equipos de Manejo de Crisis tanto nacional como territorial deberán presentar un informe al Comité de Crisis con el fin de retroalimentar las acciones implementadas para atender la crisis y restablecimiento de la normalidad.

8. PROCEDIMIENTO

a) Procedimientos que desarrolla el Centro de Operaciones y Monitoreo de Riesgos de la Unidad para las Víctimas

Área Operativa:

- Comunicación, acompañamiento, monitoreo, apoyo y coordinación con los funcionarios que reiniciaron actividades humanitarias en el Territorio.
- Comunicación con funcionarios, contratistas y personal de apoyo que labora en la Unidad, con el fin de hacer seguimiento al estado de salud y sus familias, así mismo llevar un mensaje de agradecimiento y reconocimiento a las actividades institucionales que realizan desde sus hogares.
- Comunicación con Ministerio de Defensa Nacional y Enlace de la Policía Nacional.
- Participación en los espacios virtuales de las diferentes dependencias y direcciones territoriales.

- Emitir artículos, recomendaciones de seguridad y salubridad por los diferentes medios de comunicación, como SUMA propio de la entidad, correos electrónicos, mensajes de WhatsApp, comunicación telefónica, entre otros.

Área Análisis:

- Emitir diariamente el boletín de noticias nacionales e internaciones, la cual se comparte con la Alta Dirección, Director de Dependencia, Subdirectores y Directores Territoriales.
- Atención a los requerimientos relacionados con situación de orden público, en áreas específicas mediante las apreciaciones de seguridad y análisis de riesgos en coordinación con otras agencias de seguridad para el desarrollo de actividades misionales.
- Actualización y análisis del Protocolo para el Manejo del Riesgo Público

b) Procedimientos que desarrolla el Equipo Nacional y Territorial de Manejo de Crisis y Comunicaciones Estratégicas

El Equipo Nacional o Territorial analizará el riesgo que origina la crisis y las posibles causas que la ocasionan, con el fin de determinar la forma en que sucedieron los hechos y las consecuencias que estos puedan desencadenar. De acuerdo con esto, se tendrá en cuenta:

Recopilación de la información

Se debe recopilar la información que se tenga de la ocurrencia del evento, y analizar datos de situaciones similares, con el fin de poder tomar las experiencias aprendidas como insumo para establecer estrategias de mitigación y control.

Evaluación del nivel de las crisis.

Se deberá tener en cuenta cuatro (4) variables para evaluar el nivel de las crisis:

- **Validez.** Hay que evaluar la credibilidad de las fuentes de información con las que el comité de crisis debe operar:

  - ¿Qué tan confiable es la fuente de información?
  - ¿Qué tan exacta es la fuente de información?
  - ¿Se realizó una verificación independiente de la información?

- **Severidad.** Hay que determinar el número de Grupos de Interés que pueden ser afectados por la crisis:

  - Determinar si existe algún elemento criminal en la posible causa de la crisis.
  - Determinar si la Unidad puede tener implicaciones de tipo legal derivadas de la crisis
  - Determinar el tiempo aproximado para solucionar o controlar el problema.
  - ¿Hay amenazas a la salud?
  - ¿Cuántas personas han sido afectadas y cómo?

- ¿Hay afectación a la imagen de la Unidad?
- ¿Tiempo necesario para mitigar la crisis?

- **Alcance.** Determinar la cobertura de los medios de comunicación, la cobertura de la información, así como la difusión que se le ha dado al suceso. Igualmente determinar el nivel de cuestionamientos de otras partes interesadas a nivel externo.

  - ¿Hasta dónde se ha extendido el problema en los medios?
  - ¿De qué naturaleza han sido los cuestionamientos externos?
  - ¿Qué audiencias se han visto afectadas por la emergencia?
  - Clientes internos y externos

- **Responsabilidad.** Determinar el grado de responsabilidad de la Unidad, así como los asuntos negativos que se deben anticipar como resultado de la crisis.

  - ¿Involucramiento criminal?
  - ¿Interno?
  - ¿Externo?
  - ¿Hasta qué grado es responsable la entidad?
  - ¿Potencialmente cuántos litigios podría haber?
  - ¿De qué tipo podrían ser las demandas externas?

Valoración del riesgo

Para establece la valoración del riesgo que origina la crisis se aplicará la metodología de manejo de riesgo, y la matriz de riesgo publicadas en la página web de la unidad.

Para la valoración se utilizarán los semáforos establecidos:

- Semáforo verde: detección de variables de riesgo localizadas, sin demasiada notoriedad y con final cierto.

- Semáforo amarillo: detección de variables de riesgo de amplio espectro, con notoriedad pública y final cierto.

- Semáforo rojo: detección de variables de riesgo graves, con alta notoriedad pública y final incierto.

Implementación de acciones

El Equipo Nacional o Territorial de Manejo de Crisis, según sea el caso, establecerá e implementará las acciones de mitigación y control de la crisis, las cuales deberán se comunicadas a la Dirección General para establecer los lineamientos de la estrategia de comunicación.

En el evento que por la complejidad y naturaleza del hecho que genera la crisis deba ser escalada al Comité de Crisis, se procederá realizar la respectiva citación al comité para analizar la efectividad de las estrategias formuladas por el Equipo de Manejo de Crisis que permitan la mitigación y control de la misma.

Pronunciamiento a medios de comunicación

En el evento que se requiera realizar un pronunciamiento ante los medios de comunicación, se deberá seguir los lineamientos definidos en la matriz de comunicaciones.

Antes de realizar el pronunciamiento a los medios de comunicación, el vocero deberá conocer todos los antecedentes de los hechos que generaron la crisis, de tal manera que cuente con la información suficiente que le permita responder las preguntas de las 5W2H por sus siglas en inglés:

- What: ¿Qué pasó? ¿Qué acciones se están tomando? ¿Qué acciones se van a implementar para que no vuelva a ocurrir?
- Why: ¿Por qué pasó?
- Who: ¿Quién es el responsable?
- How much: ¿Cuántos son los afectos?
- How: ¿cómo originó la crisis?
- When: ¿Cuándo se originó la crisis?
- Where: ¿Dónde se originó la crisis?

9. ASPECTOS PARA TENER EN CUENTA EN EL MANEJO DE CRISIS

Para el manejo de la crisis se debe tener en cuenta los siguientes aspectos:

- Detectar áreas y niveles de riesgo
- Monitorear permanentemente los riesgos
- Contar con fuentes de información variadas y confiables
- Contar con sistemas de alerta temprana
- Efectuar gestión oportuna de focos de riesgos
- Capturar rápidamente los antecedentes
- Realizar capacitaciones y simulacros.

10. ALMACENAMIENTO DE INFORMACIÓN

El almacenamiento de la información debe realizarse teniendo en cuenta los lineamientos señalados en el procedimiento de Control de Registro publicado en la página web, Proceso de Gestión Documental.

11. DATOS DE CONTACTO

La Unidad para la Atención y Reparación Integral a las Víctimas contará con una base de datos de:

- Todos los miembros del Comité de Crisis, miembros del Equipo Nacional de Manejo Crisis y Comunicaciones Estratégicas y miembros del Equipo Territorial de Manejo Crisis y Comunicaciones Estratégicas (nombres, apellidos, puesto o cargo dentro de la entidad, teléfono y dirección de residencia, números de teléfono de la oficina, celular, correo electrónico, etc.,)
- Base de datos de contactos con todos los interesados/afectados por la crisis (bomberos, Policía, medios de comunicación, Comités de Emergencias, etc.)

12. DOCUMENTOS DE REFERENCIA

- Protocolos para el Manejo del Riesgo Público
- Metodología para la Administración de Riesgos Institucionales
  Plan estratégico de comunicaciones
- Matriz de Comunicación
- Procedimiento de Control Registro
- Formato Identificación de partes interesadas

Anexo 1 Control de cambios

Versión	Fecha del cambio	Descripción de la modificación
1	22/12/2016	Creación
2	02/03/2017	Se incluye el COMS y el apartado del Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas.
3	06/03/2017	Se actualiza el COMR y el nombre Equipo de crisis y comunicaciones estratégicas, adicionalmente se realizan ajustes como parte de la mejora.
4		Se actualiza el manual estableciendo los procedimientos para el manejo de crisis

ANEXO 6

IDENTIFICACIÓN DE LOS RIESGOS DE CORRUPCIÓN ASOCIADOS A LA PRESTACIÓN DE TRÁMITES Y SERVICIOS EN LA UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS

1. INTRODUCCIÓN

El presente anexo se establece con base en el Protocolo para la identificación de riesgos de Corrupción asociados a la prestación de trámites y servicios el cual se enmarca en los lineamientos de dos de las dimensiones del MIPG: “Direccionamiento estratégico y planeación” y “Control interno”. Estas dimensiones establecen que se debe incluir de manera los riesgos de gestión y de corrupción en una política que permita gestionar el riesgo en la entidad y establecer controles. Como resultado de la identificación de riesgos de corrupción se deben implementar estrategias de racionalización, bien sea mediante acciones normativas, administrativas o tecnológicas de racionalización.

2. IDENTIFICACIÓN DE RIESGOS DE CORRUPCIÓN ASOCIADOS A PRESTACIÓN DE TRÁMITES Y SERVICIOS

Este anexo se establece con base en el Protocolo para la identificación de riesgos de Corrupción asociados a la prestación de trámites y servicios el cual se enmarca en los lineamientos de dos de las dimensiones del MIPG: “Direccionamiento estratégico y planeación” y “Control interno”. Estas dimensiones establecen que se debe incluir de manera los riesgos de gestión y de corrupción en una política que permita gestionar el riesgo en la entidad y establecer controles. Como resultado de la identificación de riesgos de corrupción se deben implementar estrategias de racionalización, bien sea mediante acciones normativas, administrativas o tecnológicas de racionalización.

2.1. La corrupción en los trámites administrativos

De acuerdo con estos lineamientos, se determina que los riesgos de corrupción en los trámites se pueden presentar en dos momentos:

a) Al efectuar el trámite: Esto corresponde a la interacción entre el ciudadano y el servidor público. (es decir de la ventanilla hacia afuera de la entidad por ejemplo cuando el ciudadano presenta un documento o efectúa un pago).

b) Al ejecutar los procedimientos al interior de la entidad para dar cumplimiento al trámite (de la ventanilla hacia adentro. La entidad tiene procedimientos internos, como por ejemplo distribuir la documentación recibida entre las áreas internas cambiando el turno).

Es importante establecer que un trámite es un conjunto de requisitos, pasos, o acciones reguladas por el estado dentro de un proceso misional que deben efectuar los grupos de valor ante la entidad para acceder a un derecho. De acuerdo con esta definición; el trámite se dirige al cliente externo que busca acceder a un derecho.

3. Identificación de riesgos de corrupción asociados a trámites

La identificación de riesgos de corrupción asociados a trámites inicia con el análisis de los objetivos de los procesos misionales que incluyan procedimientos que deben atender los usuarios para cumplir los requerimientos de un trámite.

El punto de partida para la identificación de riesgos de corrupción asociados a trámites, es el análisis del contexto que considere los factores internos y externos a la gestión del trámite.

En el contexto interno se deben determinar las debilidades que generan riesgos de corrupción. Algunos de ellos son: espacios de discrecionalidad (toma de decisiones con cierta autonomía), fallas en el diseño de los procesos, normatividad compleja, excesivos costos administrativos, débiles sistemas de información, inadecuada selección de personal, ausencia de manuales, tecnología obsoleta o carente de controles, entre otros.

Por otra parte, en el contexto externo se deben considerar las amenazas del entorno, que pueden incidir en el uso del poder para beneficio de un privado: la intervención de carteles de contratistas, organizaciones delictivas, grupos armados, participación y control social débiles, fragilidad en el control externo, recursos públicos no regulados efectivamente, entre otros.

En los posibles factores externos para el análisis del entorno, se pueden tener en cuenta los componentes del triángulo de la corrupción:

a) Oportunidad: falta de controles internos y externos efectivos en los procesos, procedimientos y ausencia de controles en el desarrollo de los trámites.

- Poca información al ciudadano
- Desorganización en la información
- Inexistencia de procesos y procedimientos claros
- Confianza excesiva en los trabajadores (servidores públicos)
- Pocas acciones de rendición de cuentas
- Poca o débil vigilancia

b) Responsabilidad: Las fallas éticas y de compromiso con lo público que afectan un desarrollo objetivo e imparcial en el manejo y regulación de los recursos públicos.

c) Presión: Existen factores externos e internos que afectan las conductas de integridad pública y propician riesgos de corrupción.

4. Procesos, procedimientos o actividades susceptibles de riesgos de corrupción.

A manera de ilustración, se señalan algunas actividades susceptibles de riesgos de corrupción a partir de los cuales la entidad podrá incluir otros que considere pertinentes:

Direccionamiento estratégico (alta dirección).

- Concentración de autoridad o exceso de poder
- Extralimitación de funciones
- Ausencia de canales de comunicación
- Amiguismo y clientelismo.

Financiero (está relacionado con áreas de planeación y presupuesto)

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

De contratación (como proceso o bien los procedimientos ligados a este).

- Estudios previos o de factibilidad deficientes
- Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).
- Disposiciones establecidas en los pliegos de condiciones que dirigen los procesos hacia un grupo en particular. (Ej. media geométrica).
- Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación
- Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados
- Urgencia manifiesta inexistente.
- Otorgar labores de supervisión a personal, sin conocimiento para ello
- Concentrar las labores de supervisión en poco personal.
- Contratar con compañías de papel que no cuentan con experiencia.

De información y documentación

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

- Incumplimiento de la Ley 1712 de 2014 *"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".*

De investigación y sanción

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

De trámites y/o servicios internos y externos

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

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

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

1. OBJETIVO

Definir los lineamientos para la Administración de Riesgos en la Unidad para la Atención y Reparación Integral a las Víctimas, con el fin de identificar, analizar y valorar los riesgos en las actividades o eventos que puedan afectar de manera positiva o negativa el cumplimiento de los objetivos y metas de la Unidad.

2. ALCANCE

El procedimiento inicia con la planeación de las actividades que dan cumplimiento a la Metodología de Administración de Riesgos de la Unidad y termina con el Seguimiento por parte de control interno al Mapa de riesgos Institucional.

3. DEFINICIONES

Administración de riesgos: conjunto de elementos de control que, al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública auto controlar aquellos que pueden afectar el cumplimiento de sus objetivos.

Análisis del riesgo: busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial.

Contexto estratégico: condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución. Las situaciones del entorno o externas pueden ser de carácter social, cultural, económico, tecnológico, político y legal, bien sean internacional, nacional o regional según sea el caso de análisis. Las situaciones internas están relacionadas con la estructura, cultura organizacional, el modelo de operación, el cumplimiento de los planes y programas, los sistemas de información, los procesos y procedimientos y los recursos humanos y económicos con los que cuenta una entidad.

Contexto externo: determina las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como: Políticos, sociales y culturales, legales y reglamentarios, tecnológicos, financieros y económicos.

Contexto interno: determina las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos. Se pueden considerar factores como: Estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias implementadas, recursos y cultura organizacional.

Evaluación del riesgo: proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

Evento: incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

Identificación del riesgo: establece las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes.[1]

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del 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, permitiendo conocer las políticas inmediatas de respuesta ante ellos.

Monitorear: comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios.

Probabilidad: posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad.

Políticas de administración del riesgo: identifican las opciones para tratar y manejar los riesgos basadas en la valoración de estos, permiten tomar decisiones adecuadas y fijar los lineamientos, que van a trasmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.

Proceso de administración de riesgo: aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la administración del riesgo.

Riesgo: posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

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

Valoración del riesgo: 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.

4. CRITERIOS DE OPERACIÓN

- La administración de riesgos institucionales está basada en la Metodología de Administración de Riesgos de Departamento Administrativo de la Función Pública, la cual

[1] Guía para la administración del riesgo.

se encuentra alineada al Modelo Integrado de Planeación y Gestión MIPG y los lineamientos para la gestión de riesgos de corrupción de la Secretaria de Transparencia.

- El Mapa de Riesgos Institucional es el consolidado de todos los riesgos identificados en la Unidad y contiene riesgos Operativos, de Corrupción, Públicos, Ambientales, de Seguridad de la Información, de Seguridad y Salud en el trabajo, de emergencia, crisis y seguridad pública.

- Los mapas de riesgos se elaboran siguiendo los lineamientos definidos en la Metodología de Riesgos establecida por la Unidad y con la participación y compromiso de los directivos y servidores públicos de todos los procesos y Direcciones Territoriales de la Unidad y el apoyo de los Enlaces SIG.

- Para la identificación de los riesgos, se tomará como punto de partida los objetivos de los procesos y las metas definidas por la entidad, a fin de registrar todos los riesgos existentes y que puedan afectar el normal funcionamiento de los procesos, así como el análisis del contexto interno y externo.

- Para las Direcciones territoriales se construirá un mapa de riesgos propio, bajo la misma metodología, teniendo en cuenta su contexto y sus particularidades.

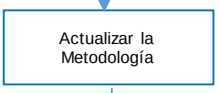
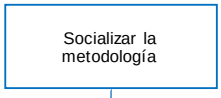
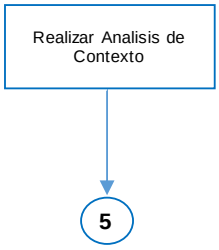
- La Oficina Asesora de Planeación asesora y avala el proceso de construcción del mapa de riesgos con respecto al cumplimiento de los parámetros establecidos en la Metodología de Administración de Riesgos de la Unidad. Sin embargo, el contenido de este documento es responsabilidad del Líder del proceso/Dirección Territorial, quien participa en su construcción y aprueba con acta el contenido de este.

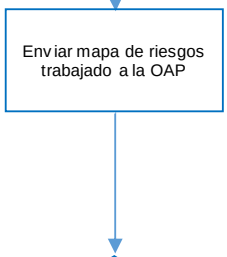
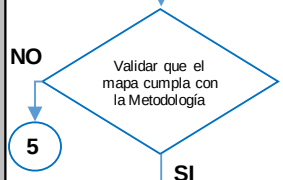
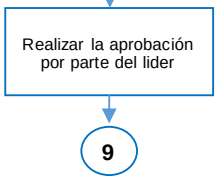
- La aprobación del Mapa de Riesgos Institucional la realiza en el Comité Institucional de Gestión y Desempeño con previa aprobación de cada uno de los lideres de los procesos y Direcciones Territoriales.

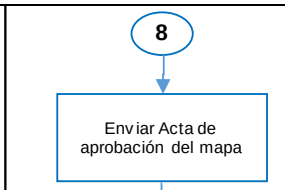
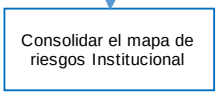
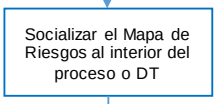
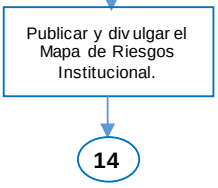
- La actualización del mapa de riesgos de realizará dos veces año de acuerdo con las fechas definidas por la Oficina Asesora de Planeación, quien acompaña esta tarea.

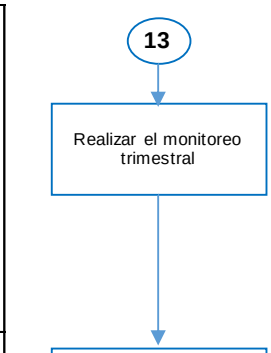
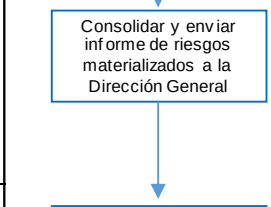
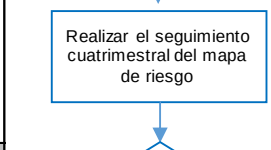
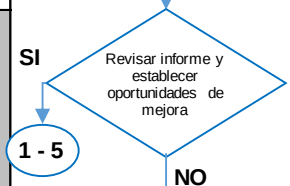
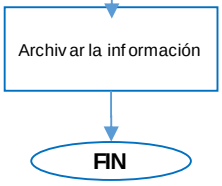
- La Normatividad requerida para el desarrollo de las actividades citas en el presente procedimiento se encuentra definida en el Normograma de la Unidad, disponible para consulta en la página web.

5. DESCRIPCION DE ACTIVIDADES

N° PC	Flujograma	Descripción	Entrada	Responsable	Salidas
1		Realizar la planeación de las actividades relacionadas con la Administración de Riesgos para cada vigencia	Normatividad vigente Lineamientos del DAFP	Profesional Oficina Asesora de Planeación	Plan de acción y Plan Anticorrupción y/o cronograma de trabajo
2		Actualizar la Metodología de Administración de Riesgos de acuerdo a las necesidades de cambio que se identifiquen de acuerdo a los Lineamientos del DAFP, recomendaciones de entes de control, mejora continua entre otros.	Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Requerimientos entes de control	Profesional Oficina Asesora de Planeación	Metodologia de Administración de Riesgos actualizada
3		Realizar socialización de la metodología a los enlaces SIG de los procesos y las Direcciones territoriales.	Metodología Administración de riesgos actualizada	Profesional Oficina Asesora de Planeación	Acta y lista de asistencia y/o evidencia de la socialización
4		Realizar el analisis del contexto estratégico de la Unidad (Contexto interno, contexto externo) de acuerdo a la Guia establecida para su elaboración. Ver Guía para la construcción del contexto estratégico	Metodología Administración de riesgos institucionales Guía para la construcción del contexto estratégico	Enlace SIG del proceso o Dirección territorial Funcionarios y contratistas del proceso o Dirección territorial Profesional Oficina Asesora de Planeación	Instrumento para realizar el Analisis de Contexto diligenciado

5		Realizar a la identificación y valoración de los riesgos a partir de la información obtenida en el analisis de contexto y a las oportunidades de mejora identificadas por recomendaciones o hallazgos de entes de control, hallazgos de auditoria o mejora del proceso entre otros. Ver Metodología de administración de riesgos institucionales -identificación de riesgos.	Metodología Administración de riesgos institucionales Analisis de contexto realizado	Lider del Proceso o Dirección territorial Enlace SIG del proceso o Dirección territorial Funcionarios y contratistas del proceso o Dirección territorial Profesional Oficina Asesora de Planeación	Mapa de riesgos trabajado por proceso y por DT
6		Enviar a la Oficina Asesora de Planeación el mapa de riesgos junto con la evidencias de su construcción para revisión.	Mapa de riesgos trabajado por proceso y por DT	Enlace SIG del proceso o Dirección territorial	Correo con Mapa trabajado y evidencia de su construcción
7 PC		Validar que el mapa de riesgos cumpla con los lineamientos establecidos en la Metodologia de Administraciónb de riesgos de la Unidad. El mapa cumple con los establecido en la Metodologia? SI: Continua en la actividad siguiente. NO: volver a la actividad 5.	Correo con trabajado y evidencia de su construcción	Profesional Oficina Asesora de Planeación	Correo con retroalimentación o aval de la OAP
8		Realizar la aprobación por parte del lider del proceso o Direccion Territorial del mapa de riesgos del proceso o DT	Correo con Aval de la OAP	Lider del Proceso o Dirección territorial Enlace SIG del proceso o Dirección territorial	Acta de aprobación del mapa de riesgos

9		Enviar a la Oficina de Planeación el acta de aprobación del mapa de riesgos del proceso o DT	Acta de aprobación del mapa de riesgos	Lider del Proceso o Dirección territorial Enlace SIG del proceso o Dirección territorial	Correo con acta de aprobación del mapa de riesgos
10		Consolidar la información de los mapas de riesgos de los procesos y direcciones territoriales para obtener el mapa de riesgos institucional	Mapa de riesgos actualizado por proceso y por DT y actas de aprobación	Profesional Oficina Asesora de Planeación	Mapa de Riesgos Institucional consolidado
11 PC		Aprobar el mapa de riesgos institucional. El mapa institucional es aprobado por el Comité Institucional de Gestión y Desempeño? SI: Continuar con la siguiente actividad. NO: Volver a la actividad 10	Mapa de Riesgos Institucional consolidado	Comité Institucional de Gestión y Desempeño	Mapa de Riesgos Institucional Aprobado
12		Socializar el el Mapa de Riesgos al interior del proceso o Dirección territorial, con el fin de dar cumplimiento a las acciones establecidas.	Mapa de Riesgos Institucional Aprobado	Enlace SIG del proceso o Dirección territorial	Acta y lista de asistencia y/o evidencia de la socialización
13		Publicar y divulgar el Mapa de Riesgos Institucional.	Mapa de Riesgos Institucional Aprobado	Profesional Oficina Asesora de Planeación	Mapa de riesgo publicado

14		Realizar el monitoreo trimestral a la materialización de los riesgos del proceso o Dirección territorial y generar las acciones correctivas correspondientes. Ver Metodología de administración de riesgos institucionales.	Mapa de riesgos Institucional	Lider del proceso o Dirección territorial Enlace SIG del proceso o Dirección territorial	Formato de monitoreo a la materialización de los riesgos diligenciado y NC registradas en el aplicativo SISGESTION
15		Consolidar y enviar informe de riesgos materializados a la Dirección General o a su representante para el tema de Riesgos	Formato de monitoreo a la materialización de los riesgos diligenciado	Profesional Oficina Asesora de Planeación	Informe de Riesgos Materializados
16		Realizar el seguimiento cuatrimestral del mapa de riesgos.	Mapa de riesgos Institucional	Oficina de Control Interno	Informe de seguimiento
17 PC		Revisar informe y establecer oportunidades de mejora frente a la implementación de la metodología y la actualización de los mapas de riesgos. Se requiere realizar ajustes a la metodologia o al plan de trabajo? SI: vuelve a la actividad 1 Se requiere realizar ajustes a la metodologia o al plan de trabajo? SI: vuelve a la actividad 5 NO: Continua con la siguiente actividad	Informe de seguimiento	Lider y Enlace SIG del proceso o Dirección territorial Profesional Oficina Asesora de Planeación	Oportunidades de mejora frente a la implementación de la metodología y la actualización de los mapas de riesgos identificadas
18		Archivar toda la información y documentación resultante de la aplicación del procedimiento de acuerdo a los lineamientos de Gestión Documental	Documentación resultante	Enlace SIG del proceso o Dirección territorial Profesional Oficina Asesora de Planeación	Documentos Achivados
FIN					

Producto y/o Servicio Generado	Descripción del Producto y/o Servicio
Mapa de riesgos Institucional	El Mapa de Riesgos Institucional de Riesgos es el consolidado de todos los riesgos identificados en la Unidad. En este documento se encuentran la identificación, valoración y tratamiento de los riesgos Institucionales.

6. ANEXOS

Anexo 1. Metodología de administración de riesgos institucionales
Anexo 2. Formato para el levantamiento del mapa de riesgos
Anexo 3. Formato de monitoreo a la materialización de los riesgos

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	30/05/2015	Teniendo en cuenta que la metodología de administración del riesgo tuvo modificaciones por parte del DAFP, se tuvo la necesidad de actualizar el procedimiento.
2	01/09/2015	Se realizó el ajuste de todas las actividades del procedimiento junto con los responsables y el registro.
3	30/03/2016	Teniendo en cuenta que la metodología de administración del riesgo tuvo modificaciones por parte del DAFP y la Guía para la gestión del Riesgo de Corrupción de la Secretaria de Transparencia se tuvo la necesidad de actualizar el procedimiento.
4	06/03/2016	Con la creación del Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas se modifican roles y responsabilidades en el procedimiento
5	07/02/2018	Se incluye en el procedimiento a la Direcciones Territoriales
6	26/08/2020	Se actualizan las actividades de acuerdo con la Metodología de Administración de Riesgos V8 y los lineamientos del DAFP