MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

DIRECCIÓN GENERAL

RESOLUCIÓN N° 04663 DEL 25 DE JULIO DE 2016

"Por la cual se adopta el Manual para la Gestión Integral del Riesgo en la Policía Nacional"

EL DIRECTOR GENERAL DE LA POLICÍA NACIONAL DE COLOMBIA

En uso de sus facultades legales que le confiere el artículo 2° numeral 8 del Decreto 4222 del 231106, y

CONSIDERANDO:

Que según la Ley 87 de 1993, conforme con el Artículo 1º, parágrafo único, los manuales de procedimientos son instrumentos a través de los cuales se cumple el control interno.

Que el Decreto 4222 de 2006 en su artículo 2º numeral 8, determina que el Director General de la Policía Nacional de Colombia, expedirá resoluciones, manuales y demás actos administrativos necesarios para administrar la Policía Nacional en todo el territorio nacional.

Que la Resolución No. 02058 del 8 de julio de 2009, "Por la cual se adoptan los procedimientos del proceso de primer nivel del Direccionamiento del Sistema de Gestión Integral, y sus despliegues para la Policía Nacional" establece como procedimiento la Administración de los Riesgos en la Policía Nacional.

Que se hace necesaria la actualización del Manual para la Gestión Integral del Riesgo en la Policía Nacional, como herramienta para estandarizar y unificar aspectos metodológicos que se ajusten a las normas vigentes.

RESUELVE:

ARTÍCULO 1. ADOPCIÓN.

Adóptese el Manual para la Gestión Integral del Riesgo en la Policía Nacional, el cual contiene los aspectos generales y específicos para la implementación y desarrollo de las fases de identificación, definición de la gestión, gestión de riesgos, medición de resultados de la gestión y cierre.

ARTÍCULO 2. CONTENIDO DEL MANUAL PARA LA GESTIÓN INTEGRAL DEL RIESGO EN LA POLICÍA NACIONAL.

El contenido de éste Manual está basado en las Políticas, Principios, Objetivos, Estructura y operacionalización de cada una de las fases mencionadas en el artículo anterior, las cuales contemplan el ciclo de mejora continua; Planear, Hacer, Verificar y Ajustar, (PHVA). Hace parte constitutiva del Manual los aspectos relacionados con el módulo de Gestión Integral del Riesgo, los cuales son definidos con base a lo establecido en este acto administrativo en el artículo 24 "operacionalización metodológica".

CAPÍTULO I

ARTÍCULO 3. GENERALIDADES PARA LA GESTIÓN INTEGRAL DEL RIESGO.

Con este documento se fortalece sustancialmente la administración del riesgo en la Policía Nacional, mediante el desarrollo y aplicación de las fases de identificación, definición de la gestión, gestión del riesgo, medición de resultados de la gestión y cierre, con las cuales se adoptará la nueva forma de actualización y tratamiento de los riesgos asociados a los objetivos de los procesos, indicadores de gestión del proceso, indicadores de proyectos, procedimientos, planes, proyectos de inversión y programas, que de manera directa o indirecta dinamizan los procesos, teniendo como base y referencia el producto no conforme, las no conformidades o hallazgos, los indicadores incumplidos y los riesgos materializados, que definirán los eventos potenciales a evaluar y los eventos a evaluar como indicador de seguimiento y control para la medición de los niveles de Gestión Integral del Riesgo en toda la Policía Nacional.

La estructuración de este Manual se hizo aplicando las directrices emitidas tanto a nivel nacional como internacional, las cuales se ven reflejadas en cada una de las fases anteriormente mencionadas y se plasman trasversalmente en todo el documento para la apropiación e interiorización de los conceptos y criterios de las normas referenciadas en el marco normativo que se enuncia posteriormente.

En este documento se incluye la Política General para la Gestión Integral del Riesgo, los principios, las políticas de operación, su alcance, objetivos, y las responsabilidades para su implementación por parte de todos los integrantes de la Policía Nacional, así como el marco legal y conceptual, que permitirán estandarizar el lenguaje de la Gestión Integral del Riesgo en la Policía Nacional.

Todas las actividades de una organización están sometidas de forma permanente a una serie de amenazas, lo cual las hace altamente vulnerables, por tal motivo es necesario tener políticas, planes, programas y proyectos tendientes a dar un manejo adecuado a los riesgos identificados en la Institución, con el fin de lograr de manera eficiente el cumplimiento de sus objetivos y estar preparados para enfrentar cualquier contingencia que pueda poner en peligro su existencia o la continuidad en el cumplimiento de su misión.

La gestión integral del riesgo en la gestión pública moderna es una función de muy alto nivel dentro de las organizaciones, orientada a establecer un conjunto de estrategias que a partir de los factores (humanos, físicos, tecnológicos y financieros) busca en el corto plazo, mantener la estabilidad de funcionamiento, garantizar la prestación eficiente de los servicios a la comunidad y minimizar las pérdidas ocasionadas por la materialización de estos.

De acuerdo con lo anterior, la Policía Nacional ha desarrollado un marco de referencia que permite el manejo integral de los riesgos, estudiar los elementos comunes que los conforman y los factores que determinan el impacto de sus consecuencias sobre la Institución. La metodología promueve la adopción de los principios básicos para la Gestión Integral del Riesgo, la creación de una estructura de soporte, los lineamientos para la implementación de la gestión, el seguimiento y la mejora continua.

ARTÍCULO 4. ALCANCE.

Este documento se construye para establecer los criterios de la administración del riesgo en la Policía Nacional de Colombia, e involucra en él a cada uno de los niveles, Estratégico, Táctico y Operacional, del orden institucional para su aplicación.

ARTÍCULO 5. ANTECEDENTES.

La gestión del riesgo, como parte integral de las buenas prácticas gerenciales, es un proceso interactivo que consta de varios elementos, cuyo objetivo es permitir que la Institución minimice pérdidas y maximice oportunidades, en todos sus campos de acción; su aplicación se basa en los parámetros y lineamientos metodológicos trazados por la norma ISO 31000:2009, ISO 27005:2009, OHSAS 18001, ISO 14001, el Departamento Administrativo de la Función Pública; dicha gestión promueve la participación y respaldo de los integrantes de la Institución, en la identificación, análisis, evaluación y tratamiento de los riesgos; contribuyendo al fortalecimiento del Sistema de Gestión Integral de la Policía Nacional y alcanzar el más alto grado de eficacia, eficiencia y efectividad.

ARTÍCULO 6. MARCO NORMATIVO.

Los parámetros del marco normativo relacionados con la Gestión Integral del Riesgo tienen como fundamento un conjunto de Leyes, Decretos, Resoluciones, Directivas y artículos, que definen y orientan su estudio y aplicación.

Entre las normas que la regulan se destacan:

- Constitución Política de Colombia. (CPC). Artículos 209, 218, 219 y 269.
- Ley 87 de 1993. "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones".
- Ley 489 de 1998. "Estatuto Básico de Organización y Funcionamiento de la Gestión Pública".
- Decreto 2145 de 1999. "Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las entidades y organismos de la Gestión Pública del orden nacional y territorial y se dictan otras disposiciones". Modificado parcialmente por el Decreto 2593 de 2000.
- Decreto 1537 de 2001. "Por el cual se reglamenta parcialmente la Ley 87 de 1993, en cuanto a elementos técnicos y administrativos que fortalezcan el Sistema de Control Interno en las entidades y organismos del Estado".
- Ley 872 de 2003. "Por la cual se crea el Sistema de Gestión de la Calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".
- Decreto 4110 de 2004. "Por el cual se reglamenta la Ley 872 de 2003 y se adopta la Norma Técnica de Calidad en la Gestión Pública".
- Decreto 4485 de 2009. "Por medio de la cual se adopta la actualización de la norma técnica de calidad en la gestión pública".
- Decreto 2641 de 2012 "Por medio del cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011 "Estatuto Anticorrupción".
- Decreto 943 de 2014. "Por el cual se actualiza el Modelo Estándar de Control Interno" – MECI.
- Decreto 124 de 2016 "Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".
- Guía de Riesgo del Departamento Administrativo de la Función Pública DAFP 2009.
- Norma Técnica de Calidad para la Gestión Pública NTCGP-1000:2009.
- Norma Técnica NTC-ISO 31000 Gestión Integral del Riesgo. Principios y Directrices.
- Norma Técnica Colombiana NTC- ISO/IEC 27001, 27002 y 27005. Sistema de Gestión de la Seguridad de la Información. Requisitos y Código de buenas prácticas para la gestión de seguridad de la información.
- Norma Técnica Colombiana NTC OHSAS 18001. Sistemas de gestión en seguridad y salud ocupacional. Requisitos.
- Norma Técnica Colombiana NTC ISO 14001. Sistemas de gestión ambiental. Requisitos.
- Norma Técnica Colombiana NTC 5722 Gestión de la continuidad de negocio. Requisitos.
- Guía Técnica Colombiana GTC 176 Manual para la gestión de la continuidad de negocio.
- Guía Técnica Colombiana GTC 45 Guía para la identificación y la valoración de los riesgos en seguridad y salud ocupacional.
- Guía Técnica Colombiana GTC 104 Guía gestión del riesgo ambiental.

- Guía Técnica Colombiana GTC 137 Gestión Integral del Riesgo.
- Guía para la Gestión del Riesgo de Corrupción.
- Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

CAPÍTULO II

DIRECCIÓN Y COMPROMISO

ARTÍCULO 7. POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO.

La Policía Nacional se compromete a administrar de manera integral los riesgos inherentes a la misionalidad institucional, sirviéndose para ello tanto de la "planeación" (misión, visión, establecimiento de objetivos, metas, factores críticos de éxito), como del campo de aplicación (procesos, planes, proyectos, programas, sistemas de información), al igual que del Componente Direccionamiento Estratégico y todos sus elementos.

Del mismo modo expresamos mediante la Gestión Integral del Riesgo, un especial compromiso en el tratamiento del riesgo de corrupción y de aquellos identificados a partir de los "Aspectos e Impactos Ambientales", "Activos de Información" y "Peligros" del quehacer policial, como medida preventiva, correctiva y/o detectiva ante la posible afectación a la integridad policial, el medio ambiente, la seguridad de la información y eventos (accidentes – incidentes) asociados a la Seguridad y Salud en el Trabajo.

ARTÍCULO 8. PRINCIPIOS.

La Institución adopta los siguientes principios para una eficaz Gestión Integral del Riesgo, como medio para el entendimiento del impacto y alcance que se pretende alcanzar con la ejecución de esta herramienta institucional, así:

- La Gestión Integral del Riesgo en la Policía Nacional es considerada de vital importancia por parte del Mando Institucional: Involucramos en todas las actividades de carácter institucional la gestión integral del riesgo para la toma de decisiones respecto al tratamiento de los riesgos Institucionales, Masivos por Procesos e Individuales.
- La Gestión Integral del Riesgo en la Policía Nacional es sinónimo de solución de fallas, problemas, inconsistencias, debilidades, peligros y amenazas: Aplicamos de forma permanente y sin limitaciones la metodología del riesgo adoptada por la Institución, como instrumento potenciador de todo lo que se realice en la misma.
- La Gestión Integral del Riesgo en la Policía Nacional es productora de sinergia: Damos una mirada holística a todos los temas de preocupación institucional, para dar solución a los mismos de forma integral y unificada; ningún tema es más importante que otro, esto lo determinamos con la aplicación de la gestión del riesgo en cada uno de los ámbitos policiales.
- La Gestión Integral del Riesgo en la Policía Nacional es influyente, incluyente y coyuntural: No tenemos espacios vetados para la aplicación de la administración del riesgo, ni se limitan los esfuerzos determinados por esta para mejorar sin pausa nuestro campo de acción.
- La Gestión Integral del Riesgo en la Policía Nacional es intuitiva y anticipativa: La prospectiva institucional desarrollada a partir del método de riesgos, nos permite vincular, descifrar y adaptarnos a escenarios inciertos y potencialmente difíciles para la Institución.
- La Gestión Integral del Riesgo en la Policía Nacional hace parte de un todo: Identificamos, valoramos, tratamos y damos nuestros resultados de la gestión del riesgo basándonos en los hallazgos y/o no conformidades evidenciadas, los productos y/o servicios no conformes traducidos en quejas y reclamos, el incumplimiento de las metas de los indicadores asociados a los planes,

proyectos y programas, al igual que a partir de los riesgos identificados materializados; significando así, que medimos la gestión de la Policía Nacional integralmente.

ARTÍCULO 9. COMPROMISO DE LA ALTA DIRECCIÓN.

La alta dirección de la Policía Nacional define la política institucional para la gestión integral del riesgo, igualmente promueve el cambio cultural para lograr el compromiso a todo nivel mediante la aplicación de los principios de la Gestión Integral del Riesgo.

ARTÍCULO 10. ESTRUCTURA PARA LA GESTIÓN INTEGRAL DEL RIESGO.

Para gestionar de manera integral los riesgos en la Policía Nacional se cuenta con la siguiente distribución de responsabilidades, bajo los lineamientos y liderazgo de la Alta Dirección.

Figura 1: Niveles de responsabilidad para la gestión integral del riesgo.

CAPÍTULO III

MARCO DE REFERENCIA PARA LA GESTIÓN INTEGRAL DEL RIESGO

ARTÍCULO 11. GENERALIDADES.

La Policía Nacional es consciente de que el éxito de la Gestión Integral del Riesgo dependerá de la eficacia de la aplicación del presente marco de referencia, a partir del cual se sientan las bases y las disposiciones que se deben implementar en todos los niveles de la Institución. El marco ayuda a la dinámica eficaz del riesgo a través de la aplicación del procedimiento para la gestión integral del riesgo en los diversos niveles y en el contexto específico. El marco de referencia para la Gestión Integral del Riesgo garantiza que se reporte de manera adecuada y se utilice como base para la toma de decisiones y la rendición de cuentas en todos los niveles.

ARTÍCULO 12. LA ORGANIZACIÓN Y SU CONTEXTO.

Antes de empezar el diseño e implementación del marco de referencia para la gestión integral del riesgo, es importante evaluar y entender el contexto tanto externo como interno de la organización, dado que este puede tener influencia significativa en el resultado final.

Para garantizar el cumplimiento de su misión y el logro de su visión, cuenta con funcionarios, distribuidos en la categoría de Oficiales, Suboficiales, Nivel Ejecutivo, Agentes, Auxiliares Bachilleres, Auxiliares de Policía y personal No Uniformado, distribuidos en todo el país (ciudades, municipios, corregimientos e inspecciones), logrando un cubrimiento nacional y cuenta con una estructura orgánica conformada por direcciones y oficinas asesoras que integran la Policía Nacional. Posee un modelo gerencial conformado por tres componentes: "Estrategia y Gestión Estratégica", "Gestión y Estructura de Procesos" y "Talento Humano y Gestión de la Cultura", componentes que interactúan entre ellos para generar la Cultura en la Policía Nacional. Así mismo tiene definida una formulación estratégica que incluye además de la misión y visión, la mega, los principios y valores, la política y objetivos de calidad, políticas y lineamientos de la Dirección General, entre otros referentes básicos que orientan los esfuerzos hacia la excelencia en el servicio. (Ver Manual del Sistema de Gestión Integral).

Puesto que la Gestión Integral del Riesgo debe estar alineado con la cultura, los procesos, la estructura y la estrategia de la Entidad, es importante ampliar el análisis del contexto mediante la consulta del documento "Revisión y formulación estratégica definida para la Policía Nacional de Colombia" para cada cuatrienio, en donde se analice el rol estratégico de las unidades y oficinas asesoras de primer y segundo nivel y a partir de ellos se evaluarán los "logros clave", los "retos clave", así como las "brechas de cumplimiento" existentes entre el nivel esperado y el nivel recibido en los servicios prestados por dichas unidades, según la percepción de sus clientes internos y externos.

ARTÍCULO 13. OBJETIVOS Y METAS DE LA GESTIÓN INTEGRAL DEL RIESGO.

Los objetivos establecidos en la gestión integral del riesgo involucran de forma específica los aspectos relacionados con el funcionamiento institucional, definiéndolos de la siguiente manera:

- Identificar los riesgos asociados a la implementación de un Sistema de Seguridad y Salud Ocupacional, al igual que la identificación y valoración de peligros (incidentes y/o accidentes) que puedan llegar a afectar la integridad física de los funcionarios en términos de "Lesión" y/o "enfermedad" o "muerte".

- Identificar los riesgos asociados a la implementación de un Sistema de Gestión de Seguridad de la Información, al igual que la identificación y valoración de "Activos de Información".

- Identificar los riesgos asociados a la implementación de un Sistema de Gestión Ambiental, al igual que la identificación y valoración de los "Aspectos e Impactos Ambientales".

- Identificar los riesgos asociados a la implementación de un Sistema de Gestión de la Calidad, al igual que la identificación de los "procesos", "procedimientos" y "actividades" críticas y/o complejas que no permitan alcanzar los objetivos institucionales.

- Identificar las causas y situaciones expresas asociadas al riesgo de corrupción, su valoración y tratamiento, a partir de la implementación de las directrices emitidas por la Secretaría de Transparencia de la Presidencia de la República, mediante el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano".

La gestión tiene como meta una disminución significativa de la materialización de los riesgos y de los impactos que pudieran generarse, así como los costos asociados.

ARTÍCULO 14. ASIGNACIÓN Y DISTRIBUCIÓN DE RECURSOS.

- La Oficina de Planeación verificará y controlará que las unidades incluyan en el "Anteproyecto de Presupuesto" y posterior "Plan Anual de Adquisiciones" de cada vigencia, los bienes y servicios que para ejecución de los planes de tratamiento de los riesgos institucionales, masivos por procesos e individuales se requieran, con el fin de garantizar la apropiación presupuestal necesaria para la ejecución de las acciones de control establecidas dentro de dicho planes.

- Los bienes y servicios que por concepto de ejecución de planes de tratamiento, asociados a mitigar los riesgos de índole institucional, masivo por proceso e individual, y que estos se encuentren dentro del "Plan Anual de Adquisiciones", podrán ser modificados, previa solicitud expresa al señor Director y/o Subdirector (a) General y concepto de viabilidad por parte del Grupo Direccionamiento Institucional – Equipo de Gestión Integral del Riesgo y Grupo de Programación Presupuestal, respectivamente.

- Para cada vigencia las unidades con delegación del gasto, deberán construir su "Plan Anual de Adquisiciones", basados inicial y prioritariamente en los riesgos identificados y/o masificados por el nivel superior y de acuerdo a la asignación de acciones de control determinadas en los diferentes planes de tratamiento asociados a dichos riesgos. (Recordemos que un plan de tratamiento puede llegar a ser un proyecto o programa o una combinación de estos).

Nota 1: Los bienes y servicios incluidos en el "Plan Anual de Adquisiciones" y que correspondan al gestionamiento de los distintos planes de tratamiento de riesgos, solo podrán modificarse de acuerdo a lo conceptuado en la materia, debiéndose especificar en las solicitudes de modificación, que dicho bien y/o servicio corresponde al desarrollo de la administración del riesgo por parte de la Policía Nacional, por lo cual se debe relacionar el bien y/o servicio, a qué acción de control, plan de tratamiento y riesgo corresponde.

Nota 2 aclaratoria del punto tres de este artículo: la expresión "inicial y prioritariamente", hace alusión a que las unidades con delegación del gasto, deben disponer de manera perentoria los recursos para mitigar los diferentes riesgos asociados a su planificación y/o quehacer policial, a partir de cada ámbito o unidad de gestión, en correlación a lo dispuesto en la Política de Gestión Integral del Riesgo definida en este manual operacional.

ARTÍCULO 15. COMUNICACIÓN INTERNA.

- La divulgación del Manual para la Gestión Integral del Riesgo, será realizada por la Oficina de Planeación a través de los canales disponibles. En este sentido el personal uniformado y no uniformado que ostente el cargo de Administrador o Gestor del Riesgo debe realizar el curso básico de Gestión Integral del Riesgo, el cual se encuentra cargado en el sitio web institucional.

- La difusión del conocimiento a las áreas involucradas, se efectuará mediante talleres de capacitación teorico prácticos tanto presenciales, como virtuales contando con material didáctico para la enseñanza de cada una de las fases que componen la Gestión Integral del Riesgo.

- La Oficina de Planeación debe incluir en el "Plan Anual de Educación", las capacitaciones sobre la "Gestión Integral del Riesgo en la Policía Nacional".

- La Dirección Nacional de Escuelas emitirá por intermedio de las Escuelas de Policía, los certificados que acrediten la capacitación dada por la Oficina de Planeación y que se encuentren incluidas en el "Plan Anual de Educación".

- Es importante que los servidores del Área de Control Interno perfeccionen sus conocimientos, aptitudes y otras competencias relacionadas con la Gestión Integral del Riesgo, mediante la capacitación profesional continua; lo cual debe ser promovido por la Institución a través de la Oficina de Planeación, con el fin de que puedan desarrollar adecuadamente el rol que les corresponde en la materia.

  Las asesorías y/o retroalimentaciones deben ser realizadas por la Oficina de Planeación a los funcionarios del Área de Control Interno, de acuerdo a la programación del "Plan Anual de Auditorias" y/o cuando surja una nueva actualización del Manual para la Gestión Integral del Riesgo en la Policía Nacional, para garantizar su interpretación y entendimiento continuo.

ARTÍCULO 16. COMUNICACIÓN EXTERNA.

En caso de presentarse una crisis o materialización de un riesgo donde se requiera la coordinación interinstitucional o con la comunidad, la Institución cuenta con los medios físicos y tecnológicos necesarios para elaborar y desarrollar los planes de contingencia requeridos y dispone de los mecanismos para consolidar la información del riesgo proveniente de diversas fuentes externas.

CAPÍTULO IV

SEGUIMIENTO

ARTÍCULO 17. LA AUDITORÍA INTERNA A LA GESTIÓN INTEGRAL DEL RIESGO.

El propósito del Área de Control Interno respecto a la Gestión Integral del Riesgo, es el de proveer una evaluación objetiva a la entidad, a través del proceso de auditoría interna sobre la efectividad de las políticas y acciones en la materia, de cara a asegurar que los riesgos institucionales estén siendo administrados apropiadamente y que el Sistema de Control Interno está siendo operado efectivamente; como resumen de la función de valoración del riesgo a cargo del Área de Control Interno se pueden destacar los siguientes puntos:

- Evaluar reportes de riesgos institucionales, masivos por proceso e individuales.
- Revisar el manejo de los riesgos institucionales, masivos por proceso e individuales.
- Evaluar los casos de materialización de riesgos, a partir de incumplimientos evidenciados en las metas de los indicadores, tanto de gestión de procesos como de proyectos, planes y programas, al igual que el incumplimiento de requisitos (hallazgos o no conformidades), falta características y estandares (producto y/o servicio no conforme), para la prestación del servicio.
- Evaluar los casos de riesgos materializados a apartir de las situaciones de materialización asociadas a los mismos.

Parágrafo 1°: Los hallazgos o no conformidades evidenciados por el Área de Control Interno, Contraloría General de la República y/o Ente certificador o evaluador, que estén previamente considerados como causas (vulnerabilidades) dentro de la descripción de un riesgo identificado, deberán categorizarse como riesgos e iniciar la aplicación metodológica en este sentido.

Parágrafo 2°: Los hallazgos o no conformidades evidenciados por el Área de Control Interno, Contraloría General de la República y/o Ente certificador o evaluador, serán considerados como "eventos potenciales a evaluar" – EPE, con el fin de determinar si estos fueron riesgos que se materializaron (RM), si se tenían identificados, al igual que las causas que los originaron, y el tratamiento realizado. Si son considerados riesgos materializados pasan a ser Eventos a Evaluar – EE, debiéndose continuar los parámetros metodológicos de la gestión del riesgo.

CAPÍTULO V

MEJORA CONTINUA DEL MARCO DE REFERENCIA

ARTÍCULO 18. MEJORA CONTINUA DEL MARCO DE REFERENCIA.

Con base en los resultados del monitoreo, las revisiones y los informes de auditoría se deberán tomar decisiones sobre la forma en que se puede mejorar el marco de referencia, la política y los planes para la Gestión Integral del Riesgo.

ARTÍCULO 19. ACCIONES DE MEJORA.

Las decisiones tomadas como resultado del monitoreo del marco de referencia, deben originar mejoras y generar cultura en la Gestión Integral del Riesgo de la Institución.

Se hace énfasis en la mejora continua de la Gestión Integral del Riesgo a través del cumplimiento de las metas y objetivos de los procesos del SGI, alineados con los objetivos estratégicos de la Institución, la medición, la revisión y modificación posterior de procesos, sistemas, recursos, capacidad y habilidades.

ARTÍCULO 20. LECCIONES APRENDIDAS.

En el ámbito del riesgo, las lecciones aprendidas se entenderán como productos extraídos de la experiencia acumulada sobre la actividad del manejo integral del riesgo en las unidades, que permite elaborar una recomendación positiva o negativa –qué hacer o qué no hacer– con vistas a tener un Manual de comportamiento para dar respuesta a un evento semejante.

El propósito final de las lecciones aprendidas es emplear el conocimiento de manera eficiente, es decir, hacer uso del mismo para responder de manera óptima frente a un hecho del que ya se tiene experiencia. (Ver documento donde se define la Doctrina y las Lecciones Aprendidas en la Institución).

Las lecciones aprendidas deberían surgir del análisis periódico de la gestión integral del riesgo.

Para tal efecto, debe tenerse en cuenta la siguiente referencia bibliográfica:

- Guía Gestión de Riesgos 2009. Departamento Administrativo de la Función Pública. Guía Rol de las Oficinas de Control Interno. Auditoría Interna o quien haga sus veces. Departamento Administrativo de la Función Pública.
- ICONTEC: NTC- ISO 9001. Sistemas de Gestión de la Calidad.
- ICONTEC: NTCGP 1000:2009 Norma Técnica de Calidad en la Gestión Pública.
- ICONTEC: NTC ISO 31000. Gestión Integral del Riesgo. Principios y Directrices.
- Manual Técnico del Modelo Estándar De Control Interno Para El Estado Colombiano MECI 2014.
- Gestión Integral del Riesgo. ICONTEC Standard Australia.
- Gestión Integral de Riesgos. Tomo I 2° Ed. Bravo & Sánchez, 2007.
- Auditoría Basada en Riesgos. Ed. Ecoe, 2007.
- Manual para la aplicación de herramientas para el análisis de datos.
- Norma Técnica Colombiana NTC OHSAS 18001. Sistemas de gestión en seguridad y salud ocupacional. Requisitos.
- Norma Técnica Colombiana NTC ISO 14001. Sistemas de gestión ambiental. Requisitos.
- Norma Técnica Colombiana NTC 5722 Gestión de la continuidad de negocio. Requisitos.
- Guía Técnica Colombiana GTC 176 Guía para la gestión de la continuidad de negocio.
- Guía Técnica Colombiana GTC 137 Gestión Integral del Riesgo.
- Estatuto Anticorrupción.

ARTÍCULO 21. ACTUALIZACIONES AL PRESENTE MANUAL.

La facultad para realizar la actualización al presente Manual en cada una de sus partes, es responsabilidad de la Oficina de Planeación.

ARTÍCULO 22. DEPENDENCIAS RESPONSABLES DE SU APLICACIÓN.

La responsabilidad de desarrollar, implementar, mantener, revisar y perfeccionar las actualizaciones, estará a cargo de las direcciones, oficinas asesoras y sus unidades desconcentradas, de acuerdo con el ámbito misional que les corresponda. Para ello, se debe tener en cuenta para la planeación (misión, visión, establecimiento de objetivos, metas, factores críticos de éxito), la aplicación (procesos, proyectos, sistemas de información), del Componente Direccionamiento Estratégico y todos sus elementos, de acuerdo a lo establecido en el Modelo Estándar de Control Interno para el Estado Colombiano – MECI y otras normas.

Parágrafo 1°. Cada unidad policial debe conformar un Equipo de Gestión Integral del Riesgo, el cual evaluará trimestralmente el comportamiento de los riesgos de sus procesos misionales y de despliegue, para realizar la gestión y registrar la materialización de los riesgos (en el día a día), en atención a lo evaluado. El mencionado equipo, estará integrado por el Dueño del Proceso, Responsables de Procesos, Analistas de Procesos, Ejecutores, Gestores del Riesgo, tanto de la unidad como de los procesos, funcionario (s) que aplique (n) Mejora Continua (procedimiento acción correctiva) de acuerdo al proceso, un funcionario de Estrategia o su equivalente y el responsable del plan de compras, quienes presentarán los resultados de la evaluación al dueño del proceso y/o Director, Jefe o Comandante de la unidad para la toma de decisiones.

Nota: Puesto que el equipo antes mencionado está integrado por personal que direcciona el proceso y/o unidad, y los cuales tienen poder de decisión, no será necesario que para la aprobación de la información de las diferentes fases de la metodología, se lleven a instancia de Subcomité de Mejoramiento Gerencial.

Parágrafo 2°. La información que resulte del desarrollo de las fases de Identificación, Definición de la Gestión, Gestión del Riesgo, Medición de Resultados de la Gestión y Cierre, debe ser insertada en el módulo de Gestión Integral del Riesgo de la herramienta tecnológica establecida para tal fin, para aprobación o desaprobación del nivel superior del proceso y/o unidad que le corresponda misionalmente.

En este sentido, se entenderá que la información insertada en el aplicativo, fue previamente revisada y validada por el dueño del proceso y/o Director, Jefe o Comandante de la unidad, para aprobación del nivel respectivamente superior.

Parágrafo 3°. Acción a tomar en relación a la aplicación de la metodología del riesgo en la Dirección de Antinarcóticos – Área de Aviación Policial.

Toda vez, que el Área de Aviación Policial cuenta con el Grupo Integral de Seguridad Operacional, donde desarrolla sus actividades preventivas, proactivas y reactivas enfocados en la identificación de los peligros; el análisis, la evaluación y el tratamiento de los riesgos en beneficio de la seguridad de las operaciones áreas, logísticas, de mantenimiento y administrativas aeronáuticas; enmarcadas en las normas, reglamentos nacionales e internacionales de aviación y las directrices institucionales con respecto a la Gestión de Riesgos se determina los Niveles Aceptables de Seguridad Operacional, para el desarrollo adecuado de los objetivos de la Aviación Policial en apoyo a la misionalidad institucional.

Dentro de las actividades de Investigación de Seguridad Aérea Aeronáutica en la Aviación Policial, se busca establecer las posibles debilidades organizacionales y tecnológicas, los errores y/o infracciones humanas referentes a los procedimientos y apreciaciones de las condiciones ambientales y lugares de trabajo, y la relevancia de las fortalezas en la toma de decisiones inmediatas que lograron mitigar una parte del accidente o incidente aeronáutico en la Aviación Policial.

Se expresan a continuación las consideraciones que se deben tener en cuenta para la ejecución de la acción preventiva, correctiva y/o acción de contingencia en el tratamiento de los riesgos, para cuando un hecho de esta naturaleza acontezca, así:

Tendrá poder preferente el procedimiento de Seguridad Aérea y la metodología en prevención de accidentes, sobre la aplicación de la acción preventiva y correctiva de mitigación exigida por los preceptos de este manual, debiéndose para ello apoyarse en el desarrollo de las acciones establecidas en el Manual de Seguridad Operacional para la Aviación de la Policía Nacional en caso de accidente o incidente aeronáutico policial; posteriormente de acuerdo a los resultados arrojados por la investigación aeronáutica, se actualizará la información para la Gestión del Riesgo tal como está definido en el numeral 7.2.4.3. Por lo anterior se requiere que la información suministrada a la dependencia de Planeación de la Dirección de Antinarcóticos, se allegue con los criterios estipulados dentro de link "Realizar Gestión del Riesgo" del módulo riesgos PRO.

Parágrafo 4°. La Dirección de Antinarcóticos debe desarrollar para efectos de administración de los riesgos asociados al Área de Aviación Policial en el ejercicio del procedimiento "Realizar Vuelos Policiales", lo establecido en el Manual del Sistema de Gestión de la Seguridad Operacional (SMS) para la Aviación Policial; así como lo contemplado en el capítulo 2 y 5 del documento 9859 "Organización Aviación Civil Internacional".

Parágrafo Transitorio. Los parágrafos 3° y 4° de que trata este artículo, entrarán en vigencia una vez se apruebe el "Manual de Seguridad Operacional para la Policía Nacional", por parte del señor Director General, lo cual debe ser notificado por la Dirección Antinarcóticos a la Oficina de Planeación, para iniciar el respectivo empalme metodológico.

Parágrafo 5°. La Policía Metropolitana de Bogotá es una dependencia policial de tercer nivel que dependerá directamente de la Oficina de Planeación, para el asesoramiento metodológico en el tema de administración del riesgo, en atención a su relevancia e importancia como unidad de referencia en el ámbito nacional y por el desarrollo de la actividad de policía en el Distrito Capital.

En esta metodología se establecen 3 flujos para la parametrización de la información de las diferentes fases, de la siguiente manera:

- Flujo para riesgos Institucionales.
- Flujo para riesgos Masivos por Procesos.
- Flujo para riesgos Individuales.

Para ampliación y mejor comprensión sobre el uso del módulo de Gestión Integral del Riesgo, se debe consultar el manual del usuario de la herramienta tecnológica donde se encuentra desarrollado el mencionado módulo. La Oficina de Planeación será la encargada permanentemente de capacitar a los Gestores del Riesgos de los niveles Estratégico, Táctico y Operacional en lo concerniente al uso y manejo del módulo en referencia.

Parágrafo 6°: Las "Notas" relacionadas en el presente Manual, son aclaraciones y/o especificaciones sobre un determinado tema, las cuales son de obligatorio cumplimiento.

ARTÍCULO 23. APROPIACIÓN, ASESORAMIENTO Y ENTRENAMIENTO DE LOS GESTORES DEL RIESGO POR NIVELES DE PROCESOS Y/O UNIDADES

El funcionario que sea designado como Gestor del Riesgo en cada uno de los niveles institucionales, tendrá la siguiente dependencia para la apropiación, asesoramiento y entrenamiento sobre la "Gestión Integral del Riesgo", así:

Parágrafo: La apropiación, asesoramiento y entrenamiento respecto a la Gestión Integral del Riesgo, será realizado por parte del nivel superior, teniendo en cuenta el proceso y/o unidad que lo requiera.

Cuando los gestores de riesgos de las direcciones y oficinas asesoras sean trasladados y/o asignados al cargo de gestor del riesgo, la Oficina de Planeación debe garantizar de manera previa la apropiación, asesoramiento y entrenamiento metodológico en el tema de administración de riesgo, de acuerdo a los preceptos de este manual.

Respecto de las direcciones y oficinas asesoras que tengan unidades desconcentradas o desplieguen sus procesos, los gestores del riesgo dependerán de estas, en cuanto a la apropiación y asesoramiento metodológico en el tema de administración de riesgo, de acuerdo a los preceptos de este manual.

Ejemplo 1:

Los gestores del riesgo de las Policías Metropolitanas y los Departamentos de Policía, dependerán de las Regiones de Policía, quienes a su vez dependerán de la Dirección de Seguridad Ciudadana.

Ejemplo 2:

Si un Gestor del Riesgo de una Escuela de Policía requiere explicación para aclarar dudas o inquietudes respecto al desarrollo de una fase o uso del módulo de riesgo (aspecto metodológico), esta solicitud debe ser atendida por el Gestor del Riesgo de la Dirección Nacional de Escuelas o los gestores del riesgo de los procesos misionales (aspecto técnico), en caso de ser una inquietud sobre la información asociada a riesgos a partir del proceso de formación, investigación o educación continua.

Nota: Además de la Inducción y entrenamiento en el cargo los gestores de riesgo no podrán prescindir de la apropiación, asesoramiento y entrenamiento que debe darle la unidad o el proceso superior.

CAPÍTULO VI

EJECUCIÓN DE LAS FASES DE LA GESTIÓN INTEGRAL DEL RIESGO

ARTÍCULO 24. OPERACIONALIZACIÓN METODOLÓGICA

La operacionalización metodológica se establece como aspecto fundamental para el desarrollo secuencial y sistemático de las fases de Identificación, Definición, Gestión, Medición y Cierre, las cuales deben

desarrollarse de la siguiente manera, teniendo en cuenta cada uno de los numerales que en ella se disponen, así:

1. Objetivo: Proporcionar las directrices para la Gestión Integral del Riesgo en la Policía Nacional. Los objetivos específicos son:

1.1. Establecer los lineamientos para identificar, describir, calificar, evaluar y priorizar el tratamiento de los riesgos que puedan afectar o impedir el logro de los objetivos institucionales.

1.2. Identificar los parámetros que se deben tener en cuenta para definir acciones de tratamiento que permitan disminuir la probabilidad de ocurrencia de los riesgos y/o disminuir su impacto.

1.3. Hacer seguimiento a la ejecución de las acciones planificadas y revisar su eficacia.

2. La metodología consta de 5 fases: Estas fases se desarrollan de acuerdo con los parámetros que se disponen tanto en los aspectos generales como específicos del presente Manual, de la siguiente manera:

Identificación de Riesgos: en esta fase el objetivo es hacer una adecuada identificación y descripción de los riesgos de forma que se facilite el desarrollo de las siguientes fases. Como aspectos relevantes se han estandarizado factores y agentes generadores (en relación con las causas o vulnerabilidades), incluye la identificación de situaciones de materialización para cada riesgo, la identificación de controles de detección tanto de riesgos materializados como de efectos y la estandarización de los efectos. Con la estandarización de factores, agentes generadores y efectos se pretende que la labor de describir un riesgo sea mucho más práctica y asertiva.

Definición de la Gestión: Incluye el análisis antes de controles, la valoración de controles y el análisis después de controles, con el fin de priorizar los riesgos para su tratamiento.

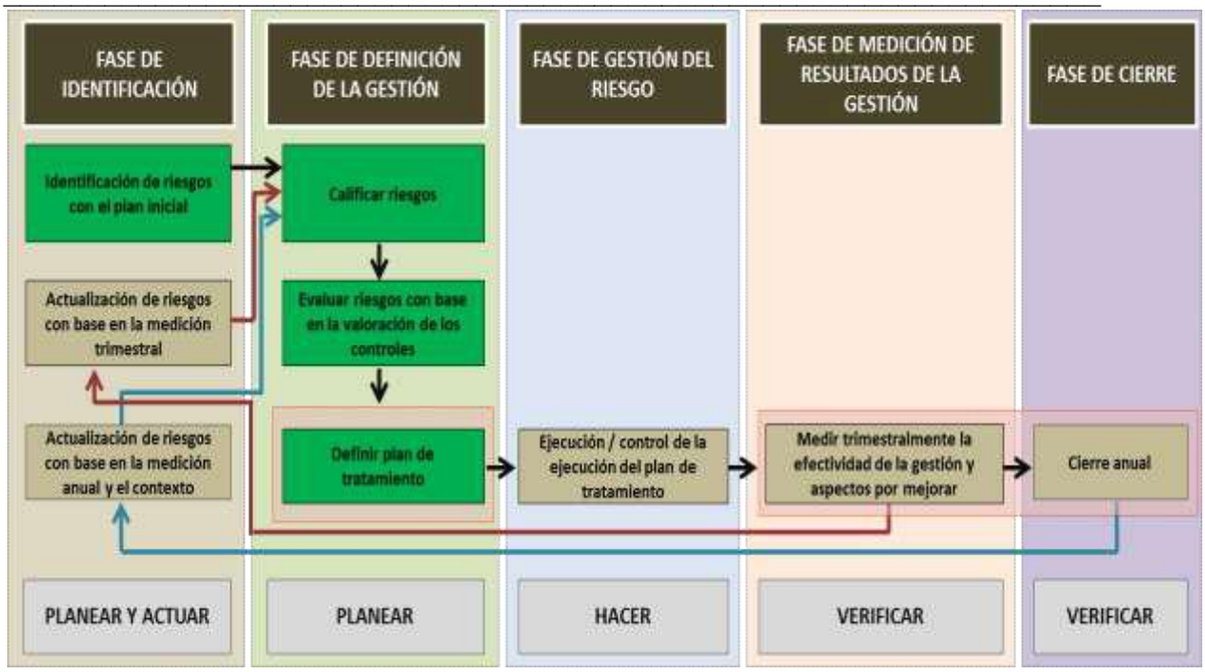
La calificación (análisis) se hace con base en las situaciones materializadas (de la fase de Identificación), la identificación / valoración de controles se hace por causa o efecto dependiendo de si es un control preventivo o correctivo. De esta forma se dan las herramientas para la formulación de planes de tratamiento coherentes con las causas más relevantes y permiten obtener un panorama global de la Institución con el fin de formular planes que impacten de forma significativa la gestión.

Gestión de Riesgos: En esta fase se registran las acciones ejecutadas de los planes de tratamiento y los resultados del proceso, tomados de las herramientas del Sistema de Gestión Integral, facilitando la actualización de la descripción de riesgos y la actualización del nivel de riesgos de manera constante y objetiva.

Medición de Resultados de la Gestión: Con base en la información registrada en resultados de gestión de los procesos, se miden los resultados en términos de la gestión del proceso. Muestra aspectos como riesgos materializados, la medición de la disminución y/o el aumento del nivel de riesgos con su respectivo análisis y la medición del desempeño de los planes de tratamiento (planes, programas y/o proyectos) de los riesgos institucionales, masivos por procesos e individuales.

Cierre: En esta fase se consolidan los resultados trimestrales y se incluye la generación y análisis de situaciones específicas que contribuyan a fortalecer los activos de la Institución en términos del conocimiento en Riesgos: Lecciones Aprendidas.

3. La siguiente gráfica muestra las fases, su secuencia y su relación con el ciclo PHVA.



La construcción de esta metodología incluye elementos de:

Manual del Departamento Administrativo de la Función Pública 2011, DAFP.
Norma de Gestión Integral del Riesgo ISO 31000:2009.
GTC137:2011. Definiciones y Términos Genéricos Relacionados con la Gestión Integral del Riesgo.
GTC 176. Guía para la Gestión de la Continuidad de Negocio.
Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014.
Normas ISO 9001:2008 y NTCGP 1000:2009.
Norma ISO 27005 Gestión del Riesgo en la Seguridad de la Información.
Norma ISO 14001 Requisitos Sistema de Gestión Ambiental.
Norma ISO 18001 Requisitos Sistema de Gestión en Seguridad y Salud Ocupacional.

4. PLAN INICIAL DE IDENTIFICACION (RIESGOS INHERENTES AL PROCESO)

4.1 OBJETIVO DEL PLAN

El objetivo de este plan es la identificación de los eventos potenciales que pueden poner en riesgo la adecuada gestión tanto de los procesos como de la Institución, utilizando como fuentes de identificación el los objetivos institucionales, objetivo del proceso, los indicadores que permiten medir el cumplimiento de ese objetivo y el análisis de los procedimientos que se ejecutan en cada proceso por nivel, se espera que al implementar este plan determinemos el panorama global de todos los riesgos asociados a los objetivos y actividades inherentes a la misión de la Institución y por ende, de sus procesos. Este Plan se debe implementar una vez, posteriormente se deberá utilizar lo descrito en la Fase 1. Identificación / actualización de Riesgos de la presente metodología.

Se requiere identificar los riesgos por las fuentes anteriormente nombradas para cada uno de los procesos definidos.

Para cada riesgo identificado se deberán establecer las posibles fuentes (Clase de factor y agente generador), causas, los efectos, las situaciones de materialización del riesgo. Una buena descripción de los riesgos es fundamental para priorizar la gestión de la Institución.

Nota: Entiéndase por proceso todo aquello que realiza la Policía Nacional para lograr su misionalidad y dar cumplimiento a los diferentes requisitos legales, los cuales se denominarán "fuentes" de acuerdo al tema específico que se considere, y serán analizados y evaluados desde la perspectiva de la gestión integral del riesgo.

4.2 RESPONSABLES DE EJECUCIÓN

Gestores de riesgos de los tres niveles.

Cada gestor de riesgos deberá hacer el trabajo de identificación con un número representativo de funcionarios que pertenezca al proceso. Como evidencia de la participación de los funcionarios del proceso deberán quedar actas de reunión.

La Oficina de Planeación revisará y retroalimentará a cada gestor de riesgos de primer y segundo nivel.

Para la revisión y retroalimentación de los riesgos identificados en los procesos de tercer nivel, se acordarán mecanismos con los gestores de primer y segundo nivel, de forma que ellos, con base en su conocimiento y experiencia participen activamente en la revisión y retroalimentación.

4.3. DESCRIPCIÓN DE ACTIVIDADES

4.3.1. Identificación de Riesgos por Proceso y/o ámbitos de gestión.

Para la identificación de riesgos se deben tener en cuenta los siguientes aspectos:

La identificación de riesgos se debe hacer por proceso y por nivel. Es importante tener claridad de cuáles son las diferencias entre los objetivos de un proceso en cada uno de sus niveles, cuáles son las actividades realizadas en cada nivel, y cuáles son los indicadores que permiten medir el desempeño en cada nivel. La redacción debe ser clara y simple, evitando "adornar" los textos.

Como ayuda para identificar los riesgos en cada proceso, se relacionan a continuación las fuentes que deben ser revisadas. No existe obligatoriedad de identificar un riesgo para cada fuente, sólo se espera que al revisar cada una de ellas, cada proceso del sistema haya realizado un trabajo estructurado que demuestre una adecuada planificación de su gestión, a través de la identificación de la mayor cantidad de riesgos de su proceso.

4.3.1.1. Fuente: Objetivo del proceso

Los gestores de riesgos deberán identificar los riesgos asociados al objetivo de su proceso, en su nivel.

El objetivo se deberá tomar de la caracterización vigente. Como ayuda, se podrá tener en cuenta lo siguiente:

NIVEL	ACTIVIDAD GENERAL
Procesos de Primer Nivel	Direccionar, dar lineamientos a toda la Institución, a su proceso en el segundo nivel o a sus despliegues en segundo y tercer nivel. Con base en los resultados del seguimiento reportados por el segundo nivel, proponer nuevos lineamientos que propicien la mejora.
Procesos de Segundo Nivel	Con base en el direccionamiento recibido del primer nivel de su proceso, definir planes, programas o proyectos para ser ejecutados e impactar al segundo y tercer nivel. Hacer control y seguimiento a la ejecución de los lineamientos por parte del tercer nivel y retroalimentar. Consolidar resultados e informar al primer nivel.
Procesos de Tercer Nivel	Ejecutar los lineamientos recibidos por su proceso en el segundo nivel, controlar la ejecución de las acciones e informar los resultados y cualquier información relevante que resulte de ello.

En la tabla se observa que los procesos de primer y segundo nivel tienen riesgos asociados con las actividades de direccionar, difundir, hacer control y retroalimentar.

Hay procesos de primer y segundo nivel que adicionalmente a las actividades mencionadas en la Tabla, expresan en su objetivo actividades adicionales. Por tanto hay que tenerlas en cuenta para la identificación.

4.3.1.2. Fuente: Indicadores del proceso

Se deben identificar los riesgos asociados a los indicadores formulados en cada proceso, en cada nivel. ¿Qué podría ocurrir que afectara el logro de las metas de los indicadores?. Los indicadores del proceso se deberán tomar de la caracterización vigente. Verificar y complementar la información de los indicadores (temporizador, meta, etc.), con las Fichas Técnicas de los indicadores.

De las normas ISO9001/NTCGP1000, numeral 8.2.3: "La entidad debe aplicar métodos apropiados para el seguimiento de los procesos del Sistema de Gestión de la Calidad, y cuando sea posible, su medición.

Estos métodos deben demostrar la capacidad de los procesos para alcanzar los resultados planificados". Con base en la definición anterior, se deberán tomar en cuenta para la identificación de riesgos en este punto, aquellos indicadores que permitan medir el cumplimiento de los objetivos de los procesos.

Nota 1: Si los objetivos de los procesos están formulados claramente y los indicadores se plantearon de acuerdo a lo descrito en el numeral 8.2.3., muy probablemente los riesgos por estas dos fuentes (objetivos e indicadores) van a ser los mismos. Si este es el caso, no se debe escribir el riesgo dos veces.

Nota 2: El enfoque de la identificación de riesgos por la fuente indicadores es en relación con la pregunta: ¿Qué podría ocurrir que afectara el logro de las metas de los indicadores en el proceso? No se deben identificar riesgos enfocados a los aspectos genéricos de los indicadores como: Indicadores que no aportan a la mejora del proceso, no contar con información oportuna y confiable para la toma de decisiones, incumplimiento de las metas del indicador, formulación equivocada del indicador, que la meta no sea la adecuada para el indicador formulado, etc.

4.3.1.3. Fuente: Actividades de riesgo en los procedimientos.

El análisis de los procedimientos permite obtener una visión detallada del proceso analizado. Este análisis tiene dos objetivos:

- Identificar las actividades de más alto riesgo para el logro de los objetivos.
- Determinar si los procedimientos existentes son suficientes para asegurar que los funcionarios del proceso tengan disponible la descripción de las actividades que deben realizar, evitando así que se cometan errores, que se dejen de realizar actividades o no se hagan de la forma adecuada, que se pierda tiempo por no tener claridad de cómo dar cumplimiento a la totalidad de sus responsabilidades.

El conocimiento del proceso es crítico para la realización de esta actividad. Lo que debe hacerse es identificar cual es el verbo en la actividad analizada y posteriormente hacer las siguientes preguntas acerca de esa actividad:

- ¿La actividad analizada genera impactos ambientales?
- ¿La actividad analizada requiere el manejo, almacenamiento o contacto con información sensible?
- ¿La actividad analizada utiliza equipos / maquinaria de alto costo?
- ¿La actividad analizada es de contacto directo con la ciudadanía o con algún ente externo?
- ¿La actividad analizada requiere o puede requerir el manejo, almacenamiento o contacto con dinero (directa o indirectamente)?
- ¿La actividad analizada puede llevar a la toma de decisiones que afecten a una gran población de la comunidad policial?
- ¿Dentro del procedimiento hay alguna actividad realizada por un tercero?
- ¿La actividad analizada requiere para su realización de un alto nivel de competencia (educación, formación, habilidades, experiencia) en algún aspecto específico?
- ¿La actividad analizada puede involucrar algún daño físico a quien la desempeña?

Los aspectos anteriores ayudarán a identificar si una actividad es crítica o no, desde el punto de vista de los riesgos en cada proceso se deberán analizar los procedimientos correspondientes al nivel para el cual se está efectuando la identificación, es decir, aquellos procedimientos en los que los ejecutores son funcionarios del proceso en el nivel que se está analizando.

El gestor de riesgos deberá asignar las responsabilidades de análisis de los procedimientos entre los funcionarios del proceso. Los resultados de esta actividad se deberán plasmar en el documento "Análisis de Documentos / Actividades por Procesos para la Identificación de riesgos". Cada procedimiento deberá ser analizado por al menos dos ejecutores del mismo. La revisión de los resultados del análisis la realizará el gestor de riesgos.

4.3.1.4 Fuente: Inventario de activos de información

El "Inventario de Activos" debe ser un documento controlado que contenga información detallada en este aspecto, tomando como base la "información electrónica", "información física", "software", "hardware" y la "infraestructura", por lo cual, se debe actualizar permanentemente por parte de la dependencia responsable de asegurar la información, en cada uno de los niveles y ámbitos institucionales.

Nota: La referencia o uso de las palabras "formato o formulario" en este manual, corresponden a los campos o formas definidas en el módulo de riesgos PRO. Al igual que a los formatos utilizados por la Oficina de Telemática dentro de la implementación de la norma ISO/IEC 27005 Gestión de riesgos de la seguridad de la información.

4.3.1.4.1 Valoración de activos de información

Para que las actividades de la metodología de riesgos sean eficientes, estas se deben enfocar al análisis de los activos con mayor valoración, es decir, los activos que en caso de materialización del riesgo puedan tener las mayores consecuencias negativas para la institución. Por esta razón, a partir de la "valoración de los activos", se seleccionan los que obtuvieron una calificación igual o superior a 3: importante, para que se tengan en cuenta en la fase de identificación de riesgos y se analicen con detalle.

Para realizar la valoración de activos, se debe tener en cuenta la Tabla de Valoración y Clasificación de Activos de Información, que se muestra a continuación.

Tabla de Valoración y Clasificación de Activos de Información

Clasificación	Valor mayor o igual a	Descripción Disponibilidad	Descripción Confidencialidad	Descripción Integridad
BAJO	1	No esenciales, la interrupción es de hasta 30 días	PÚBLICA: información entregada o publicada sin restricciones, sin que esto conlleve un impacto negativo de ninguna índole para la institución.	No afecta la operación y puede repararse fácilmente.
MEDIO	2	Normal, interrupción de hasta siete días	INTERNO: es aquella información dirigida a los miembros de la Institución, cuya divulgación, uso, alteración o destrucción podría resultar en pérdidas recuperables para la institución, pero implica asuntos de conveniencia, facilidad de la operación, credibilidad o reputación u otros asuntos relacionados con la privacidad.	Puede repararse, perdidas leves
IMPORTANTE	3	Importante, interrupción hasta por 72 horas	CONFIDENCIAL: información que por su contenido solo interesa a quienes va dirigida y cuya divulgación no autorizada puede ocasionar perjuicios a una unidad o persona.	Difícil reparación y pérdidas significativas.
ALTO	4	Urgente la interrupción hasta por 24 horas	RESERVADO: información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la Institución, proporcionar ventajas a la amenaza actual o potencial, o causar bajas o pérdidas propias en acciones de defensa nacional.	No puede repararse y ocasiona pérdidas graves para la institución
EXTREMO	5	Criticos, la interrupcion es de minutos y hasta 12 horas.	ULTRASECRETO: información pertinente a actividades o planes de la defensa nacional interna o externa o a operaciones de inteligencia cuya divulgacion no autorizada podría conducir a un rompimiento diplomatico que afecte los intereses de la Nacion a un ataque armado o a destruir la estabilidad interna.	No puede repararse y ocasiona perdidas graves para el país.

4.3.1.4.2 Identificación de riesgos por activos de información

Se realizará la identificación de riesgos a partir de la valoración de los activos de información, que puedan afectar alguno de los siguientes criterios de la seguridad de la información: confidencialidad, integridad o disponibilidad.

Se establecen tres componentes para el riesgo institucional de "Seguridad de la Información", los cuales deben quedar reflejados en el mismo para su análisis, valoración y tratamiento, así:

- Pérdida de la confidencialidad de los activos de información.
- Pérdida de la integridad de los activos de información.
- Pérdida de la disponibilidad de los activos de información.

4.3.2. Clase de Factor, Agente Generador, Causas – Vulnerabilidades.

Se deben identificar **TODAS** las posibles causas – vulnerabilidades que podrían generar cada uno de los riesgos identificados en el punto anterior, para hacerlo, tomar la información de la Tabla 1. Clase de Factor y Agente Generador, Tabla 1.1, 1.2 y 1.3 Causas-Vulnerabilidades Pérdida de Confidencialidad, Integridad y Disponibilidad. En el campo causa – vulnerabilidad, se debe describir específicamente la causa – vulnerabilidad que podría generar el riesgo en el proceso y en el nivel, coherentemente con la clase de factor y el agente generador identificado. Esta actividad la debe realizar el gestor de riesgos en el caso de los riesgos por fuentes objetivo del proceso e indicadores; en el caso de fuente procedimientos se sumarán al equipo los ejecutores designados para el análisis de los procedimientos.

Registrar la clase de factor, agente generador y causa – vulnerabilidad en el Formato o formulario de Descripción de Riesgos.

Nota 1: Para el caso de las vulnerabilidades, se debe tener en cuenta la Tabla 1.1, 1.2 y 1.3, correspondiente a las vulnerabilidades estandarizadas. (ver tablas).

Nota 2: Los únicos formatos autorizados para presentar información de riesgos, corresponden a aquellos que fueron estructurados para desarrollar la gestión del riesgo en el campo de seguridad de la información, en virtud a la implementación del "Sistema de Gestión de Seguridad de la Información". Por lo tanto la demás información producida por la aplicación de la metodología de riesgos, debe ser insertada en la herramienta tecnológica establecida para tal fin.

4.3.3. Situaciones de Materialización. Controles de Detección.

Se deben relacionar cuáles son las situaciones concretas en las que podría presentarse el riesgo, generalmente tienen formas diferentes de materialización. Para el caso de la identificación en la seguridad de la información, estás situaciones se encuentran estandarizadas por cada uno de los pilares, debiéndose tener en cuenta lo referenciado en la Tabla 1.4 Amenazas. En cuanto a las situaciones asociadas a los peligros, estas se establecerán de acuerdo a los parámetros de seguridad y salud ocupacional. Las situaciones de materialización son independientes de las causas, es decir, una sola situación de materialización puede generarse por una o por varias causas simultáneamente. Esto significa que no se debe asociar una situación específica de materialización por cada causa, sino por el riesgo.

Si un riesgo está bien identificado se debe poder responder a la pregunta: ¿cómo se puede materializar?, si no se puede responder esta pregunta, hay que revisar el riesgo identificado. Las situaciones de materialización deben ser concretas.

Establecer con claridad las posibles situaciones de materialización tiene tres objetivos específicos que son de vital importancia para las fases siguientes:

- Permite comprobar que el riesgo está bien identificado. (Fase de Identificación).
- Permite asignar con mayor claridad y criterio los valores de probabilidad de ocurrencia de riesgo. (Fase de Definición de la Gestión).
- Facilita determinar si un riesgo se ha materializado o no. (Fase de Gestión de Riesgos).

Hay situaciones en las que la materialización de un riesgo se detecta inmediatamente, mientras que hay otras situaciones en que se detecta el efecto de su materialización:

Ejemplo 1

Riesgo: (Que ocurra un accidente aéreo). ¿Cómo se puede materializar? Aquí la respuesta además de única, es obvia: cuando ocurre un accidente aéreo. Es un evento puntual. ¿Cómo se puede detectar que ocurrió? Porque de acuerdo con el protocolo (PRT0001), durante todo el tiempo en que una aeronave esté en vuelo, esta es constantemente monitoreada, lo cual, en caso de ocurrencia de un accidente permite conocer la situación inmediatamente. Adicionalmente, esta novedad queda registrada en el formato o formulario (FR0001) Reporte Novedades.

Ejemplo 2:

Riesgo: (Que un plan o estrategia no alcance los resultados planificados). ¿Cómo se puede materializar? Aquí hay que analizar un poco más que en el caso anterior. Habría que verificar cuáles eran los resultados planificados de ese plan o estrategia y este caso, la materialización del riesgo se va dar en términos de que los resultados de la medición planificada no cumplan con las expectativas.

Una situación de materialización nunca es: una queja, una demanda, una mala publicidad, etc. Estos son ejemplos de cómo se dan los efectos, no las situaciones de materialización.

Lo ideal es que se tengan mecanismos que permitan detectar los riesgos materializados inmediatamente (después de su materialización) cuando se presentan las situaciones. En el campo ¿Qué controles realiza en su proceso que permitan detectar la situación de materialización?, se debe escribir en la actualidad cómo se está detectando la situación que se materializa. En caso de que no haya un mecanismo definido para detectar la materialización, se deberá escribir: "No hay". No contar con mecanismos que permiten detectar que un riesgo se ha materializado, será un aspecto a considerar cuando se defina el plan de tratamiento del riesgo.

4.3.4. Efectos. Controles de Detección.

Se deben identificar **TODOS** los posibles efectos que podrían generarse si los riesgos identificados se materializaran y se deben registrar en el campo de "Efectos" del módulo de riesgos PRO.

Los posibles efectos para cada uno de los riesgos identificados se seleccionarán de la Tabla 2. Efectos Potenciales.

Adicionalmente, debe indicarse, en la actualidad, cual es el registro que permite determinar que el riesgo materializado ha producido un efecto. Ejemplo:

Posible Efecto: Pérdida de imagen, credibilidad, confianza.
¿Cómo se detecta este efecto?: Informe de monitoreo de medios, quejas, reclamos.

Los efectos se definen en relación con las situaciones de materialización identificadas. Una sola situación de materialización puede generar varios efectos simultáneamente y un efecto puede darse para varias situaciones de materialización.

Esto significa que los efectos deben seleccionarse para el conjunto de situaciones de materialización y no deben encontrarse efectos repetidos para un mismo riesgo.

Tabla 1. CLASES DE FACTORES Y AGENTES GENERADORES

CLASE DE FACTOR	AGENTE GENERADOR
Económico	Disminución presupuestal para la Institución.
	Disminución presupuestal para el proceso.
	No disponibilidad oportuna de recursos.
Medio Ambiental	Catástrofes naturales.
Político	Nueva legislación que afecta a la Institución.
	Baja percepción y confianza por parte de la ciudadanía.
Social	Cultura ciudadana que no favorece el cumplimiento de la misión Institucional.
	Deficiente planificación o diseño de políticas, estrategias.
Estratégico	Deficientes o insuficientes controles de políticas, estrategias.
	Falta de conocimiento o entendimiento de los objetivos estratégicos de la Institución.
	Falta de conocimiento, entendimiento o aplicación de los principios y valores de la Institución.
	Las metas/resultados esperados no se conocen, no son claros o no se concertaron con los involucrados.
	Los mecanismos de comunicación interna no están bien definidos o no son claros para los funcionarios.
	Deficiente planeación de necesidades de recursos económicos.
	Cultura de los funcionarios que no favorece el cumplimiento de los objetivos.
	Capacidad insuficiente o no disponibilidad oportuna de los recursos de infraestructura.
Infraestructura (Edificios, espacios de trabajo, herramientas, transporte)	Actividades de mantenimiento de instalaciones y equipos no apropiadas y/ o insuficientes.
	Infraestructura no apropiada.
	Dificultades con el suministro de servicios públicos y privados.
	Competencias no definidas / no definidas adecuadamente.
Personal	Competencias no apropiadas.
	Alto nivel de rotación.
	Capacidad laboral no suficiente (la cantidad de trabajo excede la capacidad del personal).
	La estructura organizacional establecida no se ajusta a las necesidades del proceso.
	Los mecanismos de formación / capacitación no son los adecuados.

	Baja motivación.
Procesos/Procedimientos / planes	Deficientes o insuficientes controles de procesos o procedimientos.
	La definición / delimitación de autoridades y/o responsabilidades no es clara.
	Los mecanismos de difusión de información no son los adecuados.
	No están documentadas las actividades.
	Deficiente formulación de los mecanismos de seguimiento y/o medición (indicadores, encuestas, cronogramas, seguimiento a proyectos, etc).
	Deficientes / insuficientes controles a los proveedores
Tecnología (hardware, Software, sistemas de Información, Comunicación)	Actividades de mantenimiento y/o soporte de infraestructura tecnológica no apropiada y/o insuficiente.
	Tecnología obsoleta o que no cumple con lo requerido.
	Deficiencias en los controles que garantizan la seguridad de la Información.

Tabla 1.1 CAUSAS-VULNERABILIDADES PÉRDIDA DE CONFIDENCIALIDAD

RIESGOS	Pérdida de Confidencialidad
CAUSAS (VULNERABILIDADES)	Trabajo de personal externo o de mantenimiento no supervisado
	Carencia de procedimientos adecuados de reutilización de medios y computadores
	Desactualización de los Gestores de Base de Datos
	Desactualización en el Antivirus
	Desconocimiento / Falta de Capacitación en seguridad de la información
	Equipos de cómputo desatendidos
	Errores en la definición de Roles en la aplicaciones
	Falta de Aplicación de buenas prácticas en la configuración de aplicación
	Falta de capacitación de los usuarios
	Falta de capacitación en el uso de los aplicativos
	Falta de Capacitación en seguridad de la Información
	Falta de capacitación para las funciones asignadas
	Falta de conciencia sobre la seguridad de la información
	Falta de controles de acceso a la información
	Falta de definición y ejecución de Procedimientos de mantenimiento
	Falta de estándares de desarrollo para aplicaciones
	Falta de planes de Sensibilización en Seguridad de la información
	Falta de políticas / normas / procedimientos de seguridad de la información
	Falta de políticas de seguridad
	Falta de Políticas de Transmisión de Documentos
	Falta de Políticas para el uso de dispositivos de almacenamiento externos
	Falta de políticas que rijan el uso de los activos de información
	Falta de Procedimientos para el manejo de la información
	Falta de protección contra virus y código malicioso
	Falta de revocación de los derechos de acceso al activo de información una vez el funcionario cambie de rol o se retire de la organización
	Falta de Sensibilización en Seguridad de la Información
	Inadecuada clasificación de activos de información
	Inadecuado control de acceso lógico y/o físico a los activos de información
	Usuarios por Defecto en las Configuraciones

Tabla 1.2 CAUSAS-VULNERABILIDADES PÉRDIDA DE INTEGRIDAD

RIESGOS	Pérdida de Integridad
CAUSAS (VULNERABILIDADES)	Desactualización de los Gestores de Base de Datos
	Desactualización del Antivirus
	Desconocimiento / Falta de Capacitación en seguridad de la información
	Equipos desatendidos
	Errores en la Asignación de Permisos
	Errores en la definición de Roles en la aplicaciones
	Falta Consideraciones de la seguridad en los acuerdos con terceras partes
	Falta de capacitación a los usuarios en el manejo de aplicaciones
	Falta de capacitación en Seguridad de la Información
	Falta de capacitación para las funciones asignada
	Falta de conciencia respecto a la seguridad de la información
	Falta de controles contra códigos maliciosos
	Falta de controles de acceso a la información
	Falta de definición y ejecución de Procedimientos de mantenimiento
	Falta de documentación de los servicios y/o aplicaciones
	Falta de Documentación de pruebas.
	Falta de estándares de desarrollo para aplicaciones
	Falta de planes de Sensibilización en Seguridad de la información
	Falta de políticas / normas / procedimientos de seguridad de la información
	Falta de políticas de seguridad
	Falta de Políticas de Transmisión de Documentos
	Falta de Políticas para el Manejo de Contraseñas
	Falta de Políticas para el Tratamiento de la Información
	Falta de Políticas Para Inactivación de Usuarios
	Falta de políticas que rijan el uso de los activos de información
	Falta de Procedimientos para el manejo de la información
	Falta de revocación de los derechos de acceso al activo de información una vez el funcionario cambie de rol o se retire de la organización
	Falta de segregación de las funciones
	Falta de Sensibilización en Seguridad de la Información
	Falta de soporte
	Falta de mecanismos de monitorización de la red.
	Inadecuada clasificación de activos de información
	Inadecuado control de acceso lógico y/o físico a los activos de información
	Inexistencia de respaldo y/o custodia de los activos de información. (iniciativa de los usuarios)
	No Existencia de Políticas para el Tratamiento de la Información
	No existencia de un proceso de gestión de incidentes
	Trabajo de personal externo o de mantenimiento no supervisado
	Usuarios por defecto en las Configuraciones
	Versiones de los motores de bases de datos desactualizados

Tabla 1.3 CAUSAS-VULNERABILIDADES PÉRDIDA DE DISPONIBILIDAD

RIESGOS	Pérdida de Disponibilidad
CAUSAS (VULNERABILIDADES)	Falta de capacitación en el uso de los aplicativos
	Falta de revocación de los derechos de acceso al activo de información una vez el funcionario cambie de rol o se retire de la organización
	Inadecuado control de acceso lógico y/o físico a los activos de información
	Carencia de procedimientos adecuados de reutilización de medios y computadores
	Contratos Vencidos o Falta de Contratos con Soportes
	Demoras en la asignación de presupuesto para operación y mantenimiento de TI, y dificultad para su ejecución
	Desactualización del Antivirus
	Desactualización de los Gestores de Base de Datos
	Desconocimiento / Falta de Capacitación
	Equipos de cómputo desatendidos
	Errores en la Asignación de Permisos
	Falta de Planes de Recuperación
	Falta Consideraciones de la seguridad en los acuerdos con terceras partes
	Falta de Aplicación de buenas prácticas en la configuración de aplicación
	Falta de capacitación a los usuarios en el manejo de aplicaciones
	Falta de capacitación en el uso de los aplicativos
	Falta de capacitación en Seguridad de la Información
	Falta de capacitación para las funciones asignadas
	Falta de conciencia respecto a la seguridad de la información
	Falta de control con el uso de dispositivos de almacenamiento externos
	Falta de controles contra código malicioso
	Falta de controles de acceso a la información
	Falta de definición de Procedimientos para el Almacenamiento y comprobación de las Copias de seguridad
	Falta de definición y ejecución de Procedimientos de mantenimiento
	Falta de documentación de los servicios y/o aplicaciones
	Falta de estándares de desarrollo de aplicaciones
	Falta de Estrategias de Escalabilidad
	Falta de mantenimiento
	Falta de políticas / normas / procedimientos de seguridad de la información
	Falta de políticas de Actualización
	Falta de políticas de clasificación de la información
	Falta de políticas de seguridad
	Falta de Políticas de Transmisión de Documentos
	Falta de políticas para el manejo de Contraseñas
	Falta de Políticas para el Tratamiento de la Información
	Falta de Políticas Para el Uso de Dispositivos de Almacenamiento Externos
	Falta de Políticas Para Inactivación de Usuarios
	Falta de políticas que rijan el uso de los activos de información
	Falta de Procedimientos para el tratamiento de la información
	Falta de protección contra virus y código malicioso

	Falta de segregación de las funciones
	Falta de Sensibilización en Seguridad de la Información
	Falta de soporte
	Falta de mecanismos de monitorización de la red.
	Inadecuada clasificación de activos de información
	Inadecuada prevención y detección de incendios
	Inadecuado control de acceso lógico y/o físico a los activos de información
	Inexistencia de respaldo y/o custodia de los activos de información. (iniciativa de los usuarios)
	No Existencia de Políticas para el Tratamiento de la Información
	No existencia de un proceso de gestión de incidentes
	Procedimientos para el manejo de la información
	Sistemas Operativos Antiguos que Presentan Fallas Conocidas
	Usuarios por Defecto en las Configuraciones.
	Versiones de los motores de bases de datos desactualizados

Tabla 1.4 AMENAZAS ¿Cómo se materializa el riesgo pérdida de confidencialidad, integridad y disponibilidad?

RIESGOS	Pérdida de Confidencialidad	Pérdida de Integridad	Pérdida de Disponibilidad
AMENAZAS ¿CÓMO SE PUEDE MATERIALIZAR EL RIESGO?	Acceso no Autorizado al sistema	Introducción de Información Incorrecta	Falla en el Software-Aplicación
	Accesos no autorizados a las bases de datos	Abuso de Privilegios de Acceso	Almacenamiento Inapropiado de la Información
	Accesos no Autorizados a las Instalaciones	Accesos no Autorizados a los Aplicativos	Congestión en la Red de Datos
	Accesos no autorizados a los Aplicativos o Sistemas de Información	Alteración de la Información	Daños de Componentes de Red (Hardware, Equipos Activos de Red)
	Desactualización de servicios o aplicaciones	Destrucción de Información	Destrucción de información
	Divulgación de Información	Errores de Mantenimiento / Actualización de Programas	Falla en el Cableado
	Errores Humanos	Errores Humanos	Falla en el Software-Base de Datos
	Escapes de Información	Manipulación de la Configuración	Falla en el Software-Sistema Operativo
	Personal Insatisfecho	Personal Insatisfecho	Falla en el suministro de Energía
	Técnicas de hacking	Sabotaje Interno	Falla en Equipos de Respaldo / Back up
	Tratamiento Inadecuado de la Información	Soborno	Falla en servicios HVAC (Aire Acondicionado, Ventilación, etc.
		Suplantación de la Identidad del Usuario	Falla en UPS
			Incendio
			Inundación
			Robo de la Información
			Temblor
			Terremoto
			Tormenta Eléctrica
			Vandalismo

Tabla 2. EFECTOS POTENCIALES

N°	EFECTOS	DESCRIPCIÓN
1	Pérdida de imagen / credibilidad / confianza/ clientes, usuarios insatisfechos	Disminución de la percepción favorable que tiene la ciudadanía, los funcionarios y la comunidad internacional acerca de la institución.
2	Afectación a la Seguridad y Salud Ocupacional	Daños que pueden presentarse en la integridad física y mental de las personas, generando lesión o muerte.
3	Pérdidas Económicas	Detrimento del patrimonio público. Se expresa en términos de salarios mínimos mensuales legales vigentes.
4	Afectación Ambiental	Impactos causados al medio ambiente como resultados de las acciones realizadas.
5	Afectación a los objetivos estratégicos de la Institución	No se alcanzan las metas estratégicas planificadas por la Institución.
6	Afectación al bienestar / motivación del personal	Afectación a los niveles de motivación de los funcionarios de la Institución.
7	Interrupción de la Prestación del Servicio	Imposibilidad de continuar con la prestación del servicio.

Nota: La información referenciada en la anterior tabla, es de carácter general, toda vez que los efectos y/o impactos, se encuentran de manera específica en la "Matriz de valoración de Riesgos" (véase numeral 6.2.1.4).

5. FASE IDENTIFICACIÓN / ACTUALIZACIÓN DE RIESGOS

5.1. OBJETIVO DE LA FASE

El objetivo de esta fase es la identificación de los riesgos que pueden llegar a afectar la adecuada gestión tanto de los procesos como de la Institución. La identificación comprende las actividades para encontrar, reconocer y describir el riesgo. Es decir, identificar un riesgo significa que se identificarán las fuentes que pueden generarlo (clase de factor y agente generador), las causas, las situaciones como se puede materializar y los efectos potenciales que podrían darse si el riesgo se materializa.

De la calidad del trabajo de identificación, depende la adecuada priorización de todos los riesgos de la Institución y se definen planes de tratamiento adecuados que agreguen valor a su gestión.

5.2. DESCRIPCIÓN DE ACTIVIDADES

Los riesgos (y su descripción) en la Policía Nacional se identifican y/o actualizan en tres (3) momentos, con base en las siguientes fuentes:

SUBFASES DE IDENTIFICACIÓN / ACTUALIZACIÓN DE RIESGOS

N°	FUENTE	CUÁNDO
1	Riesgos inherentes a las actividades del proceso.	Una sola vez, cuando se inicie la implementación de la presente metodología (Aplicando el Plan de Identificación Inicial).
2	Resultados de desempeño de los procesos.	Trimestralmente, con los resultados del informe trimestral de gestión de riesgos.
3	Análisis del contexto, resultado fase de cierre, planes, proyectos y programas.	Anualmente, con el informe de cierre, el análisis de contexto y la descripción de los planes, proyectos y programas a ejecutar en el año siguiente.

5.2.1. Riesgos Inherentes a las Actividades del Proceso

Las actividades para realizar la identificación (y descripción) de estos riesgos se describen en el "Plan Inicial de Identificación" (Numeral 4 de este Manual).

5.2.2. Actualización de Riesgos con base en el desempeño del proceso

Se hace referencia a los riesgos que no se habían identificado en el plan inicial, o riesgos a los cuales faltó identificarles causas, situaciones que se registran en el Informe Trimestral "Resultados de la Gestión Integral del Riesgo" (Fase Medición de Resultados de la Gestión). De este informe, se debe analizar lo siguiente:

1. Aquellos casos que en el campo de "Causa generadora asociada al riesgo" para los eventos a evaluar, la respuesta haya sido: "El riesgo no se había identificado": En este caso, deberá agregarse el riesgo al formato o formulario de Identificación y diligenciar todos los campos requeridos en el formato o formulario de acuerdo con las instrucciones antes dadas en el "Plan Inicial de Identificación".

2. Aquellos casos que en el campo de "Causa generadora asociada al riesgo" para los eventos a evaluar, la respuesta haya sido: "el riesgo ha sido identificado pero no la causa": Deberá agregarse la causa al formato o formulario de identificación.

5.2.3. Actualización de riesgos con base en el análisis de contexto, en los resultados de la fase de cierre y en los planes, proyectos y programas a desarrollar en el año.

La identificación / actualización de riesgos, causas y efectos asociados al contexto, a los planes, proyectos y programas, y a los resultados de la fase de cierre, se hará anualmente. Se deberá hacer la "Reunión anual de revisión de riesgos", reunión en la que debe participar un número representativo de los funcionarios del proceso. El objetivo es que en la reunión se revisen los riesgos que el proceso ya había identificado, los planes, proyectos y programas, y se haga el análisis de contexto, con el fin de identificar nuevos riesgos, causas o efectos.

Esta reunión deberá llevarse a cabo dentro de los primeros 15 (quince) días calendario del mes de noviembre de cada año.

Las responsabilidades del gestor de riesgos son; preparar, moderar, y consolidar los resultados de la reunión.

5.2.3.1. Preparar la Reunión

El éxito de la reunión estará dado por la calidad de la información con la que se cuente en el momento de realizarla, dada esta condición, el gestor de riesgos deberá asignar las responsabilidades de recolección y análisis de la información requerida entre los funcionarios del proceso. La citación a la reunión debe ser enviada a los funcionarios del proceso mínimo, con 5 (cinco) días hábiles de anticipación, a la fecha de la reunión.

Cada funcionario presentará la información que le fue asignada, y los asistentes, con base en su conocimiento y experiencia del proceso tendrán la responsabilidad de aportar a la reunión con el fin de poder actualizar los riesgos identificados y su situación.

A continuación se describe la información que debe ser preparada por los funcionarios para presentar en la reunión:

- **Presentación de Identificación del Proceso**

Con base en la caracterización del proceso, se deberá hacer la presentación y explicar a los asistentes la siguiente información con el fin de contextualizarlos:

- Nombre del Proceso.
- Dependencia o dependencias que participan en el proceso.
- Nivel.
- Objetivo del Proceso en el nivel.
- Cuál es la evidencia del cumplimiento del objetivo del proceso. (Ejemplo: Proceso de Control Interno: informes de auditorías).
- Cliente del proceso (que puede ser interno / externo).

- **Revisión de Riesgos Inherentes al Proceso**

En el caso de cambios en el objetivo del proceso, indicadores, creación, modificación o eliminación de procedimientos, será necesario revisar los riesgos ya identificados, con el fin de determinar si requieren ajustes. De ser necesarios, estos deberán seguir las mismas directrices dadas en el Plan de Identificación inicial. El gestor de riesgos será el responsable de presentar en la reunión, las modificaciones en los riesgos por cambio en el objetivo o en los indicadores y designará quien presentará las modificaciones en los riesgos por cambios en los procedimientos.

- **Revisión del Informe Anualizado o Trimestral de los Resultados de la Gestión de Riesgos (Ver Fase de Cierre)**

El gestor de riesgos presentará el informe anual de gestión de riesgos del proceso a los asistentes.

- **Análisis de Riesgos en Planes, Proyectos y Programas**

Se deberán revisar los planes, proyectos y programas, que el proceso y/o Institución vaya a llevar a cabo durante el año siguiente e identificar los riesgos asociados a las actividades de cada uno de ellos.

Dentro de estos planes, proyectos y programas, se deben considerar, proyectos de inversión y de ciencia y tecnología, entre otros, que se vayan a llevar a cabo para apoyar el cumplimiento de los objetivos estratégicos, etc.

Con el fin de poder medir si los proyectos alcanzan los resultados esperados, es recomendable que cada uno de ellos cuente con mecanismos de seguimiento y/o medición que permitan controlar al menos los aspectos de tiempo y costo.

5.2.3.2. Moderar la Reunión

El objetivo de la reunión es revisar y actualizar los eventos potenciales que pueden poner en riesgo la adecuada gestión tanto de los procesos como de la Institución, lo cual se hará mediante el análisis de la información presentada descrita en el punto anterior.

Con base en la información descrita en el numeral 5.3.3.1., el conocimiento del proceso que tiene cada uno de los asistentes, y con la orientación del gestor de riesgos, se deberán ir identificando en la reunión las debilidades, oportunidades, fortalezas y amenazas del proceso.

La idea es que al ir presentando cada uno de los puntos descritos, se vayan identificando las debilidades, oportunidades, fortalezas y amenazas. Una vez se haya diligenciado el formato o formulario, deberán tomarse las debilidades y amenazas y verificar si ya se habían contemplado como causas o como riesgos en los que ya se habían identificado, sino, se deberán incluir afectando el riesgo que corresponda.

5.2.3.3. Consolidar los resultados de la Reunión

Los resultados de la reunión deberán ser consolidados por el gestor de riesgos en los siguientes documentos:

Análisis de Contexto, Formato o formulario Descripción de Riesgos.

5.2.4. Actualización Mapa de Riesgos Institucional

La actualización de los riesgos institucionales se llevará a cabo por parte de la Oficina de Planeación de acuerdo a los comportamientos presentados por los mismos y la lectura que sobre cada uno de ellos se haga a partir de los resultados de la gestión del riesgo tanto trimestral como anual. Igualmente corresponde a los dueños de proceso de primer nivel participar en dicha actualización, (según asignación del riesgo), para lo cual podrán incorporarse modificaciones en la descripción del riesgo (factores, agentes generadores, causas, situaciones de materialización, controles), previa revisión y aprobación de la Oficina de Planeación.

Una vez el Subcomité apruebe los riesgos institucionales, los funcionarios de Planeación liderarán el trabajo de descripción del riesgo con cada uno de los procesos que deban trabajarlo.

Para determinar los riesgos institucionales del año siguiente, al inicio de la implementación de la presente metodología, se tendrá en cuenta lo siguiente:

Para la determinación de los riesgos institucionales posteriores, se tendrá en cuenta lo siguiente:

a. Los riesgos institucionales identificados en el periodo anterior.
b. Los que como resultado de la evaluación de todos los riesgos de la Institución hayan quedado ubicados en las zonas más altas de riesgo.
c. Aquellos que afecten directamente el cumplimiento de la misión institucional y los objetivos estratégicos.

Los funcionarios de la Oficina de Planeación serán los responsables de liderar la actualización de la identificación de estos riesgos, liderar / coordinar el análisis antes y después de controles, de hacer seguimiento a la ejecución de los planes de tratamiento y de rendir los informes requeridos al respecto.

Nota 1: Esta actualizaciones no requieren ser sometidas a Subcomité Central de Mejoramiento Gerencial, a menos que las modificaciones a la descripción inicial del riesgo se han sustanciales e impliquen y/o ameriten la aprobación del Mando Institucional.

Nota 2: Cualquier cambio o modificación a un riesgo institucional, en alguno de sus apartes (factor de riesgo, agente generador, causa, riesgo, descripción, situaciones de materialización, control detectivo, efecto, control para detectarlo, al igual que los planes de tratamiento), necesariamente deben surtir trámite ante la Oficina de Planeación para su respectiva aprobación metodológica, cuando dichos cambios y modificaciones sean propuestos por las direcciones y/o oficinas asesoras que tengan un riesgo asignado por el señor Director General y/o Subdirector General.

Nota 3: Para el caso del riesgo institucional de corrupción, la actualización del mismo debe cumplir el precepto de la nota anterior.

5.3. RESPONSABILIDADES POR CARGOS / NIVELES

Gestores de Riesgos en los tres niveles:

Preparar, moderar y consolidar los resultados de la reunión en los formatos o formularios, Análisis de Contexto e Identificación de Riesgos.

Funcionarios del Proceso:

Preparar la información que les sea asignada por el gestor de riesgos y presentarla en la reunión anual de Revisión de Riesgos.

Participar activamente en la reunión con el fin de ayudar a identificar las debilidades, oportunidades, fortalezas y amenazas del proceso.

Jefes, Directores y Comandantes:

Facilitar el desempeño de las actividades relacionadas con el riesgo tanto del gestor de riesgos, como de los funcionarios que tiene a cargo, mediante la asignación de tiempo suficiente para la ejecución de las actividades.

Como funcionario del proceso, participar activamente en las reuniones que se hagan, aportando su visión gerencial al ejercicio.
Nota: En los procesos de primer y segundo nivel (y despliegues de segundo nivel), las reuniones se harán por proceso. En los procesos de tercer nivel (y despliegues), con el fin de optimizar el tiempo y facilitar la asistencia y participación activa de todos los funcionarios estas reuniones se podrán hacer por unidad; en este caso, el gestor de riesgos, deberá tener especial cuidado para separar la información por proceso y así poderla enviar al gestor de riesgos de segundo nivel que corresponda.

Gestores de Riesgos de segundo nivel:

Consolidar por proceso, la información enviada por los gestores de tercer nivel. Revisar, retroalimentar y aclarar la información que reciban y enviarla a los gestores de primer nivel.

Gestores de Riesgos de primer nivel:

Consolidar por proceso, la información enviada por los gestores de segundo nivel. Revisar, retroalimentar y aclarar la información que reciban y enviarla a los funcionarios de la Oficina de Planeación.

Funcionarios de la Oficina de Planeación:

Deben recibir la información enviada por los gestores de primer nivel, para conjuntamente con los gestores, revisarla, retroalimentar y aclarar cualquier aspecto que lo requiera. Una vez la información haya surtido este proceso y los funcionarios de planeación le den su aprobación, se formalizaran los riesgos identificados y se podrá dar continuidad a las fases que siguen en la metodología.

6. FASE DEFINICIÓN DE LA GESTIÓN

6.1. OBJETIVO DE LA FASE

El objetivo de esta fase es definir las acciones que permitirán dar tratamiento adecuado a los riesgos identificados de forma que:

a) Prevengan la materialización de los riesgos, mediante el tratamiento de las causas raíces de los riesgos potenciales, de una manera integral y consolidada.

b) Se determinen acciones que permitan mitigar los efectos de los riesgos materializados y restablecer el curso normal de las actividades en el menor tiempo posible, cuando la prestación del servicio se vea afectada.

c) Se determinen los costos asociados a la implementación de las actividades con el fin de planificar las necesidades de recursos y posteriormente de controlarlos.

d) Determinar las acciones para detectar las "situaciones de materialización", "efectos" y "amenazas" del riesgo identificado en su ocurrencia.

6.2. DESCRIPCIÓN DE ACTIVIDADES

6.2.1. Diligenciar Formato o formularios de Análisis antes de Controles y Valoración de Controles.

Una vez la Oficina de Planeación haya aprobado la Descripción de Riesgos, los gestores de riesgos de cada nivel, deberán diligenciar los formatos o formularios de análisis y valoración de controles para los riesgos de su nivel y con su grupo de trabajo (el mismo del Plan Inicial).

6.2.1.1. Frecuencia

Para cada una de las posibles situaciones de materialización, clasificar cualitativamente la frecuencia de ocurrencia histórica de cada situación en el año inmediatamente anterior, en términos de:

5	Ha ocurrido siempre (si se selecciona este ítem, las situaciones de materialización se están calificando sin controles, lo que para el caso es correcto).
4	Ha ocurrido frecuentemente (si se selecciona este ítem, las situaciones de materialización se están calificando sin controles, lo que para el caso es correcto.
3	Ha ocurrido moderadamente (si selecciona este ítem, evidenciar registros y por qué se logró esa estadística. Se debe poder demostrar que la situación de materialización ocurre en la cantidad de veces de acuerdo a lo consultado, sin controles existentes).
2	Ha ocurrido ocasionalmente (si selecciona este ítem, evidenciar registros y por qué se logró esa estadística. Se debe poder demostrar que la situación de materialización, ocurre en la cantidad de veces de acuerdo a lo consultado, sin controles existentes).
1	Nunca ha ocurrido (si selecciona este ítem, evidenciar registros y por qué se logró esa estadística. Se debe poder demostrar que la situación de materialización ocurre en el número de veces indicado; ósea cero, sin controles existentes).

Nota: Se debe tener en cuenta que para realizar este análisis, es necesario desprender o quitar de la frecuencia presentada, los controles preventivos y/o correctivos, toda vez que muy probablemente la ocurrencia de la frecuencia histórica, se tomó a partir de resultados con controles aplicados. Recordemos que esta actividad se hace sin controles existentes, ósea en el contexto de un escenario caótico, por lo tanto se debe calificar la frecuencia como mínimo en 4.

6.2.1.2. Exposición

Para cada riesgo, teniendo en cuenta los factores tanto internos como externos del mismo, determinar cuál es su factibilidad en términos de:

5	Constante exposición
4	Frecuente exposición
3	Moderada exposición
2	Ocasional exposición
1	Muy rara exposición

Nota 1: Para determinar la exposición se debe tener en cuenta la frecuencia de realización de la actividad que genera el riesgo. Ejemplo.: Es más factible que ocurra un accidente aéreo para una persona que vuela todos los días que para una persona que vuela 5 veces al año, el que vuela todos los días está más expuesto al riesgo.

Nota 2: Recordemos que la Probabilidad, se da en términos de frecuencia – exposición, y que está se reflejará en la Matriz de Valoración del Riesgo, de acuerdo a la configuración de la fórmula en el aplicativo.

6.2.1.3. Impacto

Para cada uno de los efectos del riesgo (de la fase de identificación), indicar cuál es el máximo nivel de impacto que podría producir en caso de materialización. Esta actividad se debe hacer con base en la Matriz de Valoración del Riesgo, tal como se muestra en la siguiente figura.

Nota: Aplicar para la calificación del impacto el criterio dado en la nota del numeral 6.2.1.1.

Posteriormente se deberán diligenciar los formatos o formularios de valoración de controles correctivos y preventivos (existentes).

6.2.1.4. Controles Existentes

Para cada una de las causas y efectos de cada riesgo, relacionar qué controles existen. En este sentido, los procesos de nivel 1 y 2, deben estandarizar los controles preventivos, correctivos y/o detectivos para su inserción y valoración en el aplicativo.

Nota 1: No son válidos como controles existentes: actas, correos, comunicaciones oficiales, informes, entre otros.

Nota 2: Son válidos como controles existentes: Procedimientos, Instructivos, Directivas, Guías, Manuales, Resoluciones, y los que posteriormente resulten de los planes de tratamiento para cualquier riesgo antes de que estos se materialicen estando previamente identificados.

Nota 3: Las Leyes, Políticas, Lineamientos, Aplicativos, Planes (por ejemplo, Corazón Verde), por si solos no son controles existentes, y por lo tanto se debe relacionar exactamente qué parte de estos obra como control para la causa, impacto o situación de materialización.

Nota 4: Las unidades de nivel 3, pueden sugerir controles existentes a su proceso inmediatamente superior, con el fin se evalúen para inclusión en la estandarización de los mismos. Respecto a los controles para la seguridad de la información, estos deben ser tomados a partir de los que relacione en este sentido la norma.

MATRIZ DE VALORACIÓN DEL RIESGO

MATRIZ DE CALIFICACIÓN Y VALORACION DEL RIESGO (MVR / RAM)

IMPACTO							PROBABILIDAD					UBICACIÓN	OPCIÓN
Pérdida de Imagen, credibilidad, confianza, clientes / usuarios insatisfechos	Afectación a la Seguridad y Salud en el Trabajo (OSHAS18001)	Pérdidas Económicas (En S.M.M.L.V.)	Daño Ambiental (ISO14001)	Afectación a los objetivos estratégicos de la Institución	Afectación al bienestar / motivación del personal	Interrupción de la prestacion del servicio (GTC 176)	1	2	3	4	5	ZONA DE RIESGO BAJO ACEPTABLE	Asumir el riesgo
Hechos o noticias que afectan la imagen a nivel Unidades de Policia	Lesiones o enfermedades que no requieren incapacidad.	0-500	*Poca o nula afectación al medio ambiente. *Posibilita una recuperación inmediata de las condiciones originales tras el cese de la acción. *Afecta únicamente el área de trabajo.	Menos del 20% de los objetivos estratégicos	Afectacion a un funcionario	Interrupción de la prestacion del servicio hasta 2 horas.	1 (0.0-1)	(1.1 - 2)	(2.1-3)	(3.1-4)	(4.1-5)	ZONA DE RIESGO MEDIO	Asumir y Reducir el riesgo
Hechos o noticias que afectan la imagen a nivel Todos los funcionarios	Lesión o enfermedad que requiere de un tratamiento médico ambulatorio y que genere incapacidad laboral temporal (ILT)	501-1000	*Baja alteración en el medio ambiente. *Posibilita una pronta recuperación de las condiciones originales tras el cese de la acción. *La afectación sale del área de trabajo pero se mantiene en áreas bajo el control institucional.	Entre el 21% y el 40% de los objetivos estratégicos	Afectacion a una unidad	Interrupción de la prestacion del servicio hasta 6 horas.	2 (1.1.-2)	(2.1-4)	(4.1-6)	(4.1-8)	(8.1-10)	ZONA DE RIESGO ALTO	Evitar, Reducir, Compartir o Transferir el riesgo
Hechos o noticias que afectan la imagen a nivel Ciudad	Lesión o enfermedad que requiere de un tratamiento médico ambulatorio y que genere incapacidad laboral temporal (ILT) por más de 30 días, pero menos de 90	1001-1500	*Media alteración en el medio ambiente. *Posibilita una recuperación en el mediano plazo de las condiciones originales tras el cese de la acción. *Afecta levemente a terceros.	Entre el 41% y el 60% de los objetivos estratégicos	Afectacion a los funcionarios de una region.	Interrupción de la prestacion del servicio hasta 12 horas.	3 (2.1-3)	(4.1-6)	(6.1-9)	(8.1-12)	(10.1-15)		
Hechos o noticias que afectan la imagen a nivel País	Lesión o enfermedad grave irreparable (Incapacidad permanente parcial o invalidez).	1501-2000	*Alta alteración en el medio ambiente. *Recuperación solo en el largo plazo de las condiciones originales tras el cese de la acción. *Afecta en mayor grado a terceros. La afectación es a nivel local.	Entre el 61% y 80% de los objetivos estratégicos	Afectacion a los funcionarios de mas de una region, pero no toda la Institucion.	Interrupción de la prestacion del servicio hasta 18 horas.	4 (3.1-4)	(6.1-8)	(9.1-12)	(12.1-16)	(15.1-20)		
Hechos o noticias que afectan la imagen a nivel Internacional	Muerte, lesión o enfermedad que implique a largo plazo una limitación total y permanente.	Más de 2000	*Grave afectación al medio ambiente. *Pérdida permanente en la calidad de las condiciones y recursos ambientales sin posibilidades de recuperación. *Afecta gravemente a terceros. La afectación es a nivel regional.	Entre el 81% y 100% de los objetivos estratégicos	Afectacion de todos los funcionarios de la Institucion.	Interrupción de la prestacion del servicio por 24 horas o más.	5 (4.1-5)	(8.1-10)	(12.1-15)	(16.1-20)	(20.1-25)		

Existen controles de tipo preventivo y correctivo:

TIPOS DE CONTROL	DESCRIPCIÓN
Preventivos	Disminuyen la probabilidad de ocurrencia del riesgo, actuando para eliminar las causas del riesgo, con el fin de prevenir su materialización. Ejemplos: Registro a vehículo o a personas, avisos informativos (Peligro, Alta Tensión, Solo Personal Autorizado), un contrato, sistemas de claves de acceso, validaciones de datos ingresados a los sistemas de información, seguridad física como cerraduras, puertas.
Correctivos	Permiten disminuir el impacto causado por el riesgo materializado. Ejemplos: Una póliza, porque permite disminuir el impacto de una pérdida económica; Un procedimiento para atención de público cuando no hay sistema de información (plan de contingencia), porque permite disminuir el impacto de pérdida de imagen/clientes o usuarios insatisfechos, actividades de back up, porque dependiendo de la clase de información que estén respaldando podrían disminuir el impacto de la interrupción del servicio, o de clientes insatisfechos, etc.

Existe un tercer tipo de controles y es importante tener claridad de su existencia para no confundirlos con los preventivos ni con los correctivos, estos son los controles detectivos:

TIPO DE CONTROL	DESCRIPCIÓN
Detectivos	Son aquellos que no evitan la ocurrencia del riesgo, sino que los detecta cuando ocurren. Como herramienta, permiten medir la efectividad de los controles preventivos. Hay controles que permiten detectar la materialización del riesgo y otros que permiten detectar su efecto. Ejemplos de controles que permiten detectar un riesgo materializado: revisión de inventarios, sistemas de monitoreo, cámaras de vigilancia, cruce de bases de datos, auditorias, etc. Ejemplos de controles que permiten detectar un efecto: quejas, reclamos, multas, demandas noticias en medios, encuestas de satisfacción, etc.

Posteriormente, se deberán valorar los controles correctivos y preventivos respondiendo las siguientes preguntas, ("Si" en caso afirmativo o "No" en caso negativo).

Controles preventivos: (Disminuyen la probabilidad de ocurrencia de los riesgos al enfocarse en tratar las causas).

- ¿Se aplica el control?: ¿Se realizan las actividades descritas en el control?
- ¿Está documentado el control?: Existe un documento que describa las acciones del control?
- ¿Es efectivo?: Un control es efectivo si el riesgo no se ha materializado por la causa relacionada con el control.
- ¿Están definidos los responsables de la ejecución del control?
- ¿La frecuencia de ejecución del control es adecuada?

Controles correctivos (disminuyen el impacto de los efectos al materializarse un riesgo):

- ¿Está documentado el control?: Existe un documento que describa las acciones del control?
- ¿Están definidos los responsables de su ejecución?
- ¿Hay evidencia de socialización / capacitación a los responsables de la ejecución?

En cualquiera de los dos casos, si no hay controles, escribir "No Hay".

La evaluación del riesgo es el producto de confrontar los resultados de la calificación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo.

6.2.2. Consolidar, revisar y ajustar

Los gestores de riesgos de nivel 2 deberán consolidar, revisar y analizar los formatos o formularios diligenciados por los gestores de nivel 3 de su mismo proceso, con el fin de generar un solo formato o formulario de "Análisis antes de Controles" y uno solo de "Valoración de Controles" para el proceso en el nivel 3. Para realizar esta actividad se debe tener en cuenta que no haya información duplicada (los mismos controles para una causa), pero se considere toda la información enviada por los gestores de nivel 3. Los gestores de riesgo de nivel 1 deberán consolidar el trabajo de los gestores de nivel 2 (Análisis y Valoración del proceso y el consolidado del nivel 3).

Toda la información que se produzca a partir de la aplicación de cada una de las fases de la metodología del riesgo, deberá ser cargada a la herramienta tecnológica que se utilice para tal fin, donde se aprobará o desaprobará cada una de las misma, de acuerdo al cumplimiento en términos de coherencia, suficiencia, pertinencia, conveniencia y adecuación de la información.

6.2.3. Revisar, analizar y retroalimentar

Los funcionarios de la Oficina de Planeación deberán analizar la información enviada teniendo en cuenta lo siguiente:

Riesgos comunes, causas con mayor participación en el consolidado general, causas sin controles, causas con exceso de controles (para revisar efectividad), efectos sin controles, las opciones de manejo resultantes para cada riesgo en el formato o formulario de análisis después de controles, e identificación de los riesgos institucionales.

En el contexto de esta resolución, entiéndase plan, proyecto y programa como "plan de tratamiento de riesgos".

6.2.4. Diligenciar Formato o formulario Plan de Tratamiento

Cada gestor de riesgos de nivel 1 deberá diligenciar el formato o formulario de Plan de Tratamiento de acuerdo con sus necesidades; para hacerlo deberá tener en cuenta lo siguiente:

Las opciones de tratamiento de acuerdo con la ubicación del riesgo después de controles, dentro de la Matriz de Valoración del Riesgo (Matriz RAM).

ZONA DE RIESGO	QUÉ SE REQUIERE
Alto	Es obligatorio tomar acciones sobre las actividades que generan riesgo.
Medio	Se deberán definir las opciones de tratamiento teniendo en cuenta: a. Presupuesto disponible después del tratamiento a los riesgos de la Zona Alta. b. Disponibilidad de recursos físicos.
Bajo	Si no hay excedente de recursos (económicos, humanos, de infraestructura) no es necesario tomar acciones.
OPCIONES DE TRATAMIENTO	**DESCRIPCIÓN**
Evitar	Dejar de realizar la actividad que genera riesgo y/o no emprender nuevas iniciativas que generen riesgo. Intervención urgente.
Reducir	Establecer límites en cuanto a resultados, mejorar los procesos mediante la definición de planes de tratamiento para generar o fortalecer controles preventivos y/o correctivos. Corregir y adoptar medidas de control de inmediato.
Compartir/Transferir	Hacer convenios o alianzas para la realización de actividades que pueden generar riesgos, externalizar la realización de estas actividades, adoptar seguros contra pérdidas inesperadas, distribuir el riesgo mediante acuerdos contractuales con proveedores u otras entidades.
Aceptar / Asumir	Provisionar las posibles pérdidas, definir planes de contingencia cuando aplique. Mantener las medidas de control existentes, considerar posibles mejoras y verificar en periodos de tiempo determinados si el riesgo continúa en zona baja.

- Dentro del plan de tratamiento se deben definir acciones que permitan tratar aquellas causas generadoras de los riesgos, para las cuales no se identificaron controles, o la valoración de los mismos dio un resultado bajo. En este caso dentro del plan de tratamiento se considerará tomar medidas para fortalecer el control o eliminarlo si no se puede mejorar.
- Se deberán tener en cuenta las fortalezas y oportunidades identificadas en la reunión anual de identificación de riesgos (DOFA) para proponer acciones que permitan dar tratamiento a los riesgos.
- Un plan de tratamiento de riesgos podría ser considerado un proyecto y programa, cuyo fin es, crear controles que permitan disminuir la probabilidad de ocurrencia de uno o varios riesgos, o que permitan disminuir el impacto de los efectos en caso de materialización del riesgo.
- Las actividades descritas dentro de un plan de tratamiento podrán requerir la participación de diferentes funcionarios dentro del proceso, en diferentes niveles, o incluso de diferentes procesos.
- El gestor de riesgos de nivel 1 podrá coordinar reuniones con quien/es considere necesario para la formulación del plan de tratamiento. La participación de Jefes, Directores y Comandantes es obligatoria, si no en la definición del plan, sí en la revisión del mismo; el formato o formulario tiene los siguientes campos:

Nombre del Plan: Se deberá determinar un nombre para el plan, este nombre debe dar una idea general del alcance del mismo.

Líder del Plan: Se debe escribir el nombre y cargo del responsable del plan; su deber es velar porque se alcancen los objetivos y por lo tanto debe ser seleccionado teniendo en cuenta el alcance y la magnitud del plan. Una vez esté nombrado, el líder del Plan podrá solicitar a la Oficina de Planeación hacer los ajustes que considere pertinentes a cualquier campo del Formato o formulario de Plan de Riesgos (con las respectivas justificaciones).

Esta persona debe concentrarse en los objetivos específicos del plan de tratamiento, controlar los recursos asignados, controlar las variables de tiempo (cumplimiento del cronograma), costo (control del presupuesto asignado), calidad (que los entregables cumplan con las características de calidad esperadas) y alcance (trabajo que debe realizarse para entregar un producto, servicio o resultado con las características y funciones especificadas).

Descripción de la actividad: Se debe relacionar la actividad a ejecutar, debe ser una actividad puntual, que no se esté ejecutando en el momento.

Responsable: Cargo de la persona responsable de la ejecución de la actividad. No el responsable del proceso.

Entregable: Registro que da evidencia de la realización de la actividad planteada. Ejemplo: procedimiento, informe de diagnóstico, acta de capacitación, etc.

Fecha Inicio Actividad: Fecha (día /mes/ año) en la que se dará inicio a la actividad planteada.

Fecha Fin Actividad: Fecha (día /mes/ año) en la que se dará fin a la actividad planteada. Las fechas de inicio y fin indican cuando se iniciará y terminará de ejecutar la acción. Ni en fecha inicio, ni en fecha fin pueden escribirse términos como: mensual, constante, semestral, cuando se requiera, indefinido, etc.

Valor Proyectado de la Actividad o Valor Planificado (PV): En el formato o formulario de "Estimación de Costos" se deberán estimar los recursos necesarios para completar cada actividad del plan teniendo en cuenta las siguientes categorías:

- **Personal:** Costo del tiempo del personal que llevará a cabo la actividad. (Tiempo en horas hombre por salario).
- **Materiales:** Costo de los materiales que requiera la realización de una actividad específica. Ejemplo: libros, material de publicidad, etc.
- **Equipo:** Costo de la maquinaria requerida para la realización de una actividad (compra).
- **Servicios:** Costo de los servicios requeridos para completar la actividad.
- **Ejemplo:** servicios de publicidad, servicios de arrendamiento de maquinaria o de vehículos, asesorías, etc.
- **Instalaciones:** Costo del uso de las instalaciones en las cuales se realiza la actividad.
- **Licencias, permisos, autorizaciones:** Costo de las licencias permisos y/o autorizaciones que se requieran para la realización de la actividad descrita.

Para cada una de las categorías se debe diligenciar: nombre de recurso, costo unitario y cantidad.

Peso de la actividad: Debe darse un peso porcentual a cada actividad del plan, teniendo en cuenta la complejidad de la actividad.

Ejemplo:

ACTIVIDAD	PESO PORCENTUAL
Elaborar la lista de documentos a revisar para hacer el diagnóstico.	15%
Analizar documentos de la lista para documentar diagnóstico.	50%
Socializar documento de diagnóstico mediante el envío de correos electrónicos a todos los interesados (confirmar).	2%
Consolidación de comentarios para complementar el documento.	3%
Integración de comentarios pertinentes al documento.	30%
TOTAL	100%

En los casos en que una o más actividades tengan complejidad similar, el segundo criterio que permitirá determinar el peso porcentual de la actividad es el tiempo de realización de la actividad.

6.2.4.10. ¿El entregable constituye un control?: Si el entregable de la actividad es un control correctivo o preventivo, seleccione SI, de lo contrario, seleccione NO.

6.2.5. Socialización y Revisión Técnica de los Planes de Tratamiento

Una vez estén formulados los planes de tratamiento, cada "Líder de Plan" deberá socializarlos tanto con los gestores de su proceso en los demás niveles, como con todos los involucrados en el desarrollo de las actividades.
Deberán ponerse a disposición de todos por un periodo de 10 días hábiles con el fin de quien lo considere pertinente haga los comentarios, sugerencias, recomendaciones a que haya lugar. El gestor de riesgos de nivel 1 tiene 5 días hábiles, posterior a estos 10 días para que haga los ajustes pertinentes.

Una vez se hayan ajustado los planes (si hubo necesidad de ello), el gestor de nivel 1 deberá enviarlos a la Oficina de Planeación (Enviar Formato o formularios de: Plan de Tratamiento de Riesgos y Estimación de Costos y comentarios, sugerencias y observaciones que haya recibido). Los funcionarios de la Oficina de Planeación deberán revisar la formulación del plan y evaluarlo.

Dentro de la evaluación del plan se deberán tener en cuenta los siguientes aspectos:

- Que las actividades formuladas sean coherentes con las causas identificadas.
- Que las actividades planteadas estén relacionadas con los efectos del riesgo.
- Que las actividades formuladas sean claras e involucren un verbo en su redacción.
- Que el cargo responsable de la realización de la actividad sea quien efectivamente va a ejecutar la acción.
- Que el entregable o registro de cada actividad sea concreto y verificable.
- Que las fechas de inicio y fin sean apropiadas para la complejidad de la actividad.
- Que la estimación de costos se haya hecho adecuadamente.
- Que la suma de los porcentajes de cada actividad sume un 100 por ciento en el proyecto y que la asignación de porcentajes sea coherente con el criterio definido.
- Que los entregables que sean controles se identifiquen como tal.

6.2.6. Aprobación Final de los planes de tratamiento por el Subcomité de Mejoramiento Gerencial

Una vez los planes de tratamiento de los riesgos institucionales, masivos por proceso y/o individuales sean pre-aprobados, deben ser sometidos a revisión y aprobación por el Subcomité de Mejoramiento Gerencial, quien basará su respuesta y/o decisión validando los aspectos de:

a. Pertinencia de los planes para el cumplimiento de los objetivos de la institución.

b. Viabilidad Económica de los Planes.

c. Viabilidad Jurídica de los Planes.

d. Disponibilidad y pertinencia del líder del plan propuesto.

e. Disponibilidad del personal para la ejecución de las acciones.

Una vez el Subcomité de Mejoramiento Gerencial apruebe los planes, emitirá un documento expresando su aprobación y oficiando a los Jefes, Directores y Comandantes cuyo personal deba ejecutar acciones, que se requiere dar inicio a la ejecución de los planes.

Cada Oficina Asesora, Dirección o Unidad que tenga responsabilidad de realización de los planes de tratamiento, debe tener en cuenta lo establecido en el documento Guía Metodológica para la Formulación y Gestión de la Estrategia Institucional.

Si el Subcomité de Mejoramiento Gerencial no aprueba el plan, deberán hacerse los ajustes de acuerdo con las observaciones que se hagan, o si la decisión es no llevarlo a cabo, deberá documentarse en el acta de la reunión, los motivos que llevaron a dicha decisión.

Nota 1: Las unidades de tercer nivel solo están obligadas a elaborar planes de tratamiento de riesgos, cuando hayan identificado riesgos individuales y estén aprobados en la herramienta tecnologica utilizada.

Nota 2: Cuando se estructuren planes de tratamiento para la mitigación de riesgos de acuerdo a su clasificación y/o tipo, estos deben sistematizarse en el módulo "planes" de la herramienta tecnologica utilizada, teniendo en cuenta que no se cargue esta información como un "plan de acción", sino como lo inicialmente expuesto.

Nota 3: Los planes de tratamiento para la mitigación de los riesgos institucionales, masivos por procesos e individuales serán validados y aprobados por las siguientes instancias, así:

- *Plan de tratamiento institucional: Subcomité Central de Mejoramiento Gerencial.*
- *Plan de tratamiento masivo por proceso: Subcomité Regional de Mejoramiento Gerencial.*
- *Plan de tratamiento individual: Subcomité Regional o Local de Mejoramiento Gerencial.*

Nota 4: Los planes de tratamiento para la mitigación de los riesgos, tambien se pueden aprobar de acuerdo a lo establecido en la Nota del Parágrafo 1° del artículo 22 de este acto administrativo, siendo pertinente y necesario dejar los registros documentales de lo actuado.

Nota 5: Cuando los planes de tratamiento asociados a riesgos institucionales, masivos por procesos e individuales, hayan cumplido su finalidad, no es necesario u obligatorio implementar nuevas acciones, siempre y cuando se pueda demostrar que el control generado a partir de la ejecución del plan, está mitigando el riesgo en terminos de evitarlo y/o reducirlo.

Nota 6: Para el caso del "Plan de tratamiento del riesgo institucional de corrupción", este debe surtir trámite ante el Subcomité Central de Mejoramiento Gerencial, cuando se deba actualizar y/o ajustar, en atención a solicitud justificada y motivada por parte de las direcciones u oficinas asesoras responsables de cumplir el mencionado plan a través de las tareas establecidas.

6.3. RESPONSABILIDADES POR CARGOS / NIVELES

Gestores de Riesgo de los tres niveles:

Diligenciar los formatos o formularios de Análisis antes de Controles y Valoración de Controles para los riesgos de su proceso y de su nivel.

Gestores de Riesgo de Nivel 2:

Los gestores de riesgos de nivel 2 deberán consolidar, revisar y analizar los formatos o formularios diligenciados por los gestores de nivel 3 de su mismo proceso, con el fin de generar un solo formato o formulario de "Análisis antes de Controles" y uno solo de "Valoración de Controles" para el proceso en el nivel 3. Para realizar esta actividad se debe tener en cuenta que no haya información duplicada, pero se considera toda la información enviada por los gestores de nivel 3.

Los gestores de riesgo de nivel 1 deberán consolidar el trabajo de los gestores de nivel 2 (Análisis y Valoración del proceso y el consolidado del nivel 3).

Los gestores de riesgo de nivel 1 deberán enviar a la Oficina de Planeación la información consolidada por proceso de sus riesgos en los 3 niveles.

Cada gestor de riesgos de nivel 1 deberá diligenciar el formato o formulario de Plan de Tratamiento de Riesgos de acuerdo con sus necesidades; para hacerlo deberá tener en cuenta lo siguiente:

Líder del Plan: Se debe escribir el nombre y cargo del responsable del plan; su deber es velar porque se alcancen los objetivos y por lo tanto debe ser seleccionado teniendo en cuenta el alcance y la magnitud del mismo. Una vez este nombrado, el líder del Plan podrá solicitar a la Oficina de Planeación ajustes que considere pertinentes a cualquier campo del Formato o formulario de Plan de Tratamiento de Riesgos (con las respectivas justificaciones). Esta persona debe concentrarse en los objetivos específicos del proyecto, controlar los recursos asignados, controlar las variables de tiempo (cumplimiento del cronograma), costo (control del presupuesto asignado), calidad (que los entregables cumplan con las características de calidad esperadas) y alcance (trabajo que debe realizarse para entregar un producto, servicio o resultado con las características y funciones especificadas).

7. FASE GESTIÓN DE RIESGOS

7.1. OBJETIVO DE LA FASE

Esta fase de la metodología comprende la ejecución de los planes de tratamiento de riesgos y el control a la ejecución de las acciones de esos planes. El control a la ejecución incluye el registro de: cumplimiento de actividades planificadas y los costos incurridos, riesgos materializados, costos incurridos por riesgos materializados (correcciones, acciones correctivas, planes de contingencia). También deberá registrarse cualquier iniciativa que permita generar acciones preventivas que provengan de cualquier fuente: resultado de la evaluación de quejas, reclamos y sugerencias, análisis de satisfacción del cliente, resultados de revisión por la Dirección, informe de la autoevaluación del control y la gestión.

7.2. DESCRIPCIÓN DE ACTIVIDADES

Las responsabilidades de los gestores de riesgo son:

- Registrar información que permita monitorear el desarrollo de los planes de tratamiento de riesgos: Cumplimiento de actividades planificadas, costos incurridos.

- Registrar la información de eventos ocurridos en el día a día del proceso, validar si estos eventos constituyen riesgos materializados o no y hacer análisis de causas de los riesgos materializados desde la perspectiva de tratamiento del riesgo.

- Registrar las iniciativas de cualquier funcionario en relación con los campos de identificación de riesgos (riesgos, causas, efectos, situaciones de materialización y controles de detección).

7.2.1.1. Registro de Seguimiento de Actividades Planificadas

El gestor de riesgos deberá hacer seguimiento a la ejecución de las actividades descritas en el Formato o formulario "Plan de Tratamiento de Riesgos" para aquellos planes de responsabilidad de ejecución de actividades o porque el riesgo afecta su proceso.

Para realizar esta actividad se deberá diligenciar el formato o formulario de "Seguimiento a Planes" que contiene los siguientes campos:

- **Fecha de revisión del registro**: fecha en la que se hace la revisión de la ejecución de las actividades.

- **Descripción del entregable (calidad):** Describir si el entregable cumple con las características de calidad esperadas de acuerdo con su finalidad.

- **Fecha efectiva de realización de la tarea:** Fecha en la que se terminó de realizar la tarea. (De acuerdo con la evidencia).

- **Costo real de la actividad ejecutada (AC):** Costos reales incurridos para dar cumplimiento a la actividad planificada.
- **Observaciones:** Cualquier comentario adicional que se considere pertinente cuando se hace el seguimiento.

7.2.2. Registro de Riesgos Materializados del día a día

Para poder identificar los riesgos materializados es necesario revisar ciertos eventos que ocurren en el día a día de un proceso. El primer paso es registrar todos los "posibles eventos que podrían ser riesgos materializados", estos serán llamados Eventos Potenciales a Evaluar **(EPE)**. Una vez se haya hecho el registro de todos estos eventos, se procederá a validar con unos criterios específicos si ellos constituyen un riesgo materializado.

Serán considerados Riesgos Materializados **(RM)** las situaciones descritas en los numerales del 7.2.2.2. al 7.2.2.5.

7.2.2.1. Riesgos materializados

Un riesgo materializado es la ocurrencia de un evento que se había identificado como incierto, cuando esto ocurre, es crítico detectar esta situación lo más pronto posible para que en el proceso se lleven a cabo las acciones pertinentes sin demora (corrección / plan de contingencia) y/o acción correctiva.

Para poder determinar si un riesgo se ha materializado, es importante que desde la identificación del mismo se tenga claro cómo se podría materializar y que se tengan definidos e implementados los controles, que en caso de su materialización, permitan detectar la ocurrencia de la situación inmediatamente.

En el Formato o formulario "Riesgos Materializados", se deberá relacionar para cada uno de los riesgos materializados, la siguiente información:

Descripción de la Situación (Riesgo Materializado)	**Fecha**

Para poder registrar los riesgos materializados se deben tener en cuenta, además de los riesgos que están dentro del formato o formulario de identificación de riesgos, las siguientes situaciones descritas en los numerales 7.2.2.2, 7.2.2.3, 7.2.2.4 y 7.2.2.5.

7.2.2.2. Metas incumplidas de los Indicadores de Proceso

De las normas ISO 9001 / NTCGP1000:2009, numeral 8.2.3: "La entidad debe aplicar métodos apropiados para el seguimiento de los procesos del Sistema de Gestión de la Calidad, y cuando sea posible, su medición. Estos métodos deben demostrar la capacidad de los procesos para alcanzar los resultados planificados (eficacia)".

Para dar cumplimiento a este requisito uno de los mecanismos utilizados son los indicadores de los procesos. Si un indicador no cumple sus metas, significa que no se cumplió un resultado planificado. Teniendo en cuenta que el objetivo de la gestión de riesgos es prevenir el impacto de los eventos que afectan el cumplimiento de los objetivos, el incumplimiento de una meta de los indicadores se constituye como un evento a ser evaluado en la gestión de riesgos.

La información de cuáles son los indicadores, cuál es su meta y cuál es la frecuencia con que se deben analizar (este análisis debe estar documentado), debe ser tomada de la caracterización de los procesos. La información de los resultados de los indicadores y el análisis correspondiente de esos resultados, se encuentra en los Informes de Autoevaluación del Control y la Gestión de cada proceso.

Esta relación entre los indicadores y la gestión de riesgos se cumple cuando los indicadores de gestión se han formulado de manera que permitan medir el cumplimiento de los objetivos del proceso.

En el Formato o formulario Indicadores de Gestión de Proceso, en Eventos Potenciales a Evaluar, para cada uno de los indicadores del proceso incumplidos en el periodo, se deberá relacionar la siguiente información:

(Nombre del Indicador)	**Fórmula**	**Temporizador**

7.2.2.3. Metas incumplidas de los Indicadores de los Planes, Proyectos y Programas

Un plan, proyecto o programa, es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.

Tienen un principio y un final definidos. El final del plan, proyecto o programa se alcanza cuando se logran los objetivos de los mismos o cuando se termina el plan, proyecto o programa, porque sus objetivos no se cumplirán o no pueden ser cumplidos, o cuando ya no existe la necesidad que le dio origen a estos. En una organización se espera que estos planes, proyectos o programas contribuyan a mejorar la gestión de sus procesos y adicionalmente a contribuir al logro de los objetivos estratégicos de la Institución.

En el desarrollo de un plan, proyecto o programa hay muchas variables que se pueden y se deben controlar: tiempo (cronograma), costo (presupuesto), alcance, entre otras. Los controles que se definan para estos proyectos deberían traducirse en indicadores que permitan conocer el estado del proyecto mientras que avanza.

Dicho lo anterior, es claro que el éxito o fracaso de un plan, proyecto o programa afecta el cumplimiento de los objetivos de un proceso y de la institución y por lo tanto su desempeño y sus resultados deben ser medidos.

El éxito de un plan, proyecto o programa, medido a través de los indicadores que se definan, permitirá determinar si la gestión de riesgos en esos proyectos ha sido efectiva. Si alguno de estos indicadores no cumplió la meta, será considerado un evento a evaluar para la gestión de riesgos.

En el "Formato o formulario Indicadores de Proyectos", se deberá relacionar para cada uno de los indicadores con metas incumplidas, la siguiente información:

(Nombre del Indicador)	**Fórmula**	**Tipo de Proyecto***	**Temporizador**

*Tipo de Proyecto: Plan de Acción, PAS, Proyecto de Inversión, etc.

7.2.2.4. Producto No Conforme

El Producto No Conforme es un producto o servicio que no cumple con los requisitos establecidos; las actividades que permiten identificarlo, controlarlo y evitar su uso o entrega no intencionados se han documentado por parte la Institución. De acuerdo con lo establecido en este procedimiento, un no conforme puede llegar a afectar la satisfacción del cliente externo (ciudadanía) y/o la de la comunidad policial, es importante entonces analizarlo desde este punto de vista en relación con el riesgo. Cada proceso deberá tener claridad de si el PNC aplica a su proceso y a su nivel. El registro de productos/servicios no conformes, su análisis y tratamiento se encuentra en el documento (formato o formulario) establecido para tal fin.

Para efectos de la medición de los Resultados de la Gestión Integral del Riesgo, solo se registrarán los productos no conformes que se deriven de la prestación del servicio misional de acuerdo a su ámbito de gestión.

Nota: Las quejas y/o reclamos, deben ser evaluados y analizadas desde la perspectiva de riesgos, con el fin de determinar si fue un riesgo materializado y si se tenía o no identificado. En este sentido debe existir un cruce de información permanente entre la dependencia de atención al ciudadano y planeación de cada unidad policial, para definir, a parte de los trámites legales, qué se debe hacer desde la metodología del riesgo.

Por favor tener en cuenta el nivel del proceso para determinar si aplica o no el concepto de No Conforme, de acuerdo a la guía para el control del producto o servicio no conforme en la Policía Nacional.

En el formato o formulario de Producto y/o Servicio No Conforme, se deberá relacionar para cada uno de los productos no conformes la siguiente información:

Descripción del Producto / Servicio No Conforme	**Fecha**

7.2.2.5. No Conformidades

Una no conformidad es el incumplimiento de un requisito; las actividades que permiten identificarlas, determinar sus causas, determinar e implementar acciones y determinar la eficacia se han documentado en el procedimiento establecido para tal fin.

Las fuentes establecidas para declarar una no conformidad son: auditorías internas y externas, autoevaluación, los resultados de cualquiera de las siguientes actividades: revisión por la dirección, evaluación de la rendición de cuentas, evaluación de quejas, reclamos y sugerencias, satisfacción del cliente, seguimiento al cumplimiento del Plan Estratégico Institucional. Las no conformidades se documentan en el Formato o formulario de Plan de Mejoramiento.

Para efectos del análisis de riesgos, se deberán considerar solo aquellas no conformidades que describan incumplimientos ya presentados sobre el producto o servicio que evidencia el cumplimiento del objetivo del proceso.

En el Formato o formulario No Conformidades y Hallazgos, se deberá relacionar para cada una de las no conformidades identificadas en el periodo evaluado, la siguiente información:

Descripción de la No Conformidad	**Fecha (de detección de la no conformidad)**

7.2.3. Validar EPE para identificar Riesgos Materializados (RM)

El objetivo de esta "validación" es determinar si las situaciones registradas en los numerales del 7.2.2.2. al 7.2.2.5. Son riesgos materializados o no.

Para cada uno de los eventos potenciales a evaluar, en la "Matriz de Validación" o módulo de riesgos PRO – link: "Realizar Gestión del Riesgo", identificar y registrar cuál es el riesgo asociado al incumplimiento, de igual forma, identificar y registrar la causa y agente generador de ese riesgo. Si es posible hacer la identificación del riesgo a partir del incumplimiento, el evento será un RM y se deberá marcar SI en la casilla correspondiente, de lo contrario marcar NO y justificar la respuesta.

Una vez se hayan validado todos los eventos, se deberá hacer una revisión integral con el fin de asegurar que no queden eventos repetidos. Si esto ocurre, eliminar uno de ellos y en el que queda, aclarar la situación en el campo de observaciones.

7.2.4. Hacer Análisis de Causa a los Riesgos Materializados (RM)

Son aquellos que en la "Matriz de Validación" fueron marcados como "SI". Estos eventos se deberán analizar para determinar cuál fue la causa para que ese riesgo se haya materializado desde la perspectiva de tratamiento del riesgo. El análisis se hace mediante el diligenciamiento de los siguientes campos:

7.2.4.1. Causa Generadora Asociada al Riesgo

Determinar y seleccionar desde la perspectiva de riesgos cual fue la causa que generó el evento. Las dos primeras opciones toman como referencia el "Formato o formulario de Descripción de Riesgos", las tres que siguen los "Formato o formularios de la Fases de Definición de la Gestión". Para esto se deberá seleccionar la opción más apropiada de la siguiente tabla (opciones de 1 a 5):

TABLA 3. CAUSA GENERADORA ASOCIADA AL RIESGO

	CAUSA ASOCIADA AL RIESGO - OPCIONES
1	El riesgo no se había identificado (en el formato o formulario de identificación de riesgos).
2	El riesgo se había identificado pero no la causa.
3	El plan de mitigación para la causa identificada no se ejecutó.
4	El plan de mitigación para la causa identificada se llevó a cabo, pero no fue efectivo.
5	El plan de mitigación para la causa identificada se llevó a cabo, y fue parcialmente efectivo.

7.2.4.2. Acción / Plan de Contingencia.

Se debería definir una acción de contingencia cuando como resultado de la materialización de un riesgo, se vean afectadas las operaciones normales de la Institución y por lo tanto se requiere restablecerlas lo más pronto y con la mejor calidad posible.

Es claro que para cada uno de los eventos que se describen en la metodología, se requiere un tratamiento y dado que estos eventos hacen referencia a incumplimientos, se asume que para cada uno de ellos se ha debido generar una no conformidad y darle el debido tratamiento de acuerdo con lo establecido en el procedimiento "Ejecutar Acciones de mejoramiento", formulando las correcciones y/o acciones correctivas a que hubiere habido lugar con base en el análisis de causas.

Esas correcciones y acciones correctivas deben haberse relacionado en el Formato o formulario de Plan de Mejoramiento y por lo tanto no se espera que se relacionen nuevamente en este formato o formulario.

Un riesgo materializado puede requerir cualquiera de las siguientes respuestas:

a. Solo una acción correctiva.
b. Corrección y acción correctiva.
c. Corrección, acción correctiva y acción /plan de contingencia.
d. Acción correctiva y plan/acción de contingencia.

Las correcciones y/o acciones correctivas deberán ejecutarse de acuerdo al procedimiento obligatorio establecido, y posteriormente de definidas las tareas a desarrollar, deben cargarse como "plan de tratamiento" del riesgo (s) en la herramienta tecnológica dispuesta para tal fin. Esta actividad se debe realizar de acuerdo a los resultados obtenidos en la ejecución de los numerales 7.2.3, 7.2.4, 7.2.4.1 y 7.2.4.2 del presente manual.

Es importante tener en cuenta que los tres conceptos son diferentes. Se requieren acciones de contingencia cuando como resultado de la materialización del riesgo se puede presentar interrupciones en la prestación del servicio.

Analizar y seleccionar la opción apropiada.

	ACCIÓN DE CONTINGENCIA
1	No se requería.
2	Se requería, pero no se había definido.
3	Estaba definida y se implementó, pero no fue efectiva.
4	Estaba definida, se implementó y fue efectiva.
5	Estaba definida, se implementó y fue parcialmente efectiva.

7.2.4.3. Acción a tomar en la Descripción de Riesgos.

Teniendo en cuenta la información obtenida hasta el momento, determinar y registrar si se requiere hacer ajustes sobre el mapa de riesgos (incluir información, no se requiere acción). Ejemplo:

Si la causa generadora del riesgo es que no se había identificado el riesgo en el Mapa de Riesgos, se deberá marcar la Opción 1: "Se incluirá información en la Descripción de Riesgos", porque se deberá incluir el nuevo riesgo en el mapa y diligenciar todos los campos del formato o formulario de identificación.

ACCIÓN A TOMAR EN RELACIÓN AL RIESGO	
1	Se incluirá información en la descripción de riesgos.
2	Se modificará información en la descripción de riesgos.
3	No se tomará ninguna acción en relación con en la descripción de riesgos.

Cuando un riesgo se materializa se debe identificar la causa específica que lo generó e inmediatamente se deberán revisar las calificaciones dadas a cada uno de los criterios de valoración de los controles asociados a esa causa. Ejemplo: Si un riesgo se materializa es claro que la efectividad del control no es la esperada y eso deberá reflejarse en la valoración del control en ese criterio. De igual forma se deben revisar los otros criterios de valoración. En estos casos el nivel de riesgo del proceso aumenta; por el contrario, cuando se generan nuevos controles como resultado de los planes de tratamiento, se esperaría que el nivel de riesgos disminuya.

Es responsabilidad del gestor de riesgos monitorear constantemente la valoración de los controles.

7.2.4.4. Observaciones

Se debe relacionar cualquier información que se considere relevante para la situación que se esté tratando.

7.2.4.5. Costos Generados

Se deberán registrar los costos generados como resultado del riesgo materializado, ejemplo: multas, resarcimientos, implementación de planes de contingencia, etc.

7.2.5. Registro de iniciativas de funcionarios del proceso

El gestor de riesgos deberá registrar y analizar las iniciativas que provengan de cualquier funcionario, que permitan generar acciones preventivas. Las fuentes que pueden dar origen a estas iniciativas son:

- Resultado de la evaluación de quejas, reclamos y sugerencias.
- Análisis de satisfacción del cliente.
- Resultado de revisión por la Dirección.
- Informe de la autoevaluación del control y la gestión.
- Los riesgos identificados.

Las iniciativas / sugerencias de los funcionarios pueden expresarse en términos de: nuevos riesgos, nuevas causas, nuevos efectos, nuevas situaciones de materialización, nuevos controles de detección.

Estas sugerencias, una vez analizadas por el gestor de riesgos, deberán relacionarse en el Formato o formulario Propuestas de Sugerencias.

7.3. RESPONSABILIDADES POR CARGOS / NIVELES

Los funcionarios designados en el "Plan de Tratamiento de Riesgos" deberán ejecutar la actividad.

Gestores de Riesgos de los tres niveles: Registrar todos los eventos descritos en el presente documento, evaluarlos y analizarlos.

Gestores de Riesgos de Nivel 2: Solicitar y recibir el trabajo de los gestores de riesgo de nivel 3 de su proceso, analizarlo, verificarlo para asegurarse de su calidad y coherencia.

Gestores de Riesgos de Nivel 1: Solicitar y recibir el trabajo de los gestores de riesgo de nivel 2 de su proceso, analizarlo, verificarlo para asegurarse de su calidad y coherencia. Enviar a la Oficina de Planeación.

Funcionarios de la Oficina de Planeación: Revisar y aprobar el trabajo enviado por los niveles 1 y 2.

8. FASE MEDICIÓN DE LOS RESULTADOS DE LA GESTIÓN

8.1. OBJETIVO DE LA FASE

El objetivo de esta fase es determinar el nivel de efectividad de la gestión realizada, es decir, si las actividades ejecutadas en las fases anteriores han dado los resultados que se esperan.

Que un proceso tenga una gestión adecuada, significa:

- Que pudo cumplir su objetivo.
- Que pudo llevar a cabo con éxito los planes, proyectos y/o programas con los que esperaba contribuir a los objetivos estratégicos de la Institución para cumplir su misionalidad.
- Que los riesgos que identificó no se hayan materializado y si se materializaron que el impacto haya sido controlado por las acciones de contingencia.
- Que no se presentaron productos / servicios no conformes y si se presentaron hayan sido adecuadamente tratados.
- Que no se hayan identificado no conformidades al proceso en relación con su misionalidad, y si se presentaron hayan sido adecuadamente tratadas.

8.2. DESCRIPCIÓN DE ACTIVIDADES

Las responsabilidades de los gestores de riesgo son:

- Analizar los indicadores de la gestión de riesgos.
- Formular acciones que lleven a la mejora.

Se debe utilizar el formato o formulario de "Informe Trimestral Resultados de Gestión Integral del Riesgo".

8.2.1. Diligenciamiento del Informe Trimestral de Gestión Integral del Riesgo

El informe trimestral se alimenta de la información recopilada, registrada y analizada en la fase de Gestión de Riesgos. El informe tiene tres secciones, la intencionalidad de cada una se describe a continuación:

NÚMERO SECCIÓN	NOMBRE SECCIÓN	DESCRIPCIÓN / INTENCIONALIDAD
SECCIÓN 1	Variación del Nivel de Riesgo del Proceso	En esta sección se presentan los niveles de riesgo del proceso al inicio y al final del periodo, la variación de nivel permite mostrar la efectividad de la gestión. Adicionalmente, se presenta la información que permite soportar y analizar los datos presentados.
SECCIÓN 2	Riesgos Materializados	Se muestran (en cantidad) los riesgos materializados en el periodo y los indicadores que permiten analizar las causas de esas materializaciones desde la perspectiva de tratamiento del riesgo. Se presentan también los costos generados por riesgos materializados.
SECCIÓN 3	Desempeño de Planes Tratamiento	El objetivo de esta sección es mostrar cómo ha sido la labor de implementación de planes de tratamiento en relación con las variables de tiempo y costo.

8.2.1.1. Sección 1. Variación del Nivel de Riesgos del Proceso.

VNR (Variación de Nivel de Riesgos): Esta información debe ser tomada de la registrada y/o emitida por la herramienta tecnológica utilizada para tal fin.

El nivel de riesgos de un proceso se ve modificado cuando cambia la probabilidad o el impacto de uno o más de sus riesgos, esto puede ocurrir cuando se presenta cualquiera de las siguientes situaciones:

SITUACIÓN
Cuando se identifica un nuevo riesgo, causa, efecto o situación de materialización.
Cuando se elimina un riesgo, causa, efecto o situación de materialización.
Cuando se crean o eliminan controles.
Cuando un riesgo se materializa.

8.2.1.2. Sección 2. Riesgos Materializados.

En esta sección se muestra el número de riesgos materializados y los costos incurridos por la Institución por esta materialización. Adicionalmente se presentan indicadores que permiten identificar en que parte del proceso se presentaron las fallas que produjeron la ocurrencia del evento.

El gestor de riesgos deberá analizar esta información para que con juicio crítico y conociendo su proceso, documente el análisis. El análisis deberá dar información con respecto a lo siguiente:

- En qué parte de la gestión de riesgos se concentran las mayores debilidades: en la identificación de riesgos, en la identificación de causas, en la definición de acciones, en la ejecución de acciones; por qué y qué se va a hacer al respecto.
- En los casos en los que se requería plan de contingencia, que tan efectivo fue este y por qué.
- Un resumen ejecutivo de los riesgos materializados, indicando cual/es tuvo/tuvieron más impacto o trascendencia.
- Cualquier otro aspecto que el gestor considere que se debe mencionar con base en su criterio.

Las conclusiones deben referirse específicamente a la administración de riesgos, no deben ser una copia del análisis de causa raíz de cada uno de aspectos incumplidos.

IR (Identificación de Riesgos): Este indicador muestra, del total de riesgos materializados, cuantos se generaron porque no se habían identificado.

IC (Identificación de Causas): Este indicador muestra, del total de riesgos materializados, cuantos se generaron porque la causa que ocasionó el evento no se había identificado.

MR (Mitigación de Riesgo): Este indicador muestra, del total de riesgos materializados, cuantos se generaron por dificultades en la ejecución de las acciones definidas en los planes de mitigación (acciones).

Para analizar esta información, es útil revisar los resultados parciales que lo conforman y que se encuentran en la Evaluación Consolidada: **MR3, MR4 y MR5.**

La suma de los eventos de **IR, IC y MR** dan el 100% de los eventos.

CT1, CT2, CT3 Y CT4. (Contingencia): Estos datos muestran si para el evento específico analizado se requería una acción de contingencia o no, y en los casos en que si, evalúa la calidad de esas acciones.

Para analizar esta información, es útil revisar los resultados parciales que lo conforman y que se encuentran en el Consolidado de Resultados.

8.2.1.3. Sección 3. Desempeño de los Planes de Tratamiento.

Se muestran dos medidas (indicadores) que permiten ver cómo ha sido el desempeño de los planes de tratamiento. Los dos indicadores deberán ser generados para cada plan de tratamiento que lleve el proceso.

La primera, el **CPI**, es el Índice de Desempeño del Costo, (por sus siglas en inglés). Mide como se han administrado los costos del plan, proyecto y/o programa, qué tan bien se planificaron los recursos para la ejecución de las actividades. Es igual al valor ganado (**EV**) sobre el costo real (**AC**).

El (**EV)** Valor Ganado, es el valor del trabajo que se ha realizado a la fecha de corte del periodo evaluado.

El (**AC)** Costo Real, es igual a la suma de los costos en los que se ha incurrido para la realización de las actividades propuestas.

La segunda medida es el **SPI** o Índice de Desempeño del Cronograma, (por sus siglas en inglés); este indicador mide el avance logrado en un plan, proyecto y/o programa en comparación con el avance planificado. Los resultados se interpretar de acuerdo con la siguiente tabla:

CUANDO	SIGNIFICA
CPI > 1	Que los costos incurridos son inferiores con respecto al desempeño a la fecha de la evaluación.
CPI < 1	Que hay un sobrecosto en relación con el trabajo completado.
CPI = 1	Que los costos incurridos son iguales a los planificados para el trabajo ejecutado.
SPI > 1	Que la cantidad de trabajo efectuada es mayor a la prevista.
SPI < 1	Que la cantidad de trabajo efectuada es menor que la prevista.
SPI = 1	Que el trabajo efectuado es el que se había planificado.

Ejemplo:

Ejemplo:	PV (Valor Planificado)	Costo Real (AC)
Actividad 1	100	95
Actividad 2	20	30
Actividad 3	35	35
Actividad 4	40	
Actividad 5	70	

En este ejemplo se da el valor planificado para 5 actividades y se da el costo real para aquellas actividades que ya fueron ejecutadas. Solo se han ejecutado las primeras tres actividades.

El **EV** es igual a 100+20+35 = 155, es el valor planificado para las actividades que se han llevado a cabo a la fecha.

El **AC** es igual a igual a 95+30+35 = 160, es la suma de los costos reales de las actividades ejecutadas.

Por lo tanto el **CPI** es igual a 155 / 160 = 0,968 que es un valor menor que 1. Eso significa que hay un sobrecosto con respecto al trabajo completado.

Ahora, el **PV** es el valor planificado (costos estimados y autorizados) para las 5 actividades, en este caso 256. (100+20+35+40+70).

El **SPI** es igual a **EV / PV, EV** = 155, **PV** = 256. Entonces, **SPI** = 155 / 256 = **0,60** que es menor que 1, lo anterior significa, que la cantidad de trabajo efectuada es menor que la prevista.

El gestor deberá hacer el análisis y definir acciones a tomar con base en los resultados de estos indicadores, el entendimiento de los datos, y el conocimiento del proceso y su situación.

Los funcionarios de la Oficina de Planeación serán los responsables de consolidar y presentar los resultados de la gestión para los riesgos institucionales.

8.3. RESPONSABILIDADES POR CARGOS / NIVELES

Gestores de Riesgos de los tres niveles: Diligenciar el informe trimestral de Resultados como lo indica este documento. Este informe es válido siempre y cuando sea el emitido por la herramienta tecnológica utilizada para tal fin.

Gestores de Riesgos de Nivel 2: Solicitar y recibir el trabajo de los gestores de riesgo de nivel 3 de su proceso, analizarlo, verificarlo para asegurarse de su calidad y coherencia. Enviar a la los gestores de nivel 1.

Gestores de Riesgos de Nivel 1: Solicitar y recibir el trabajo de los gestores de riesgo de nivel 2 de su proceso, analizarlo, verificarlo para asegurarse de su calidad y coherencia. Enviar a la Oficina de Planeación.

Funcionarios de la Oficina de Planeación: Revisar, aprobar y analizar el trabajo consolidado de los niveles 1, 2 y 3. Con base en este análisis consolidado se deberán proponer acciones de mejoras estructurales o puntuales cuando sea pertinente.

9. FASE CIERRE DE LA GESTIÓN DE RIESGOS

9.1. OBJETIVO DE LA FASE

El objetivo de esta fase es organizar de manera sistemática las experiencias (positivas y negativas), conocimientos y resultados de la gestión de riesgos, con el fin de generar lecciones aprendidas que permitan a la Institución obtener mejores resultados en el futuro a través de la réplica de los aciertos y de la no repetición de los desaciertos.

9.2. DESCRIPCIÓN DE ACTIVIDADES

Las responsabilidades de los gestores de riesgo son:

- Diligenciar el Informe Anual de Gestión de Riesgos.
- Documentar Situaciones Relevantes.

Los funcionarios de la Oficina de Planeación deberán:

- Consolidar y analizar informes anuales y situaciones relevantes.
- Proponer lecciones aprendidas.
- Preparar la información para la Revisión por la Dirección.
- Retroalimentar a los gestores de riesgos.

9.2.1. Diligenciamiento del Informe Anual de Gestión de Riesgos.

El informe anual se alimenta de los Informes Trimestrales de Gestión de Riesgos de cada proceso, que se elaboran en la Fase de Medición de Resultados de la Gestión.

El informe tiene cuatro secciones, la intencionalidad de cada una se describe a continuación:

NÚMERO SECCIÓN	NOMBRE SECCION	DESCRIPCIÓN / INTENCIONALIDAD
SECCIÓN 1	Variación del Nivel de Riesgo del Proceso	En esta sección se presentan los niveles de riesgo del proceso al inicio y al final del periodo. La variación permite mostrar la efectividad de la gestión. El análisis de este indicador debe permitir conocer cuáles fueron los factores más relevantes que incidieron en el resultado.
SECCIÓN 2	Riesgos Materializados	Se muestran (en cantidad) los riesgos materializados en el periodo y los indicadores que permiten analizarlas causas de esas materializaciones desde la perspectiva de tratamiento del riesgo. El análisis debe presentar los riesgos materializados que fueron críticos para el proceso y para la Institución.
SECCIÓN 3	Desempeño de Planes Tratamiento	El objetivo de esta sección es mostrar cómo ha sido la labor de implementación de planes de tratamiento en relación con las variables de tiempo y costo. El análisis de los indicadores de esta sección debe permitir conocer cuáles fueron los factores más relevantes que incidieron en los resultados.
SECCIÓN 4	Conclusiones	Con base en lo presentado en las secciones 1, 2 y 3 se debe concluir como fue la Gestión de Riesgos y presentar cuales fueron los aciertos y desaciertos.

9.2.1.1. Sección 1. Variación del Nivel de Riesgos del Proceso.

VNR (Variación de Nivel de Riesgos): Esta información debe ser tomada de la registrada y/o emitida por la herramienta tecnológica utilizada para tal fin.

Se deberá analizar el resultado del indicador presentando y los factores más relevantes que incidieron en él.

9.2.1.2. Sección 2. Riesgos Materializados.

En esta sección se muestra el número de riesgos materializados y los costos incurridos por la Institución por esta materialización. Adicionalmente se deben calcular los indicadores que permiten identificar en que parte del proceso se presentaron las fallas que condujeron a la ocurrencia de los eventos.

Las conclusiones deben referirse específicamente a la gestión de riesgos, no deben ser una copia del análisis de causa raíz de cada uno de aspectos incumplidos.

Para el cálculo de estos indicadores se deberá tomar lo registrado en cada uno de los cuatro (4) informes trimestrales previos.

IR (Identificación de Riesgos): Número total de riesgos materializados porque no se había identificado el riesgo; dividido por el número total de riesgos materializados.

IC (Identificación de Causas): Número total de riesgos materializados porque no se había identificado la causa que lo genero, dividido por el número total de riesgos materializados.

MR (Mitigación de Riesgo): Número total de riesgos materializados por dificultades en la ejecución de acciones de los planes de mitigación, dividido por el número total de riesgos materializados.

La suma de los eventos de **IR, IC y MR** dan el 100% de los eventos.

CT1, CT2, CT3 Y CT4. (Contingencia): Se deberá diligenciar la tabla de acciones de contingencia con base en los resultados de los informes trimestrales.

El gestor deberá hacer el análisis de los indicadores en su conjunto, y documentar cuales fueron los factores más relevantes que influyeron en los resultados.

9.2.1.3. Sección 3. Desempeño de los Planes de Tratamiento.

Se debe mostrar el resultado del **CPI** y el **SPI** para cada uno de los planes de tratamiento del proceso.

El gestor deberá hacer el análisis de los indicadores en su conjunto, y documentar cuáles fueron los factores más relevantes que influyeron en los resultados.

9.2.2. Documentación Situaciones Relevantes

Dado que la presente metodología se ajusta al principio de que la Gestión Integral del Riesgo es parte integral de todos los procesos de la Institución, la información recopilada durante todo el ciclo permite conocer situaciones relacionadas no sólo con la gestión de riesgos en sí, si no con la misionalidad de cada proceso.

Con base en los datos y análisis presentados en el "Informe Anual de Gestión", cada gestor de riesgos deberá documentar las situaciones que generaron mayores efectos en el año evaluado. Para documentar estas situaciones se deberá tener en cuenta lo siguiente:

- **Número de situación:** Este campo será diligenciado por la Oficina de Planeación.
- **Periodo en el que se presentó la Situación:** Se deben escribir las fechas de inicio y fin de la situación, o una aproximación de las dos fechas si no se pueden identificar fechas específicas.
- **Lugar en el que se presentó la situación:** Lugar o lugares donde ocurrieron los hechos.
- **Involucrados en la Situación:** Cargos de las personas involucradas (no nombres), ciudadanía, entes externos, etc.
- **Por qué es una situación relevante:** Justificar porque esta situación se destaca de las demás ocurridas en el año. Los argumentos deben ir en relación con los efectos generados.
- **Descripción de la situación:** Describir claramente la situación que se presentó, aunque se espera que la narración sea breve y concisa, se deben relacionar los detalles que soportan la veracidad (evidencia).
- **Aciertos:** Relacionar aquellas actuaciones que lograron que la situación se desenvolviera de manera favorable para la Institución o para el Proceso.
- **Desaciertos:** Relacionar aquellas actuaciones que generaron efectos no deseables para la Institución.
- **Aspectos adicionales:** Comentarios, sugerencias, recomendaciones, información que el gestor de riesgos considere importante para el caso y que no se haya nombrado anteriormente.

Estas situaciones relevantes podrán hacer referencia a temas específicos de la misionalidad de cada proceso, o específicamente a la temática de administración de riesgos.

Todos los procesos deben remitir las situaciones relevantes documentadas a la Oficina de Planeación.

9.2.3. Consolidación y Análisis de Información.

El informe anual de resultados de la gestión de riesgos y las situaciones relevantes documentadas deben ser remitidos a la Oficina de Planeación.

Los funcionarios de la Oficina de Planeación deberán revisar la información enviada en términos de coherencia de los datos, de pertinencia de los análisis, relevancia y claridad de las situaciones presentadas. Se podrá solicitar a los gestores de los procesos la documentación que se considere para aclarar y/o soportar el informe.

Se enviaran oficios de retroalimentación cuando se considere necesario.

9.2.4. Lecciones Aprendidas.

Las situaciones relevantes presentadas por los procesos, deberán ser evaluadas como posibles insumos para lecciones aprendidas, para esto se deberán tener en cuenta las definiciones del documento "Lecciones Aprendidas en la Policía Nacional (2009)": lecciones aprendidas del orden operativo y procedimental, lecciones aprendidas del orden táctico policial, lecciones aprendidas del orden estratégico.

9.2.5. Preparación de Información para la Revisión por la Dirección.

Los funcionarios de la Oficina de Planeación deberán preparar la información para carácter gerencial, el contenido de este informe deberá ser concreto y deberá mostrar solo aspectos relevantes para la Institución.

Deberán presentarse los cuatro (4) aspectos siguientes:

9.2.5.1. Informe Anual de Gestión.

Con la misma estructura que el informe de procesos se elabora el informe anual de gestión de riesgos para toda la Institución. Se deberá documentar y presentar el análisis de los datos del informe, mostrando los aspectos más relevantes que llevaron a esos resultados.

9.2.5.2. Riesgos Institucionales.

Los funcionarios de la Oficina de Planeación presentarán el informe anual de gestión para los riesgos institucionales con su respectivo análisis.

9.2.5.3. Lecciones Aprendidas.

Una vez se ha surtido el procedimiento para identificar las lecciones aprendidas (Documento Lecciones Aprendidas en la Policía Nacional) con base en las "Situaciones Relevantes" puestas a consideración, se presentan el resumen de las que si fueron aprobadas.

9.2.5.4. Retroalimentación de los resultados de la Gestión.

Los funcionarios de la Oficina de Planeación deberán retroalimentar a todos los gestores de riesgos con la siguiente información:

- Información presentada en la Revisión por la Dirección.
- Conclusiones de la Revisión por la Dirección (relativas a los riesgos).
- Recomendaciones, sugerencias, instrucciones especiales.

Todos los productos resultantes de esta fase son insumos que deben tener en cuenta los gestores de riesgos para la identificación / actualización de los riesgos de su proceso en el siguiente periodo.

9.2.6 Informes de Resultados de Gestión del Riesgo trimestral y/o anual

Los "informes de gestión del riesgo" generados a partir de la ejecución de las fases de medición de los resultados de la gestión y cierre, respectivamente, serán considerados independientes de la información reflejada en los informes de autoevaluación de la gestión y el control. Por tal razón, en este último solo aparecerá la información de la siguiente manera: *"Resultados de la gestión del riesgo" (esta información debe ser consultada en la herramienta utilizada para tal fin, en link "reporte", "resultados de la gestión de riesgos".*

Nota: Siempre y en la medida de lo posible, los resultados de gestión del riesgo, tanto trimestral como anual, no deben imprimirse ya que los mismos son consultables en cualquier momento y las veces que se quiera en el sistema y/o herramienta utilizada para tal fin.

9.3. RESPONSABILIDADES POR CARGOS / NIVELES

Gestores de Riesgos de los tres niveles: Diligenciar el "Informe anual de Gestión de Riesgos" y documentar las situaciones relevantes de su proceso.

Gestores de Riesgos de Nivel 2: Solicitar y recibir el trabajo de los gestores de riesgo de nivel 3 de su proceso, analizarlo, verificarlo para asegurarse de su calidad y coherencia. Enviar a la los gestores de nivel 1.

Gestores de Riesgos de Nivel 1: Solicitar y recibir el trabajo de los gestores de riesgo de nivel 2 de su proceso, analizarlo, verificarlo para asegurarse de su calidad y coherencia. Enviar a la Oficina de Planeación.

Funcionarios de la Oficina de Planeación: Consolidar y analizar informes anuales y situaciones relevantes, proponer "Lecciones Aprendidas", preparar la información para la Revisión por la Dirección, retroalimentar a los gestores de riesgos.

10. TÉRMINOS Y DEFINICIONES

10.1 TÉRMINOS RELATIVOS AL PLAN INICIAL DE IDENTIFICACIÓN / FASE DE IDENTIFICACIÓN.

Efecto: Desviación de aquello que se espera, sea positivo, negativo o ambos.

Incertidumbre: Es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o posibilidad.

Riesgo: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. (Guía de Admón. De Riesgos DAFP Septiembre 2011).

Riesgo: Algo que podría suceder y afectar el logro de los objetivos organizacionales. (GTC 176)

Riesgo: Efecto de la incertidumbre sobre los objetivos. (GTC137: 2011)

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo. (GTC137: 2011).

Descripción del Riesgo: Declaración estructurada del riesgo que usualmente contiene cuatro elementos: fuentes, eventos, causas y consecuencias. (GTC137:2011).

Fuente de un Riesgo: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (GTC137:2011). Puede ser tangible o intangible.

Evento: Ocurrencia o cambio de un conjunto partículas de circunstancias. (GTC137:2011) en algunas ocasiones se hace referencia a un evento como un "incidente" o "accidente".

Propietario del Riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (GTC137:2011). En la Policía Nacional el concepto aplica para procesos con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo, decidir las estrategias de mitigación del riesgo, aceptar el riesgo, aprobar los presupuestos para mitigación de riesgos y ejecutar los planes de tratamiento.

Riesgos Transversales: En la Policía Nacional, con este término se designarán los eventos que aunque tienen como propietario a un solo proceso, pueden ser causa o efecto de otros eventos de riesgo para los demás procesos de la Institución:
Ejemplo: "Que el personal no cuente con las competencias apropiadas para desempeñar un cargo", para el proceso de Administración del Talento Humano identifiquen, será un agente generador, no un riesgo. Ningún proceso que no sea el de Administración del Talento Humano podrá relacionarlo como riesgo, porque solo este proceso (Talento Humano) tiene la autoridad para gestionarlo y la responsabilidad de rendir cuentas.

Nota 1: Generalmente los procesos propietarios de los riesgos transversales son los de Soporte.

Análisis de Contexto: Son las 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 sea 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.

10.2 TÉRMINOS RELATIVOS A LA FASE DEFINICIÓN DE LA GESTIÓN

Alcance de un Proyecto: Trabajo que debe realizarse para entregar un producto, servicio o resultado con las características y funciones especificadas (PMBOK, 4ta. Edición).

Control: Medida o acción que modifica el riesgo mediante la afectación ya sea de la probabilidad o del impacto. (GTC137:2011).

Consecuencia: Resultado de un evento que afecta a los objetivos. (GTC137:2011)

Evaluación del Riesgo: Proceso de comparación de los resultados del análisis del riesgo (probabilidad e impacto antes de controles), con los criterios del riesgo (valoración de controles) para determinar si el riesgo, su magnitud o ambos, son aceptables o tolerables. (GTC137:2011)

Exposición: Extensión hasta la cual una organización, una parte involucrada o ambas están sujetas a un evento. (GTC137:2011).

Frecuencia: Número de eventos o efectos por unidad de tiempo definida. (GTC137:2011)

Matriz de Valoración de Riesgos: Herramienta para la evaluación de los riesgos y su clasificación.

También se le dice matriz RAM por sus siglas en ingles. (Matriz Risk Assessment Matrix). La matriz permite calificar y evaluar los riesgos en términos de impacto y probabilidad.

Nivel de Riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad. Sumatoria de la multiplicación de la probabilidad por el impacto de todos los riesgos de un proceso o de la Institución. (GTC137:2011).

Posibilidad: Oportunidad de que algo suceda. (Likehood). (GTC137:2011).

Probabilidad: Posibilidad de que algo ocurra bien sea que se haya definido, medido, o estimado objetiva o subjetivamente, o en términos de los descriptores generales (tales como raro, improbable, probable, casi cierto). La probabilidad puede expresarse cuantitativa o cualitativamente).

Proyecto: Es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.

Programa: Un programa es una unidad lógica organizada y coherente de actividades orientada a un propósito superior.

Plan: Los planes son instrumentos de operacionalización macro, mediante los cuales la Institución ordena y organiza programas, proyectos.

Por su naturaleza temporal, tienen un principio y un final definidos. (PMBOK, 4ta. Edición).

Riesgo Inherente: riesgo al cual se enfrenta una entidad en ausencia de acciones para modificar su probabilidad o impacto.

Riesgo Residual: Remanente después del Tratamiento del Riesgo. (GTC137:2011). Es aquel que permanece aún después de desarrolladas las acciones de tratamiento del riesgo. Capacidad total de riesgo que una organización está dispuesta a aceptar, tolerar o asumir en cualquier momento dado.

Tratamiento del Riesgo: Proceso para modificar el riesgo (GTC137:2011). Conjunto de acciones que permiten a través de la creación, fortalecimiento o implementación de controles, modificar la probabilidad o el impacto de un riesgo. (Un plan de tratamiento del riesgo, puede derivar o constituirse en un proyecto y/o programa de acuerdo al tema a mitigar o mejorar).

10.3 TÉRMINOS RELATIVOS A LA FASE GESTIÓN DE RIESGOS

Acción Correctiva: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable. (ISO9000:2005).

Acción Preventiva: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable. (ISO9000:2005).

Autoridad: Poder con que se cuenta o que se ha recibido por delegación. (NTCGP1000:2009).

Corrección: Acción tomada para eliminar una no conformidad detectada. (ISO9000:2005).

Eventos Potenciales a Evaluar: Son aquellas situaciones ocurridas en un proceso que podrían llegar a ser clasificadas como riesgos materializados, pero se debe hacer un análisis previo para llegar a esa conclusión.

Eventos a Evaluar: Son aquellas situaciones que después de realizar el análisis como un evento potencial a evaluar, se consideran como riesgos materializados.

Plan de Contingencia: Las acciones o planes de contingencia garantizan que la Institución tiene la capacidad de seguir prestando sus servicios sin interrupciones o con periodos mínimos de interrupción, ante eventos inesperados como terremotos, fallas de sistemas de información, cortes del suministro de servicios públicos, inundaciones, terrorismo, atentados a funcionarios y/o instalaciones, entre otros. Deben estar previamente elaborados, socializados y aprobados para su ejecución. Estos no cuentan con un procedimiento, formato o guía para su elaboración.

Proyecto: Proceso único consistente en un conjunto de actividades coordinadas y controladas con fechas de inicio y de finalización, llevadas a cabo para lograr un objetivo conforme con requisitos específicos, incluyendo las limitaciones de tiempo, costo y recursos. (ISO9000:2005)

NOTA 1: Un proyecto individual puede formar parte de la estructura de un proyecto mayor.

NOTA 2: En algunos proyectos, los objetivos se afinan y las características del producto se definen progresivamente según evolucione el proyecto.

NOTA 3: El resultado de un proyecto puede ser una o varias unidades de producto (3.4.2).

Queja: Es la manifestación verbal o escrita de protesta, censura, descontento e inconformidad que eleva un ciudadano ante la insatisfacción que le causa la prestación del servicio de uno o varios de sus funcionarios.

Reclamo: Es el derecho que tiene toda persona de exigir, reivindicar o demandar una solución o respuesta relacionada con la prestación indebida de un servicio propio de la Policía.

Registro: Tipo de documento que da evidencia del cumplimiento de un requisito o de la realización de una actividad. Ejemplo: acta de reunión, informe de auditoría, etc.

Revisión por la Dirección: Revisión sistemática y planificada que hace la Alta Dirección del estado general del sistema, con el fin de tomar decisiones que propicien su mejora continua.

Riesgo Materializado: Ocurrencia de un evento que se había identificado como incierto.

Satisfacción del Cliente: Percepción que el cliente tiene sobre el grado en que se han cumplido sus requisitos. (ISO 9000:2005).

Sugerencia: Es la opinión o insinuación que eleva una persona para adecuar o mejorar un proceso o la prestación de un servicio policial.

10.4 TÉRMINOS RELATIVOS A LA FASE MEDICIÓN DE LA GESTIÓN

Causa Raíz: Es el origen de una falla o incumplimiento.

Control: Medida o acción que modifica el riesgo mediante la afectación ya sea de la probabilidad o del impacto. (GTC137:2011).

Plan de Tratamiento: Conjunto de acciones que se planean y se ejecutan con el fin de generar controles que eviten la materialización de un riesgo o disminuyan su impacto en caso de que ocurra. (GTC137:2011).

10.5 TÉRMINOS RELATIVOS A LA FASE DE CIERRE

Aciertos: Experiencias exitosas, aspectos que pueden ser replicables, fortalezas, logros, cumplimiento de los objetivos trazados en términos institucionales. (Lecciones Aprendidas en la Policía Nacional).

Desaciertos: Acciones / planes que no arrojaron los resultados esperados, deficiencias en la planeación, fracasos.

Lección Aprendida: Conocimiento adquirido a través de la experiencia organizacional, que analizado y difundido apropiadamente puede convertirse en acciones que lleven a la Institución a obtener mejores resultados, no repitiendo las acciones erróneas y replicando las que condujeron al éxito, considerando en todo momento un contexto de seguridad en constante transformación. (Lecciones Aprendidas en la Policía Nacional).

10.5 TÉRMINOS RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN.

Activo: Es todo aquello que posea valor para la Policía Nacional. Ejemplo: información en formato físico y/o digital; el software; el hardware; los servicios de información, de comunicaciones, de almacenamiento, etc.; las personas y otros.

Confidencialidad: Propiedad que determina que la información sea accesible sólo por quienes están autorizados.

Control: Medio para mantener el riesgo en un nivel aceptable. Los controles pueden ser administrativos, técnicos o legales y pueden materializarse en políticas, procedimientos, guías, lineamientos, prácticas y estructuras organizacionales.

Custodio: Es una parte designada de Policía Nacional la cual puede ser un cargo, un proceso o un grupo de trabajo, quien se encuentra encargado de administrar y hacer efectivos los controles de seguridad que el propietario del activo haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Disponibilidad: Propiedad de la información que define que los usuarios autorizados tengan acceso a la misma y a sus recursos asociados cuando se requiera.

Información: Datos relacionados que tienen significado para la Policía Nacional. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

Integridad: Propiedad que permite salvaguardar la exactitud y completitud de la información y sus métodos de procesamiento.

Seguridad de la Información: La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades de negocio.

Causas: Debilidad de un activo o control, que puede ser explotada por una o más amenazas.

ARTÍCULO 25. INTEGRACIÓN CON LA NORMA DE SEGURIDAD DE LA INFORMACIÓN

Este Manual establece en sus diferentes fases, los aspectos relacionados con la seguridad de la información, tanto en el ámbito de planeación como de aplicación de la norma técnica que para tal efecto se considere pertinente apropiar e implementar en la Institución, por intermedio de la Oficina de Telemática.

Parágrafo 1°: El ajuste del módulo de riesgos PRO, en virtud a la integración del tema de seguridad de la información al Manual para la Gestión Integral del Riesgo, deberá realizarlo la Oficina de Telemática, de acuerdo a las necesidades y complejidad de los requerimientos, proyectando para ello un cronograma de actualización, el cual no deberá sobrepasar los 18 meses, a partir de la expedición de este acto administrativo.

Parágrafo 2°: La única información válida por fuera del sistema, será aquella que presente la Oficina de Telemática, en los formatos estructurados para desarrollar la metodología del riesgo con base a la seguridad de la información, como aplicación de la normatividad que en este contexto lo exija. Estos formatos perderán su vigencia una vez entre en producción el módulo de riesgos con las adaptaciones realizadas de acuerdo al parágrafo anterior.

Parágrafo 3°: La apropiación, asesoramiento y entrenamiento sobre la "Gestión del Riesgo en Seguridad de la Información", será responsabilidad de la Oficina de Telemática, de acuerdo a los parámetros definidos en el artículo 23 de esta Resolución, quien nombrará a un funcionario distinto al Gestor del Riesgo de la unidad para la realización de esta actividad, en cuanto a la identificación, valoración, tratamiento, seguimiento y monitoreo de los riesgos asociados a la posibilidad de pérdida de confidencialidad, disponibilidad e integridad de la información en todos los ámbitos y/o niveles institucionales.

ARTÍCULO 26. OBLIGATORIEDAD.

El Manual adoptado mediante el presente acto administrativo, será de obligatorio cumplimiento en el desarrollo de las actividades relacionadas con la Gestión Integral del Riesgo en la Policía Nacional.

ARTÍCULO 27. VIGENCIA.

La presente Resolución rige a partir de la fecha de su expedición y deroga la Resolución No. 02069 del 28 de mayo de 2014.

Parágrafo 1°: Los documentos del Sistema de Gestión Integral que requieran ser actualizados en razón al presente documento, son responsabilidad de los dueños de procesos y contarán hasta con 3 meses de plazo después de su expedición para ser actualizados en el listado maestro de documentos.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C.

Original firmado
General **JORGE HERNANDO NIETO ROJAS**
Director General Policía Nacional de Colombia

Elaboró: IT. Manuel Salvador Gallego Polo
Revisó: CT. Carlos Antonio Ardila Quintero
TC. Olga Lucia Hernández Benavides
Aprobó: BG. Fabián Laurence Cárdenas Leonel
Fecha: 21/06/2016