MANUAL DE ADMINISTRACION DE RIESGOS Y OPORTUNIDADES

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Andrey Rodriguez Rodriguez	**NOMBRE:** Martha Eugenia Cortés Baquero Jaime Rafael Morón Barros Cesar Adolfo Gonzalez Peña Ronald Oswaldo Duarte Rodriguez	**NOMBRE:** Martha Eugenia Cortés Baquero
CARGO: Profesional Defensa	**CARGO:** Jefe de la Oficina Asesora Jurídica Jefe Oficina Asesora e Innovación Institucional Coordinador Grupo Redes e Infraestructura encargado de las funciones de la Oficina TIC Coordinador Desarrollo Organizacional y Gestión Integral - OAPII	**CARGO:** Jefe de la Oficina Asesora jurídica encargada de las funciones del Despacho de la Dirección General de la Agencia Logística de las Fuerzas Militares
FIRMA:	**FIRMA:**	**FIRMA Y FECHA DE APROBACIÓN:** 30 06 2026

TABLA DE CONTENIDO

INTRODUCCIÓN

La Gestión del Riesgo constituye un proceso esencial liderado por la Alta Dirección de la Agencia Logística de las Fuerzas Militares, en el que la participación y compromiso de todo el personal son fundamentales para proporcionar a la administración una seguridad razonable en la consecución de los objetivos institucionales. Este enfoque va más allá de la mera aplicación de una metodología; su éxito radica en integrar la evaluación integral de riesgos de manera natural en el proceso de planificación.

La Institución demuestra su capacidad para afrontar los eventos que podrían afectar adversamente la consecución de sus metas y salvaguardarse de los efectos derivados de su ocurrencia. En este contexto, la Norma Técnica NTC-ISO 31000 destaca que la eficiencia del control reside en la gestión de los riesgos. En otras palabras, el propósito principal del control es prevenir o reducir riesgos, asegurando que el proceso y sus controles minimicen o reduzcan los riesgos de manera razonable, garantizando así el logro de los objetivos institucionales.

La Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública (DAFP), incorpora los elementos necesarios según el Modelo Integrado de Planeación y Gestión (MIPG). Este modelo integra sistemas de gestión de calidad y desarrollo administrativo, conformando un sistema de gestión único alineado con los estándares internacionales, como el modelo de las tres líneas de defensa. Este enfoque busca ofrecer a los ciudadanos una gestión de alta calidad, generar cambios significativos en las condiciones de vida y fortalecer la lucha contra el fraude y la corrupción.

La Administración del Riesgo, como herramienta establecida, se concibe para minimizar, monitorear y mitigar riesgos, evitando la propagación de sus efectos, bajo los principios de calidad, eficiencia, economía y eficacia. La gestión del riesgo establece pautas precisas para el tratamiento, manejo y seguimiento de los riesgos para los funcionarios de la Agencia Logística de las Fuerzas Militares.

OBJETIVO DEL MANUAL

Establecer la política y lineamientos orientadores para las acciones frente a administración del riesgo en la Agencia Logística de las Fuerzas Militares, que conduzcan a disminuir la vulnerabilidad frente a situaciones que puedan interferir y afectar total o parcialmente la operación y el cumplimiento de sus funciones y en el logro de sus objetivos institucionales.

1. ALCANCE

La administración de riesgos en la Agencia Logística de las Fuerzas Militares, tendrá un carácter prioritario y estratégico, fundamentado en el modelo de operación por procesos, fomentando la cultura del autocontrol al interior de los procesos, la cual debe ser aplicada por todos los responsables o líderes de los procesos determinados en la caracterización de cada uno de estos y funcionarios de la Agencia Logística de las Fuerzas Militares, de acuerdo con las responsabilidades definidas en el presente documento. Así mismo, integrando los parámetros que son requeridos para la implementación del MIPG.

2. REFERENCIA NORMATIVA

A continuación, se encontrarán establecidas las normas nacionales e internacionales que rigen el proceso de Administración del Riesgo, para las entidades del sector público.

Tabla 1.
Normatividad aplicable a la gestión de riesgo

Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 Objetivos del control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
Ley 489 de 1998	Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno.
Ley 1474 de 2011. Estatuto Antifraude o corrupción	Art. 73. Modificador por el Art. 31 de la Ley 2195 de 2022 Plan Antifraude o corrupción y de Atención al Ciudadano: Señala la obligatoriedad para cada entidad del orden nacional, departamental y municipal de elaborar anualmente una estrategia de lucha contra la fraude o corrupción y de atención al ciudadano; siendo uno de sus componentes el Mapa de Riesgos de Fraude o corrupción y las medidas para mitigar estos riesgos. Al Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Fraude o corrupción, -hoy Secretaría de Transparencia-, le corresponde diseñar la metodología para elaborar el Mapa de Riesgos de Fraude o corrupción.
Ley 1712 de 2014 Ley de Transparencia y de Acceso a la Información Pública	Art .9°. Literal g) Deber de publicar en los sistemas de información del Estado o herramientas que lo sustituyan el Plan Antifraude o corrupción y de Atención al Ciudadano.
Ley 2195 de 2022	PROGRAMAS DE TRANSPARENCIA Y ETICA EN EL SECTOR PUBLICO. Modifíquese el Artículo 73 de la Ley 1474 de 2011, … b) Prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno Nacional dentro del año siguiente a la expedición de esta norma. Articulo 31 literal b.

Decreto 2145 de 1999	*Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art. 8º. de la ley 1474 de 2011).*
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 de las entidades y organismos del Estado. El parágrafo del Artículo 4º señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (…) y en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su Artículo 4º la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…).*
Decreto 1599 de 2005	*Por el cual se adopta el Modelo Estándar de Control Interno para el Estado colombiano y se presenta el anexo técnico del MECI 1000:2005. 1.3 Componentes de administración del riesgo.*
Decreto 4637 de 2011 Suprime y crea una Secretaría en el DAPRE	*Art. 4°. Suprime el Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Fraude o corrupción.*
	Art. 2°. Crea la Secretaría de Transparencia en el Departamento Administrativo de la Presidencia de la República.
Decreto 943 de 2014 MECI	Art. 1 ° y siguiente. Adopta la Actualización del MECI.
Decreto 1649 de 2014 Modificación de la estructura del DAPRE	*Art. 55. Deroga el Decreto 4637 de 2011.*
	Art .15. Funciones de la Secretaría de Transparencia: 13) Señalar la metodología para diseñar y hacer seguimiento a las estrategias de lucha contra la fraude o corrupción y de atención al ciudadano que deberán elaborar anualmente las entidades del orden nacional y territorial.
Decreto 1081 de 2015 Único del Sector de la Presidencia de la República	*Art .2.1.4.1 y siguientes. Señala como metodología para elaborar la estrategia de lucha contra la fraude o corrupción la contenida en el documento "Estrategias para la construcción del Plan Antifraude o corrupción y de Atención al Ciudadano."*
Decreto 1083 de 2015 Único Función Pública	*Art. 2.2.22.1 y siguientes. Establece que el Plan Antifraude o corrupción y de Atención al Ciudadano hace parte del Modelo Integrado de Planeación y Gestión.*
	Art. 2.2.21.6.1. Adopta la actualización del Modelo Estándar de Control Interno para el Estado Colombiano (MECI).
Decreto 1499 de 2017	*Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015*
Decreto 612 de 2018	*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.*
NTC ISO 9001:2015	*Numeral 6 Planificación 6.1. Acciones para abordar riesgos y oportunidades*
NTC ISO 14001:2015	*Numeral 6 Planificación 6.1. Acciones para abordar riesgos y oportunidades*
NTC ISO 45001:2018	*Numeral 6 Planificación 6.1. Acciones para abordar riesgos y oportunidades*
NTC - ISO 31000:2018	*Ofrece principios y directrices genéricas sobre gestión de riesgos*
NTC ISO 27001:2022	*Numeral 6 Planificación 6.1. Acciones para abordar riesgos y oportunidades*
Directiva Presidencial 09 de 1999	*Lineamientos para la implementación de la Política de Lucha contra la Fraude o corrupción.*
Manual Operativo del MIPG V6 diciembre de 2024	*Dimensión 2. Direccionamiento estratégico y Planeación - Política Planeación Institucional incluye la formulación de lineamientos para la administración del riesgo. Política de Seguridad Digital: La implementación de la política, se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital*
Guía de riesgos DAFP V7 de 2025	*Guía para la administración del riesgo y el díselo de controles en entidades publicas*

3. DEFINICIONES

Tabla 2.
Definiciones en gestión de riesgo

Activo	En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
Administración de Riesgo	Es la capacidad que tiene la Institución para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
Amenaza	Situación que potencialmente cause pérdidas
Análisis de riesgos	Determinar el impacto y la probabilidad del riesgo. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos. (ISO/IEC 27000).
Apetito de riesgo	Es el nivel de riesgo que una Entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la Alta Dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe gestionar.
Autocontrol	Es la capacidad que tiene cada servidor público, independientemente de su nivel jerárquico dentro de la Institución, para evaluar su trabajo, detectar desviaciones, efectuar correctivos, mejorar y solicitar ayuda cuando lo considere necesario, de tal manera que la ejecución de los procesos, actividades y tareas bajo su responsabilidad garanticen el ejercicio de una función administrativa transparente y eficaz.
Bien público	Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así: a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. *Ejemplos: Las calles, plazas, puentes, vías, parques etc.* b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. *Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.*
Capacidad de riesgo	Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la Alta Dirección considera que no sería posible el logro de los objetivos de la entidad. (relacionado con la solvencia y liquidez).
Causa	Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Causa Inmediata	Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata.
Causa Raíz	Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. *Nota: Denominada Causa Eficiente o Causa Adecuada: Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. La causa raíz se asocia con aquel hecho potencial generador del daño.*
Cliente	Organización, entidad o persona que recibe un producto y/o servicio.
Colocación	es la disposición del dinero proveniente de actividades delictivas. Durante esta fase inicial, el determinador o autor introduce sus fondos ilegales en actividades legales o aparentemente legales, bien a través del sistema financiero o de otros tipos de negocios o contratos, tanto nacionales como internacionales.
Confidencialidad	Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Conflicto de interés	Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un

	interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011)
Consecuencia	Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. *Nota:* Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.
Control	Medida que permite reducir o mitigar un riesgo.
Contexto Externo	Entorno externo en el que la organización busca alcanzar sus objetivos, el contexto externo puede incluir: La cultural, social, político, jurídico, reglamentario, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local; Factores clave y las tendencias con repercusiones en los objetivos de la organización, y la relaciones con, y las percepciones.
Contexto Interno	Ambiente interno en el que la organización busca alcanzar sus objetivos, el contexto interno puede incluir: Gobernanza, la estructura organizativa, las funciones y responsabilidades; Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos
Control Preventivo	Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
Control Correctivo	Aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia.
Compartir el Riesgo	Cambiar la responsabilidad o carga por las pérdidas que ocurran luego de la materialización de un riesgo mediante legislación, contrato, seguro o cualquier otro medio.
Consecuencia	Efectos que podrían generarse en la Entidad con la materialización de un riesgo
Contraparte	Cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización.
Corrupción	Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015)
Debida diligencia (due dilligence)	Proceso que deben llevar a cabo las entidades para identificar, prevenir, mitigar y explicar cómo abordan los impactos negativos reales y potenciales en sus propias actividades, su cadena de suministro y otras relaciones comerciales.
Debida diligencia (debida diligencia del cliente):	Proceso que le permite a la entidad conocer aspectos relevantes de sus contrapartes, sean partes vinculadas o relacionadas, para poder gestionar el riesgo que cualquier vinculación o relacionamiento genera.
Delito fuente	según el artículo 323 de la Ley 599 de 2000, son delitos fuente del lavado de activos: tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, contrabando, contrabando de hidrocarburos o sus derivados, fraude aduanero o favorecimiento y facilitación del contrabando, favorecimiento de contrabando de hidrocarburos o sus derivados, en cualquiera de sus formas.
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Enfoque basado en procesos	Identificación y gestión sistemática de los procesos empleados en las entidades.
Evaluación del Riesgo	Proceso utilizado para determinarlas prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
Evento	Incidente o situación, que ocurre en un lugar determinado durante un periodo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.
Factores de Riesgo	Son las fuentes generadoras de riesgos.

Financiación de la Proliferación de Armas de Destrucción Masiva (FP)	fondos u otros activos a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del Consejo de Seguridad de las Naciones Unidas dentro del Capítulo VII de la Carta de las Naciones Unidas, en lo relativo a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento. La Financiación de la Proliferación puede darse por: recaudación, transmisión, utilización
Financiación del Terrorismo (FP)	el artículo 345 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien *"directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas"*. La Financiación del Terrorismo puede darse por: recaudación, transmisión, utilización.
Frecuencia	Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
Fraude	errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025)
Función de cumplimiento	función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública.
Gestión del Riesgo Fiscal	son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
Gestor Fiscal	Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)". *Ejemplo: entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.*
Gestor público	Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales. *Ejemplo: además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.*
Identificación del Riesgo	Elemento de Control que posibilita conocer los eventos potenciales, estén o no bajo el control del a Entidad Pública, que ponen en riesgo el logro de su Misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite.
Impacto	Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Indicador	Es la valoración de una o más variables que informa sobre una situación y soporta la toma de decisiones, es un criterio de medición y de evaluación cuantitativa o cualitativa.
Integración	es dar apariencia legítima a riqueza ilícita mediante el reingreso en la economía con transacciones comerciales o personales que aparentan ser normales. Esta fase conlleva la colocación de los fondos lavados de vuelta en la economía para crear una percepción de legitimidad. El lavador podría optar por invertir los fondos en bienes raíces, artículos de lujo o proyectos comerciales, entre otros.
Integridad	Propiedad de exactitud y completitud.
Intereses patrimoniales de	Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los

naturaleza pública	intereses patrimoniales de naturaleza pública son expectativas.
Lavado de activos	el artículo 323 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien *"adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades [relacionadas con un delito fuente], o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito"*. El Lavado de Activos puede darse por: colocación, ocultamiento e integración.
Materialización	Evento mediante el cual los riesgos identificados y evaluados se convierten en eventos reales que afectan el logro de los objetivos de la entidad. Es decir, es el momento en el cual un riesgo identificado se manifiesta y tiene un impacto real en las operaciones, proyectos o actividades.
Mapa de Riesgo	Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.
Mitigación	Planificación y ejecución de medidas dirigidas a reducir o disminuir el riesgo
Monitorear	Comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.
Nivel de Riesgo	Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
Parte Interesada	Es un tipo de contraparte con la cual no se ha establecido ninguna relación o vinculo, pero que ha manifestado formalmente su interés en establecerlo.
Parte Relacionada	Para efectos del SIGRIP, es una contraparte independiente de la organización con la cual se ha establecido una relación comercial, contractual o legal; o respecto de la cual se ejerce algún grado de control jerárquico, de tutela o de propiedad, sin detrimento de su independencia.
Parte Vinculada	Para efectos del SIGRIP, es una contraparte dependiente de la organización con la cual se ha establecido una relación de especial de sujeción por su relación legal o reglamentaria, o laboral.
Patrimonio Público	Se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).
Pérdida	Consecuencia negativa que trae consigo un evento.
Perfil de Riesgo	En términos generales, el perfil de riesgo se refiere a la descripción detallada de los riesgos a los que está expuesta una organización, proyecto o actividad en particular. El perfil de riesgo proporciona información esencial sobre los diferentes riesgos identificados, su probabilidad de ocurrencia, su impacto potencial y otros atributos relevantes.
Plan Anticorrupción y de Atención al Ciudadano	Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
Política de Administración de Riesgos	Identifican las opciones para tratar y manejar los riesgos basadas en la valoración de los mismos, permiten tomar decisiones adecuadas y fijar los lineamientos, que van a transmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.
Probabilidad	Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
Proceso de Administración del Riesgo	Aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la Administración del Riesgo.
Punto de Riesgo	Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Nota: Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo:

	Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas
Ocultamiento	Es la separación de fondos ilícitos de su fuente mediante una serie de transacciones, cuyo fin es desdibujar la transacción ilícita original. Esta etapa supone la conversión de los fondos procedentes de actividades ilícitas a otra forma y crear esquemas complejos de transacciones financieras para disimular el rastro documentado, la fuente y la propiedad de los fondos.
Recaudación	Consiste en la búsqueda de fuentes de financiación por las organizaciones terroristas, bien sean de origen legal, como los aportes de los Estados, individuos, entidades, organizaciones y donantes en general que apoyan su causa o son engañados, así como recursos provenientes de cualquier actividad delictiva, fondos que generalmente circulan en efectivo.
Reducción del Riesgo	Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia
Recurso Público	Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.
Riesgo	Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
Riesgo de Fraude o Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgo de Seguridad de la Información	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)
Riesgos para la Integridad	Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas
Riesgo Inherente	Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de Severidad.
Riesgo Residual	El resultado de aplicar la efectividad de los controles al riesgo inherente.
Riesgo Fiscal	Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. *Nota: ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública.*
Riesgo Reputacional	La posibilidad de que una organización sufra daños en su reputación, imagen o prestigio, lo que puede derivar en la pérdida de clientes, ingresos, e incluso en procesos legales.
Sistema de Administración de Riesgo	Conjunto de elementos del direccionamiento estratégico de una entidad concerniente a la Administración del Riesgo.
Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP	Esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos.
SIG	Sistema Integrado de Gestión
Soborno	ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar. (A partir de ISO37001:2025)
Soborno entrante	ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad.
Soborno saliente	ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la entidad.
Tolerancia del Riesgo	Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
Transmisión	Es la fase intermedia que busca poner el dinero recaudado a disposición de la organización terrorista, quedando simplemente la espera de su utilización final; corresponde al movimiento de los fondos a través de distintas técnicas, se trata de ocultar sus movimientos y destino final.
Utilización	fase donde los fondos se utilizan básicamente para la financiación de la logística estructural de la organización o la logística operativa en materia de planeación y ejecución de actos terroristas.
Valoración del	Es el resultado de confrontar la evaluación del riesgo con los controles existentes.

Riesgo:	
Valoración después de Controles	Grado de exposición al riesgo con la calificación de probabilidad e impacto aplicando los controles existentes (valoración residual).
Vulnerabilidad	Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
Zona de riesgo	Es el nivel de exposición al riesgo, hallado mediante el cruce entre la probabilidad y el impacto.

4. CUERPO DEL MANUAL

4.1. POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

Enunciado de la Política

La Agencia Logística de las Fuerzas Militares, en el marco de sus objeto y funciones reglamentarias, se compromete a establecer un enfoque preventivo de evaluación permanente de la gestión, control, y mejoramiento continuo en la gestión de riesgos. Aplicando la identificación, valoración, tratamiento, monitoreo, comunicación, consulta y el análisis de estos, buscando articular aquellos que involucran la gestión general, la gestión preventiva de riesgos fiscales, la gestión en seguridad de la información y aquellos que afectan la Integridad pública.

Esta política tiene como propósito fortalecer la gobernanza, la toma de decisiones informadas y la generación de valor público, asegurando la integridad, transparencia y eficacia en la administración de recursos al igual de promover una cultura organizacional orientada a la anticipación y gestión proactiva de los riesgos, contribuyendo al cumplimiento de la misión institucional, la mejora continua, la confianza ciudadana y contar con un sistema de gestión que le permita prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), de manera integral.

4.2. OBJETIVOS DE LA GESTIÓN INTEGRAL DE RIESGOS.

Definir y aplicar un método que facilite identificar, analizar y valorar los riesgos de manera permanente.

Identificar los procesos y actividades que pueden ser afectados por eventos potenciales para el logro de los objetivos.

Identificar los riesgos de los procesos a fin de implementar el mapa de riesgos institucional y las acciones de mitigación.

Proteger los recursos de la entidad, buscando su adecuada administración ante posibles riesgos que los puedan afectar.

Establecer controles en el marco de la gestión de riesgos de integridad pública que promuevan un enfoque preventivo y la naturalización de la cultura de la legalidad al interior de la Entidad.

4.3.SOPORTE METODOLÓGICO

Para la elaboración del Mapa de riesgos en todos sus niveles de despliegue, la Agencia Logística de las Fuerzas Militares, se rige por los parámetros y lineamientos metodológicos que sobre la materia imparta el Departamento Administrativo de la Función Pública – DAFP-, en concordancia con el Modelo Estándar de Control Interno –MECI, adaptando estos a la cultura organizacional institucional y el esquema de procesos definido para la ALFM.

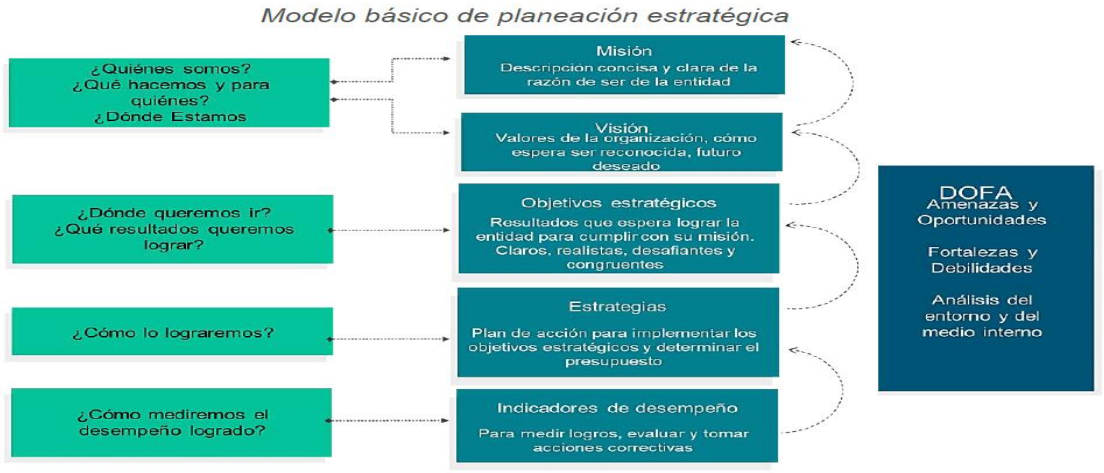
4.3.1. Análisis Estratégico de la Entidad

La gestión integral de riesgos, es posible definirla como "la cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en la que la Entidad confía para gestionar el riesgo, de cara la creación, preservación y materialización de valor, esto implica que la gestión se consolida a través de:

El reconocimiento de la cultura
El desarrollo de capacidades
El uso de las técnicas aplicadas
La integración de la estrategia y el desempeño
La alineación con la estrategia y objetivos clave
La relación con el valor

La planeación estratégica en el ámbito público es un instrumento que ayuda al establecimiento de prioridades, objetivos y estrategias como apoyo a la definición de los recursos que se requieren para lograr los resultados esperados.

Figura 1.
Modelo Planeación.



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desarrollo hacia los objetivos de los procesos, los cuales deben quedar incorporados en las caracterizaciones de cada uno de

estos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características SMART.

Figura 2.
Características SMART.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

4.3.2.Niveles de Madurez para la Gestión del Riesgo

Teniendo en cuenta que la gestión estratégica del riesgo involucra una serie componentes y elementos que se deben fortalecer desde la cultura organizacional, se hace necesario evaluar su nivel de madurez. Para este efecto, atendiendo uno de los marcos que sustentan el desarrollo del presente manual que corresponde al COSO-ERM-2017 se propone una estructura que, "*consta de cinco componentes interrelacionados de la gestión del riesgo empresarial y su relación con la misión, visión y valores clave de la entidad*". Tal como se ilustra en la siguiente imagen.

Figura 3.
COSO-ERM.

Elaborado por Grupo DOGI –2026

Los cinco componentes que integran una óptima gestión del riesgo a la luz de este marco de referencia, se describen a continuación:

Gobierno y Cultura: Juntos forman una base para todos los demás componentes de la gestión del riesgo. El gobierno marca la pauta de la entidad, reforzando la importancia de la gestión del riesgo y estableciendo responsabilidades de supervisión al respecto. La cultura se refleja en la toma de decisiones.

Establecimiento de la estrategia y objetivos: Se integra en el plan estratégico de la entidad a través del proceso de establecimiento de la estrategia y de los objetivos estratégicos institucionales de la Entidad.

Desempeño: Identifica y evalúa los riesgos que pueden afectar la capacidad de la entidad para alcanzar la estrategia y los objetivos de los procesos.

Revisión y monitorización: Examina las capacidades y técnicas de gestión del riesgo, y el desempeño de la entidad en relación con sus objetivos.

Información, Comunicación y Reporte: La comunicación es el proceso continuo e interactivo de obtener y compartir información en toda la entidad.

Bajo este marco, para el análisis de niveles de madurez se propone un esquema de diagnóstico que analiza los componentes y principios que desarrolla el modelo COSO-ERM, a partir de una serie cuestiones o puntos de reflexión.

Figura 4.
Modelo Madurez

Componentes y principios evaluables modelo de madurez

Componente	Principios
Gobierno y Cultura	Supervisión de riesgos a través del consejo de administración.
	Establece estructuras operativas
	Define la cultura deseada
	Demuestra compromiso con valores clave
	Atrae, desarrolla y retiene a profesionales capacitados
Establecimiento de la estrategia y objetivos	Analiza el contexto (externo e interno)
	Define el apetito del riesgo
	Evalúa estrategias alternativas
	Formula objetivos estratégicos y operacionales
Desempeño	Identifica y describe el riesgo
	Evalúa el riesgo inherente
	Diseña controles efectivos
	Prioriza riesgos
	Desarrolla visión integral
Análisis y monitorización	Evalúa los cambios significativos
	Revisa el riesgo y el desempeño
	Persigue la mejora de la gestión del riesgo
Información, Comunicación y Reporte	Aprovecha la información y la tecnología
	Comunica información sobre riesgos
	Informa sobre el riesgo, la cultura y el desempeño

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

Una vez calificados los principios por cada uno de los componentes, a partir de los puntos de reflexión que se plantean en la herramienta **Matriz estado de madurez de la Gestión del Riesgo** con un esquema de preguntas orientadoras, se establecerá el grado de madurez para la gestión del riesgo en el que se ubica la entidad.

La Oficina Asesora de Planeación e Innovación Institucional será la responsable de realizar el diagnóstico, dejando registro en la Matriz definida por el Departamento de la Función Pública al menos una vez al año.

4.3.3. *Esquema de Líneas de defensa*

A. Línea Estratégica

Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos desde de una adecuada gestión de riesgos con relación a lo siguiente:

a. **Revisar los cambios en el "Direccionamiento Estratégico"** y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
b. **Revisar el adecuado desdoblamiento de los Objetivos Institucionales** a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.
c. **Hacer seguimiento en el Comité Institucional de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno** a la implementación de cada una de las etapas (identificación, evaluación, tratamiento, monitoreo y comunicación) de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.
d. **Revisar la posible materialización de Riesgos** en el cumplimiento de los objetivos institucionales y de procesos e indicadores, identificando por qué no se estén cumpliendo. Esta acción puede realizarse mediante presentaciones del comité de coordinación de control interno o mediante informes de seguimiento elaborados fruto de las evaluaciones realizadas a los procesos.
e. **Hacer seguimiento y pronunciarse por lo menos cada año** sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de fraude o corrupción de acuerdo a los lineamientos establecidos en este manual.
f. **Revisar los informes presentados por lo menos cada cuatrimestre** por parte de la tercera línea de defensa acerca de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de fraude o corrupción, así como las causas que dieron origen los eventos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
g. **Revisar los planes de contingencia** establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

B. Primera Línea de Defensa

Esta línea de defensa les corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad. Se debe precisar que cuando se trate de servidores que ostenten un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controles de gerencia operativa, ya que son aplicados por líderes o responsables de proceso.

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los líderes de los procesos, programas y proyectos de la entidad.

El modelo de operación de la entidad se conforma de doce procesos, por tanto, cada líder de proceso debe monitorear y revisar el cumplimiento de los objetivos instituciones a través de una adecuada gestión del riesgo, incluyendo los riesgos de fraude o corrupción con relación a lo siguiente:

a. **Identificación de Riesgos:** Los funcionarios de la primera línea de defensa son responsables de identificar los riesgos asociados con las actividades y procesos que ejecutan. Esto implica la identificación temprana de los riesgos potenciales, ya sea a través de la observación directa, la recopilación de información o el análisis de datos relevantes.
b. **Evaluación de Riesgos:** La primera línea de defensa debe evaluar la probabilidad de ocurrencia y el impacto potencial de los riesgos identificados. Esto implica analizar la información disponible, evaluar los controles existentes y determinar la magnitud de los riesgos en relación con los objetivos y metas establecidos.
c. **Implementación de Controles:** Los funcionarios de la primera línea de defensa deben implementar controles adecuados para mitigar o manejar los riesgos identificados. Esto implica establecer y seguir políticas, procedimientos y prácticas operativas que reduzcan la probabilidad de ocurrencia de los riesgos y minimicen su impacto en caso de que se materialicen.
d. **Monitoreo de Riesgos:** La primera línea de defensa es responsable de monitorear continuamente los riesgos en el desarrollo de las actividades y procesos. Esto implica establecer mecanismos de seguimiento y vigilancia para identificar cambios en los riesgos, evaluar la efectividad de los controles implementados y tomar acciones correctivas o preventivas según sea necesario.
e. **Reporte de Riesgos:** Los funcionarios de la primera línea de defensa deben informar regularmente sobre los riesgos identificados, las medidas de control implementadas y los resultados del monitoreo. Esto implica generar informes periódicos, comunicar los riesgos relevantes a los niveles superiores de la organización y colaborar con otras líneas de defensa en la gestión integral de riesgos.

C. Segunda Línea de Defensa

Esta línea de defensa está conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.

Aquí se incluyen a los jefes de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC, entre otros que se deberán definir acorde con la complejidad y misionalidad de cada organización. Esto le permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica).

Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos.

En el contexto particular de la gestión de riesgo para la ALFM se encuentra dividida en tres partes, estratégica, táctica y operacional.

a. Gestión Estratégica de Riesgos: Se centra en el nivel más alto de la organización y se relaciona con la dirección estratégica y la toma de decisiones a largo plazo. En este nivel, se definen los objetivos estratégicos de la organización y se identifican los riesgos clave que podrían afectar su capacidad para lograr esos objetivos. La gestión estratégica de riesgos implica:

- Identificar y evaluar los riesgos estratégicos que podrían afectar la visión y los objetivos de la organización.
- Definir las políticas y estrategias de gestión de riesgos a nivel organizacional.
- Establecer un marco de gestión de riesgos que guíe la toma de decisiones estratégicas.
- Asignar responsabilidades para la gestión de riesgos en toda la organización.
- Monitorear y revisar regularmente los riesgos estratégicos y ajustar las estrategias de gestión de riesgos en consecuencia.

b. Gestión Táctica de Riesgos: Se enfoca en la implementación de las estrategias y políticas establecidas en el nivel estratégico. En este nivel, se desarrollan planes y acciones específicas para abordar los riesgos identificados y garantizar que se cumplan los objetivos estratégicos. La gestión táctica de riesgos implica:

- Desarrollar acciones para ser documentadas a través de la herramienta dispuesta con el fin de gestionar los riesgos identificados.
- Establecer y asignar recursos para implementar medidas de control y mitigación de riesgos.
- Supervisar y evaluar el progreso de las acciones de gestión de riesgos tácticas.
- Realizar revisiones periódicas para asegurar la efectividad de las medidas implementadas.
- Informar a la dirección sobre el estado y el impacto de los riesgos tácticos gestionados.

c. Gestión Operacional de Riesgos: Se enfoca en los procesos y actividades diarias de la organización. En este nivel, se implementan y ejecutan las acciones de gestión de riesgos tácticas y se asegura el cumplimiento de los controles y procedimientos establecidos. La gestión operacional de riesgos implica:

- Ejecutar las acciones de gestión de riesgos establecidas en el nivel táctico.
- Monitorear y controlar los riesgos operacionales en tiempo real.
- Implementar y mantener controles internos efectivos en los procesos y actividades operacionales.
- Reportar incidentes y desviaciones de riesgos a la línea de gestión superior.
- Realizar revisiones y auditorías operativas para identificar áreas de mejora y asegurar el cumplimiento de los controles.

La segunda línea de defensa es la encargada de asistir y guiar a la línea estratégica y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de fraude o corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.

La Oficina Asesora de Planeación e Innovación Institucional realizara una validación muestral de las tareas gestionadas en el plan de Mitigación aleatoriamente dejando como registro un informe de lo identificado en dicha revisión. Esta revisión no estará sujeta al contenido técnico de las tareas, sino a la coherencia entre formulado y ejecutado.

El jefe de la Oficina Asesora de Planeación e Innovación Institucional, monitoreará al menos una vez al año los riesgos institucionales revisando el cumplimiento de los objetivos institucionales y de procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de fraude o corrupción, con relación a lo siguiente:

- El componente estratégico de la segunda línea de defensa es el responsable, junto con la línea estratégica, de revisar los cambios en el Direccionamiento Estratégico o en el entorno de la entidad, cambios en los componentes táctico y operacional y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
- Revisar el adecuado ajuste de los objetivos institucionales a los objetivos de procesos, y que los mismos se hayan tenido en cuenta como base para llevar a cabo la identificación de los riesgos.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
- Los componentes tácticos y operacionales de la segunda línea de defensa harán seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos y que las mismas se encuentren documentadas y actualizadas en los

procedimientos. Presentar informe u observación documentada a la primera línea de defensa sobre las observaciones encontradas en caso de ser requerido.
- Revisar los planes de contingencia establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

Corresponde al área encargada de la gestión del riesgo la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

Adicionalmente se definen responsabilidades Oficina Tecnologías de la Información y las Comunicaciones (TIC), perteneciente a la segunda línea de defensa, la cual será la encargada en el marco de la seguridad de la información de:

- Liderar, asesorar y acompañar a los procesos en la identificación y actualización de los activos de información, así como el análisis de vulnerabilidades y amenazas propio de los mismos.
- Analizar y mantener documentados los diferentes controles asociados a los activos de información que serán ejecutados en el marco de la gestión de riesgos de seguridad de la información, con el acompañamiento de la Oficina Asesora de Planeación e Innovación Institucional.
- Asegurar la protección de los activos de información que la oficina tenga a cargo que sean accesibles a proveedores o terceros con los que la Entidad tenga contratos o convenios.
- Generar el conocimiento necesario dentro de la entidad y sensibilizar a los funcionarios sobre la importancia de preservar y mantener integra la información y su responsabilidad sobre el adecuado uso en todo lo relacionado con activos de información, su criticidad, y riesgos de seguridad de la información.
- Presentar ante el Comité Institucional de Gestión y Desempeño los resultados del análisis de activos de información generado con los procesos y las necesidades de ajustes o cambios al mismo.
- Identificar los riesgos, las amenazas y vulnerabilidades inherentes a la seguridad de la información.
- Elaborar y actualizar Planes de Tratamiento de Riesgos e indicadores de seguridad de la información.
- Elaborar y actualizar el Manual del Plan de Contingencia Informática y Plan de Continuidad del Negocio ante la ocurrencia o materialización de riesgos.
- Monitoreo y revisión de los controles a los riesgos identificados para los temas relacionados a la seguridad de la información.
- Informar a la Oficina Asesora de Planeación e Innovación Institucional por medio de mesas de trabajo para la actualización de riesgos, cuando sea necesario, los niveles o valoraciones de los Riesgos de seguridad de la información.

D. Tercera Línea de Defensa

Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad de la gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el

cumplimiento de los objetivos institucionales y de proceso, así como los riesgos oficiados al fraude o corrupción. Está conformada por la Oficina de Control Interno o Auditoría Interna y se encargará de lo siguiente:

- **Auditoría interna:** La tercera línea de defensa corresponde a la función de auditoría interna en la organización. Su responsabilidad principal es evaluar de manera independiente y objetiva la eficacia de los controles internos y la gestión de riesgos en toda la entidad.
- **Evaluación de cumplimiento:** La tercera línea de defensa también es responsable de evaluar el cumplimiento de las leyes, regulaciones, políticas y procedimientos aplicables en la organización. Esto implica verificar si se están cumpliendo los requisitos legales y normativos en la gestión de riesgos.
- **Informes y recomendaciones:** La tercera línea de defensa elabora informes sobre los hallazgos de auditoría y evaluación de cumplimiento, y proporciona recomendaciones para mejorar la gestión de riesgos y el sistema de control interno. Estos informes se comparten con la alta dirección y otras partes interesadas relevantes.

NOTA: Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar periódicamente la gestión de riesgos y si es del caso ajustarlo, (primera línea de defensa). Le corresponde, igualmente a la Oficina Asesora de Planeación e Innovación Institucional adelantar el seguimiento (segunda línea de defensa). Para este propósito se cuenta con la herramienta SVE. Adicional se realizará un monitoreo el cual se realizará según lo establecido por la Oficina Asesora de Planeación e Innovación Institucional en el presente documento y realizado por el responsable de cada proceso (primera línea de defensa). Su importancia radica en la necesidad de monitorear la gestión del riesgo y la efectividad de los controles establecidos. Teniendo en cuenta que el fraude o corrupción es, por sus propias características, una actividad difícil de detectar.

Figura 5.
Responsabilidades Gestión del Riesgo.

Línea de Defensa	Responsable	Responsabilidad
Línea Estratégica 	Alta Dirección	Evaluar el estado del Sistema de Control Interno, Aprobar la Política de Riesgos Institucional.
Primera Línea 	Funcionarios ALFM en todos los niveles	Definir y aplicar los controles para la mitigación de riesgos, reportando su gestión en los planes o registros definidos por la Entidad.

Segunda Línea 	Líderes de proceso, Oficina Asesora de Planeación e Innovación Institucional	Definir y consolidar los riesgos institucionales, realizando monitoreo periódico.
Tercera Línea 	Oficina de Control Interno	Adelantar ejercicios de auditoría basada en riesgos y retroalimentar los resultados en los comités institucionales de coordinación de control interno.

Elaborado por Grupo DOGI –2026

Tabla 3.
Funciones de las áreas organizativas

RESPONSABLE	FUNCIÓN
Alta Dirección	Establecer la metodología para Riesgos Realizar seguimiento por medio de los comités institucionales.
Secretario General, Subdirectores Generales, Jefes de Oficina, Directores Nacionales, Directores Regionales y Responsables de Procesos	Identificar los riesgos, controles de procesos y proyectos a cargo en cada vigencia. Realizar seguimiento y análisis a los controles y actividades asociadas de los riesgos según periodicidad establecida en la herramienta SVE. Actualizar de manera oportuna el mapa de riesgos cuando la administración de los mismos lo requiera.
Oficina Asesora de Planeación e Innovación Institucional	Acompañar y orientar sobre la metodología para el análisis, calificación y valoración de los Riesgos. Consolidar el Mapa de riesgos de la entidad.
Todos los funcionarios	Participarán en la realización e implementación del Mapa de Riesgos de los Procesos en los cuales participan, poniendo en práctica los principios y valores éticos de la Agencia Logística de las Fuerzas Militares, en materia de manejo de recursos y de autocontrol.
Oficina de Control Interno	Realiza e informar los resultados de las auditorias basadas en Riesgos y los seguimientos a estos.

Nota: Funciones de las áreas Organizativas – Elaborado por Grupo DOGI –2026

4.3.4.Esquema Metodológico Aplicable

Con base en los lineamientos emitidos por el Departamento administrativo de la Función Pública la Agencia Logística de las Fuerzas Militares dispone de un instrumento de identificación de riesgos que contendrá los siguientes aspectos metodológicos:

Figura 5.
Aspectos metodológicos necesarios para la identificación de riesgos y su tratamiento.

1 Identificación y Descripción del Riesgo

Identificación de Factores de riesgo
Áreas de impacto
Descripción del riesgo

2 Análisis de Riesgo Inherente

Determinar la probabilidad e impacto

3 Diseño y Análisis de Controles

Estructurar los controles

4 Valoración de Riesgo Residual

Aplicar la valoración de la efectividad de los controles sobre los riesgos

Elaborado por Grupo DOGI –2026

4.3.5.Marco Conceptual sobre el Apetito del Riesgo

Apetito del Riesgo

La Agencia Logística de las Fuerzas Militares establece los siguientes niveles de apetito, tolerancia y capacidad en los riesgos institucionales:

Apetito de Riesgo: Es nivel de riesgo que una entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección.

Solo se asumirán los riesgos que se encuentran en una escala del mapa de calor de probabilidad Muy Baja e impacto Leve, por lo cual para estos riesgos no será obligatorio establecer actividades dentro del plan de mitigación de riesgos.

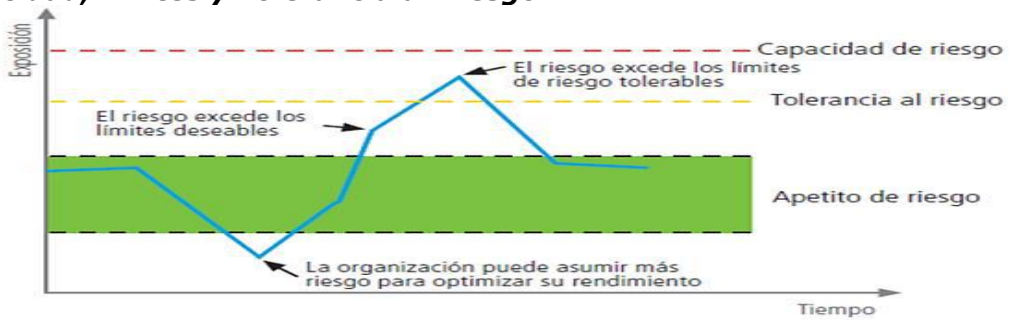
Tolerancia del Riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

No se tolerará desviaciones en la ALFM, pues los recursos son de carácter público y deben administrarse de forma eficaz.

Capacidad de Riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Los procesos evaluaran aquellos riesgos que se valoraron y quedaron en zonas extremas para determinar planes de contingencia principalmente en procesos de tipo misional.

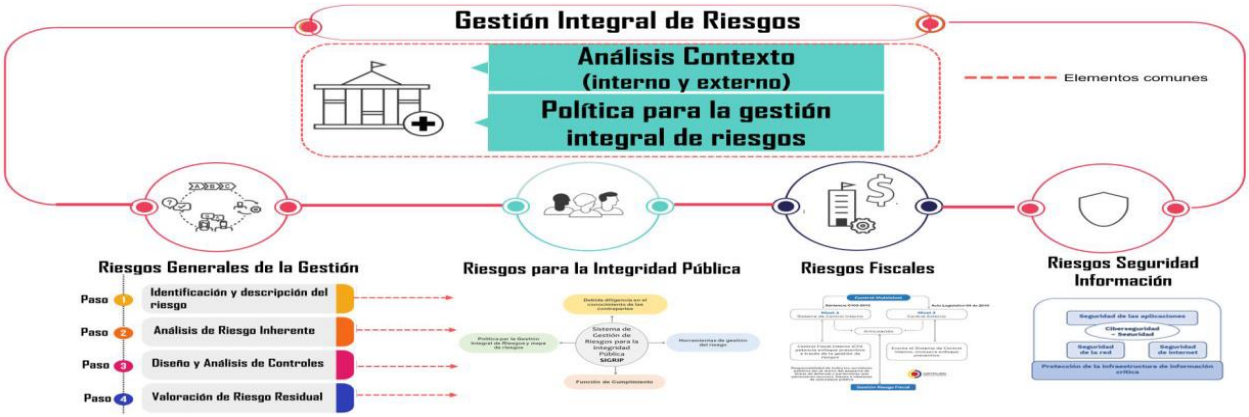
Figura 6.
Capacidad, límites y Tolerancia al Riesgo



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

4.3.6.Articulación para la Gestión Integral de Riesgos

Figura 7.
Articulación ámbitos gestión del Riesgo



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

4.4.DOCUMENTOS DEL PROCESO

4.4.1.Mapa de Riesgos por Procesos

Para la Entidad se establece el formato Mapa de Riesgos Integral en el cual los procesos conforme las instrucciones establecidas en el formato, deberán identificar y administrar los riesgos del proceso.

Este mapa de riesgos se registrará por parte de la Oficina Asesora de Planeación e Innovación Institucional en la herramienta Suite Vision Empresarial, antes del 31 de enero de cada vigencia para conformar el mapa de riesgos institucional, el cual se deberá publicar en el portal web en el enlace descrito a continuación a más tardar el 31 de enero de cada año.
https://www.agencialogistica.gov.co/sig/gestion-del-riesgo/mapa-de-riesgos-institucionales-y-corrupcion/

4.4.2. Guia para la Gestión y Clasificación de Activos de Información por Proceso

Cada proceso deberá identificar y clasificar los activos de información que administra según su criticidad y de acuerdo con las directrices emitidas por el proceso gestión de TIC y registrarlos en los planes institucionales definidos por esta dependencia, la clasificación de los activos debe estar alineada con las Tablas de Retención Documental y todo activo adicional que por lineamientos internos se deba clasificar.

4.4.3. Información Consolidada Resultado de la Administración de Riesgo

La Oficina Asesora de Planeación e Innovación Institucional dispondrá en la herramienta Suite Visión Empresarial el registro de los riesgos institucionales para consulta de todos los

funcionarios. Adicional se asociarán por medio del módulo de riesgos, los planes institucionales que soportan la gestión de riesgos.

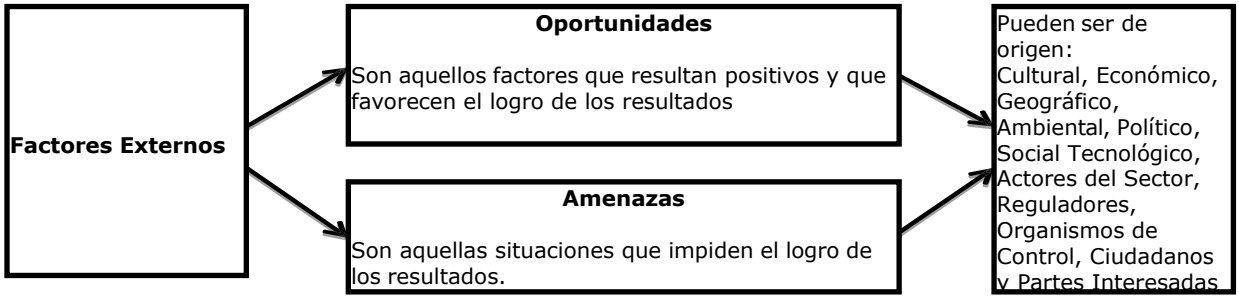
Los procesos podrán formular planes independientes para la gestión de controles o articular las actividades en el plan de mitigación institucional de cada vigencia.

4.5. ANALISIS DE CONTEXTO

Son las condiciones internas y del entorno, que pueden generar efectos positivos o negativos en el cumplimiento de la misión y los objetivos de la Entidad y de cada uno de los procesos definidos. Para determinar los diferentes factores internos y externos se aplica la herramienta de gestión denominada matriz DOFA formato GI-FO-26 el cual debe ser actualizado como mínimo una vez al año.

Realizando este análisis del entorno se logra identificar como factores externos que inciden las siguientes: oportunidades y Amenazas.

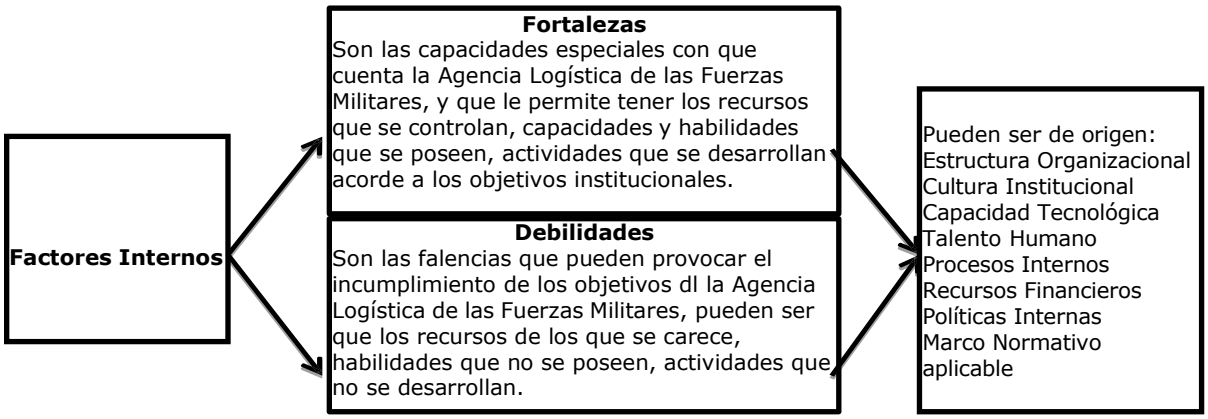
Figura 8.
Amenazas y Oportunidades



Nota: Factores externos del Entorno – Elaborado por Grupo DOGI -2026

Oportunidades: Como aquellos factores que resultan positivos, favorables, explotables, que se deben descubrir en el entorno de la entidad, y que favorecen el logro de los resultados.
Amenazas: son aquellas situaciones que provienen del entorno y que pueden llegar afectar de manera considerable los resultados de la entidad.
Realizando este análisis de la 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 se logra identificar como factores que inciden la siguientes: Fortalezas y debilidades.
Fortalezas: Son las capacidades especiales con que cuenta la Agencia Logística de las Fuerzas Militares, y que le permite tener los recursos que se controlan, capacidades y habilidades que se poseen, actividades que se desarrollan acorde a los objetivos institucionales.
Debilidades: Son las falencias que pueden provocar el incumplimiento de los objetivos de la Agencia Logística de las Fuerzas Militares, pueden ser que los recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan.

Figura 9.
Determinación de fortalezas y debilidades



Nota: Determinación de fortalezas y debilidades – Elaborado por Grupo DOGI -2026

La tabla a continuación presenta algunos ejemplos de factores internos y externos de riesgo u oportunidades:

Tabla 4.
Ejemplos de factores internos y externos

FACTORES EXTERNOS	FACTORES INTERNOS
ECONÓMICOS: Disponibilidad de capital, emisión de deuda o no pago de esta, liquidez mercados financieros, desempleo, competencia.	**INFRAESTRUCTURA:** Disponibilidad de activos, capacidad de los activos, acceso de capital.
	PERSONAL: Capacidad del personal, salud, seguridad
MEDIO AMIBIENTALES: Emisiones y residuos, energía, catástrofes naturales, desarrollo.	**PROCESOS:** Capacidad, diseño, ejecución, proveedores, entradas, salidas, conocimiento
POLITICOS: Cambios de gobierno, legislación, políticas públicas, regulación.	**TECNOLOGÍA**: Integridad, disponibilidad y accesibilidad a los datos, aplicativos y sistemas de información, desarrollo, producción, mantenimiento.
SOCIALES: Demografía, responsabilidad social, terrorismo.	
TECNOLÓGICOS: Interrupciones comercio electrónico, datos externos, tecnología emergente.	

Nota: Ejemplos de factores internos y externos – Elaborado por Grupo DOGI –2026.

4.6.MAPA DE RIESGOS

El mapa de riesgos es la consolidación de la información referente a riesgos analizada para cada uno de los procesos que componen el modelo de operación de la entidad.

Respecto al Mapa de riesgos, contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, son aquellos riesgos que permanecieron en las zonas más altas de riesgo, así como los riesgos de fraude o corrupción y que afectan el cumplimiento de la misión institucional y objetivos de la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos. En ambos casos se utiliza el mismo formato.

El Mapa de riesgos en la herramienta Suite Visión Empresarial – Modulo de gestión del riesgo – tiene vinculado el plan de mitigación, indicadores de riesgos u otros planes que soporten la ejecución de los controles definidos para los riesgos, allí se puede consultar el

avance de las acciones propuestas y esta información puede ser revisada por cualquier funcionario de la Agencia Logística de las Fuerzas Militares. En caso de existir evidencia en planificaciones que no se encuentran o no sean parametrizables en la herramienta SVE se debe establecer dentro del mapa de riesgos integrales como puede evidenciarse la aplicación del control fuera de la herramienta. De igual manera, los planes asociados a la gestión de las oportunidades se pueden consultar a través de la SVE. Es de vital importancia tener encuentra que la documentación correspondiente a la ejecución de los controles diseñados debe mantenerse disponible en caso de ejercicios de seguimiento y evaluación.

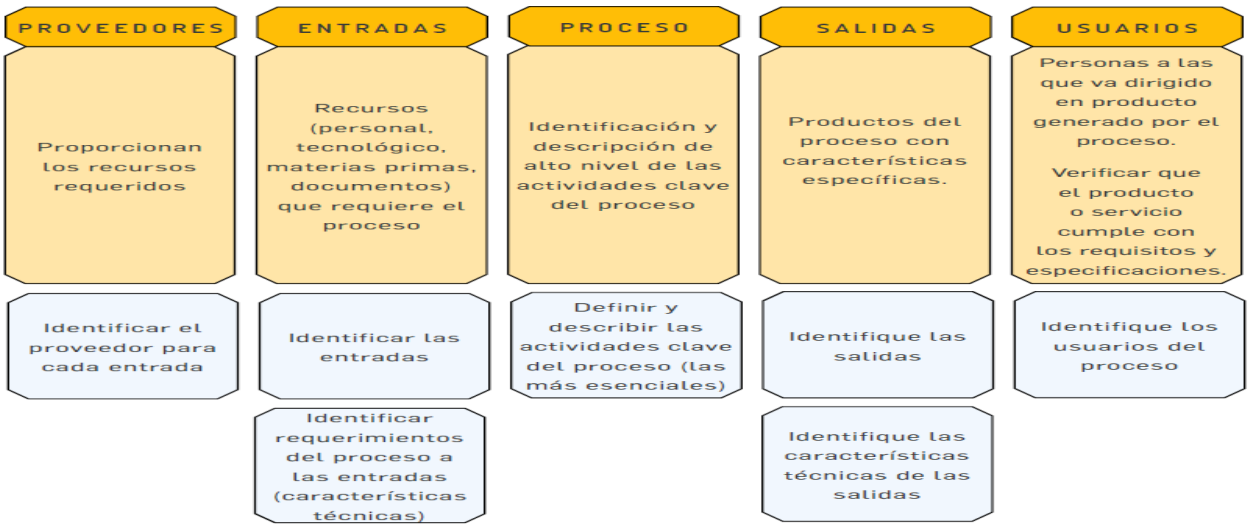
En el plan de mitigación de riesgos se encuentra en el módulo "planes" de la SVE, desde allí se direccionan las actividades para los riesgos identificados.

4.7. GESTIÓN DE RIESGOS GENERALES

4.7.1. Identificación y Descripción del Riesgo

Para una identificación asertiva y precisa de los riesgos claves de cada proceso, deberán considerarse aquellos eventos que podrían afectar de forma previsible el logro de los objetivos de proceso, considerados y ya descritos con los atributos SMART; Para llevar a cabo este análisis se debe considerar, adicional al objetivo del proceso, la estructura del mismo con sus actividades clave y la forma como participa dentro de la cadena de valor o ciclo de los procesos, teniendo en cuenta que las diferentes tareas que se encuentran al interior del ciclo de procesos están interrelacionadas, el orden en el que estas se llevan a cabo puede variar de acuerdo con cómo se conciba cada uno de los procesos.

Figura 10.
Componentes dentro del ciclo de procesos.



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

Lo anterior implica que consideren los atributos de los bienes o servicios que podrían verse afectados por diferentes eventos, en el marco de la cadena de valor.

Figura 11.
Cadena de Valor Publico

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

De este modo, para establecer los puntos de riesgo clave en los procesos, es necesario considerar los atributos de los productos, servicios o resultados de procesos que podrían verse afectados dentro del ciclo del proceso que se esté analizando, así como el efecto de estos posibles eventos en el resultado de otros procesos, dentro de una misma cadena de valor. Esta información se condensa en la caracterización de los procesos de la ALFM.

4.7.2. Identificación de Areas de Impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional, por ello se las principales áreas de impacto en la Entidad, será las que administren recursos de tipo económico.

4.7.3. Identificación de Areas de Factores de Riesgo

Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición. Los siguientes serán los factores de riesgo definidos para la Entidad:

Tabla 5.
Factores de riesgo

Factor	Definición	Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Falta de aplicación de los procedimientos
		Falta segregación de funciones
		Errores de grabación, autorización
		Falta de supervisión o interventoría
		Errores en cálculos para pagos internos y externos
		Alta rotación o insuficiencia de personal
		Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
		Acciones contrarias a las leyes o acuerdos contractuales
		Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP)	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la entidad (naturales o jurídicas)
		Productos (bienes o servicios) que oferta/requiere
		Canales utilizados para la operación
		Jurisdicciones (nacional o territorial)
Talento Humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Fraude Interno
		Soborno
		Gestión inadecuada de conflicto de Intereses
		Corrupción
		Hurto Activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Hurto Activos
		Daño de equipos
		Caída de sistemas de información y aplicaciones
		Caída de redes
		Errores en hardware o software
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.	Fraude Externo
		Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.
NOTA: En caso de identificar un factor de riesgo adicional se deberá informar a la Oficina Asesora de Planeación para incluirlo en la matriz y componentes metodológicos.

4.7.4. Descripción del Riesgo

A partir del punto de riesgo, área de impacto y área(s) de factor(es) de riesgo identificados, se debe proceder con la descripción del riesgo para lo cual se aplicará la siguiente estructura:

Figura 12.
Estructura para la redacción del Riesgos

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

A. **Impacto:** Las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la entidad la materialización del riesgo.
B. **Causa inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
   Estos dos elementos permiten plantear el evento no deseado (¿qué puede ocurrir?), es decir la situación, acción, condición o suceso incierto, que si ocurre, podría afectar el logro de los objetivos de la entidad.
C. **Causa raíz:** Se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o sub-causas que pueden ser analizadas.

Identificar las causas raíz y condiciones contribuyentes que se pueden clasificarse en: humanas, tecnológicas, normativas, ambientales, organizacionales.

La causa inmediata, entendida esta última como las circunstancias más evidentes sobre las cuales se presenta el riesgo y que en ocasiones, no constituyen la causa principal del riesgo.

Premisas para una adecuada redacción del Riesgo

- No describir como riesgos fallas ni desviaciones del control
- No describir como riesgos como la negación de un control
- No existen riesgos transversales, lo que pueden existir son causas transversales

El modelo de descripción del riesgo contiene cuatro elementos

- Evento no deseado y sus posibles consecuencias: ¿Qué puede pasar?
- Causas: ¿Por qué puede pasar?
- Tipología: ¿A qué categoría pertenece?
- Factor de riesgo: ¿Qué condición aumenta su probabilidad?

4.7.5. Análisis de Riesgo Inherente

A. Determinar la Probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, teniendo en cuenta la siguiente información:

Figura 13.
Frecuencia en los Riesgos

Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Muy Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

Teniendo en cuenta la anterior imagen se establecen los criterios en la siguiente tabla

Tabla 7.
Criterios para definir el nivel de probabilidad

	Descripción	Calificación
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

B. Determinar el Impacto

Son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. Y se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se deberá tomar el nivel más alto.

Tabla 8.
Criterios para definir el nivel de impacto

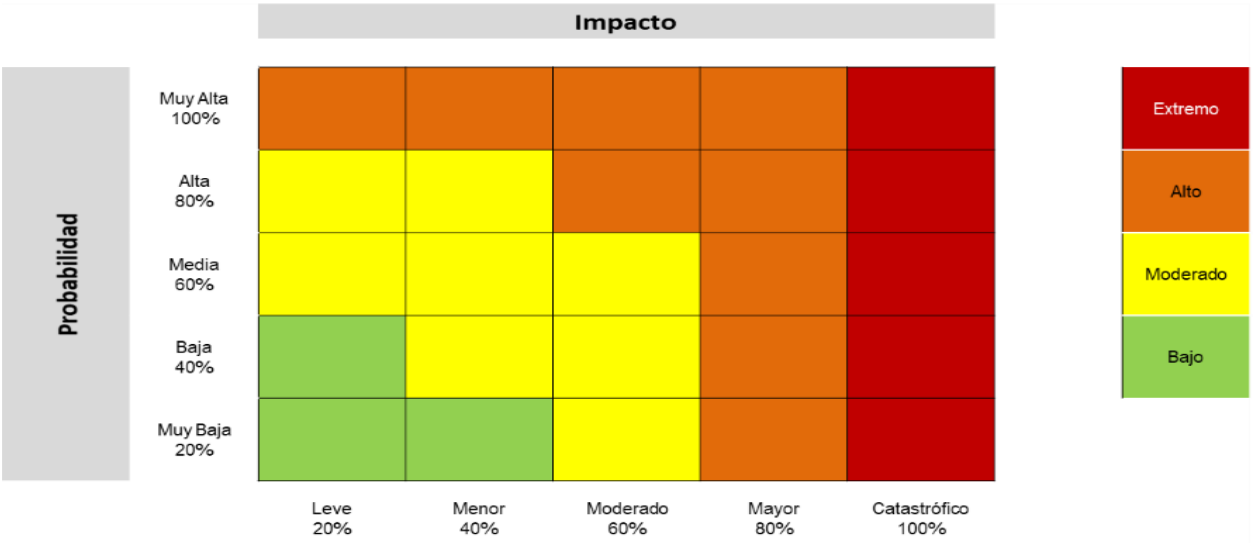
Nivel de Impacto	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la Entidad.
Menor 40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de consejo directivo y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7

C. Análisis de Severidad

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

Figura 14.
Matriz de calor (niveles de severidad del riesgo)



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

4.7.6. Diseño y Análisis de Controles

Las actividades de control son acciones concretas y con unos atributos específicos que son establecidas a través de políticas, procedimientos u otras directrices o documentos institucionales e implementadas con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos.

Para la identificación o el diseño de controles se debe tener en cuenta que:

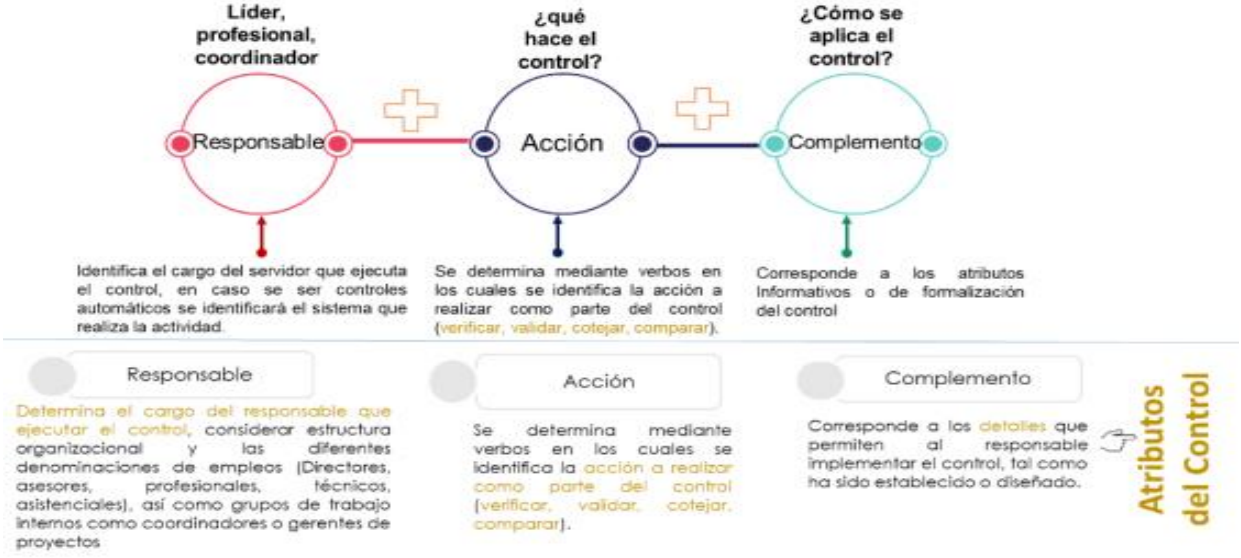
- Se pueden diseñar y establecer para cada riesgo a través de diferentes mecanismos, a través de las entrevistas con los líderes de procesos o servidores expertos en su labor, o del análisis de los procedimientos, manuales, guías y/o instructivos que el líder del proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo.

- Se requiere los diferentes atributos de las actividades de control para asegurar aspectos tales como: los responsables de su ejecución, la segregación de funciones y niveles de autoridad apropiados, esto se identificará en los planes asociados a los diferentes riesgos institucionales, adicional se deberá garantizar por cada proceso que los controles definidos se encuentren documentados en los procedimientos, guías o manuales adoptados.

- Las actividades de control deberán atender las causas raíz identificadas y enfocarse en la gestión de los factores de riesgo previamente identificados.

A. Estructura para la Descripción del Control

Figura 15.
Estructura para la redacción de controles



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

B. Responsabilidades en la Gestión De Riesgos

Las responsabilidades en términos de riesgos se fundamentan en el modelo de líneas de defensa establecidas modelo integrado de planeación y gestión (MIPG).

Responsable: Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (Directores, asesores, profesionales, técnicos, asistenciales), así como su despliegue grupos de trabajo internos e incluir coordinadores o gerentes de proyectos. Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.
Acción: Determina para qué se realiza el control, se debe utilizar verbos fuertes como, Verificar, validar, conciliar, comparar, revisar, cotejar, detectar.

Atributos Informativos o de formalización del control: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado.

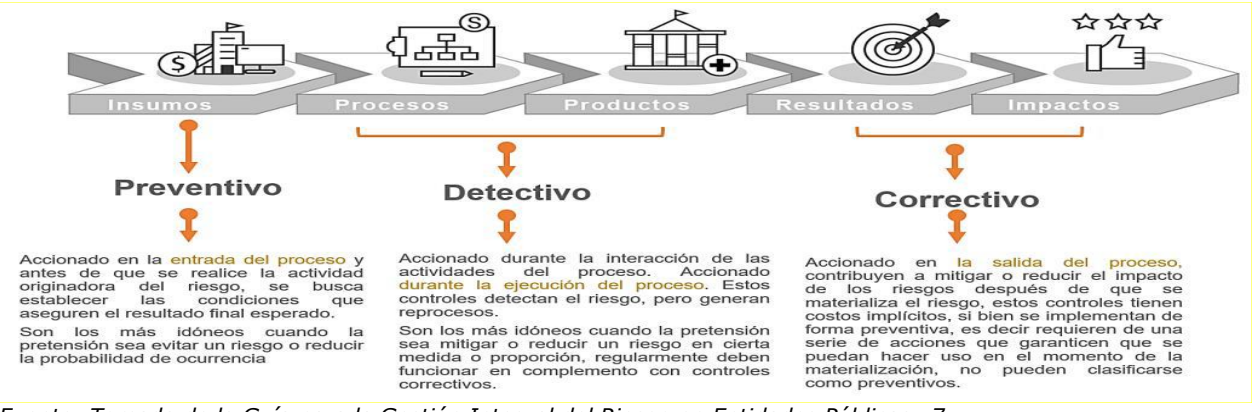
Se contemplan los siguientes aspectos:

- Documentación: se refiere a la fuente documental de los controles (manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso).
- Frecuencia: corresponde a la periodicidad con la cual se ejecuta una actividad de control. (puede ser periódica o por evento).
- Evidencia: permite contar con una trazabilidad en la ejecución del control. (registro físico manual o registro electrónico).
- Ejecución: Permite establecer cómo se ejecuta el control

C. Tipologías de Controles

Para establecer la tipología de controles para su validación, es necesario acudir al ciclo de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo, o bien una combinación de estos.

Figura 16.
Cadena de valor del proceso y las tipologías de controles



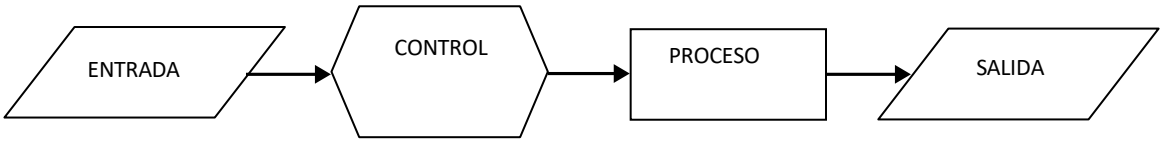
Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Los controles son mecanismos con los que cuenta la entidad para reducir la probabilidad de ocurrencia o el impacto que pueda generar la materialización del riesgo tanto de

gestión como de fraude o corrupción. Es necesario identificar los ***puntos de control*** existentes para el desarrollo de esta etapa, estos pueden ser detectivos, preventivos y correctivos, así mismo también se pueden identificar por cómo se efectúan: manuales o automáticos.

a. Control Preventivo: Accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo; actúan sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos.

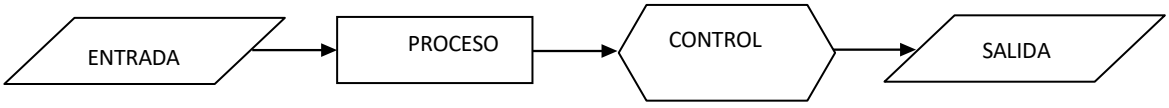
Figura 17.
Controles Preventivos



Nota. Controles preventivos – Elaborado por Grupo DOGI -2026

b. Control Detectivo: Accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Se diseñan para descubrir un evento, irregularidad o un resultado no previsto; alertan sobre la presencia de los riesgos y permiten tomar medidas inmediatas; pueden ser manuales o computarizados. Generalmente sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos. Ofrecen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear, o alertar a los funcionarios.

Figura 18.
Controles Detectivos

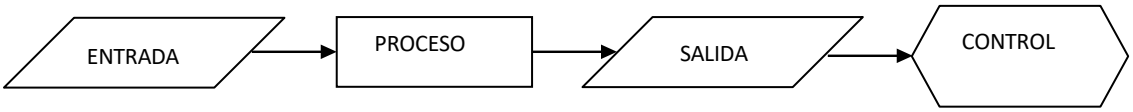


Nota. Controles detectivos – Elaborado por Grupo DOGI -2026

c. Control Correctivo: Accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Permiten el restablecimiento de una actividad, después de ser detectado un evento no deseable, posibilitando la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan, y permiten mejorar las deficiencias. Por lo general, actúan con los

controles detectivos, implicando reprocesos. Son de tipo administrativo y requieren políticas o procedimientos para su ejecución.

Figura 19
Controles Correctivos



Nota. Controles correctivos – Elaborado por Grupo DOGI - 2026

d. Control manual: Controles que son ejecutados directamente por el funcionario.

e. Control automático: Son aquellos ejecutados por sistemas de información o automatizados.

D. Valoración de Controles

El procedimiento para la valoración del riesgo parte de la evaluación de los controles existentes, lo cual implica:

Describirlos (estableciendo si son preventivos, detectivos, correctivos).

Revisarlos para determinar si los controles están documentados, si se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.

Es importante que la valoración de los controles incluya un análisis de tipo cuantitativo, que permita saber con exactitud cuántas posiciones dentro de la Matriz de Calificación, Evaluación y Respuesta a los Riesgos es posible desplazarse, a fin de bajar el nivel de riesgo al que está expuesto el proceso analizado.

Para valorar los controles y determinar lo desplazamientos dentro de la Matriz de Calificación, Evaluación y Respuesta a los Riesgos, se puede hacer utilizando las matrices que a continuación se presentan, los cuales permiten de manera objetiva determinar dicho desplazamiento.

En la siguiente imagen, se muestra la forma como se califican los atributos o características de Eficiencia.

Figura 20.
Valoración de Controles

Valoración de controles

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Figura 21.
Análisis Atributos

Análisis atributos formalización del control

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

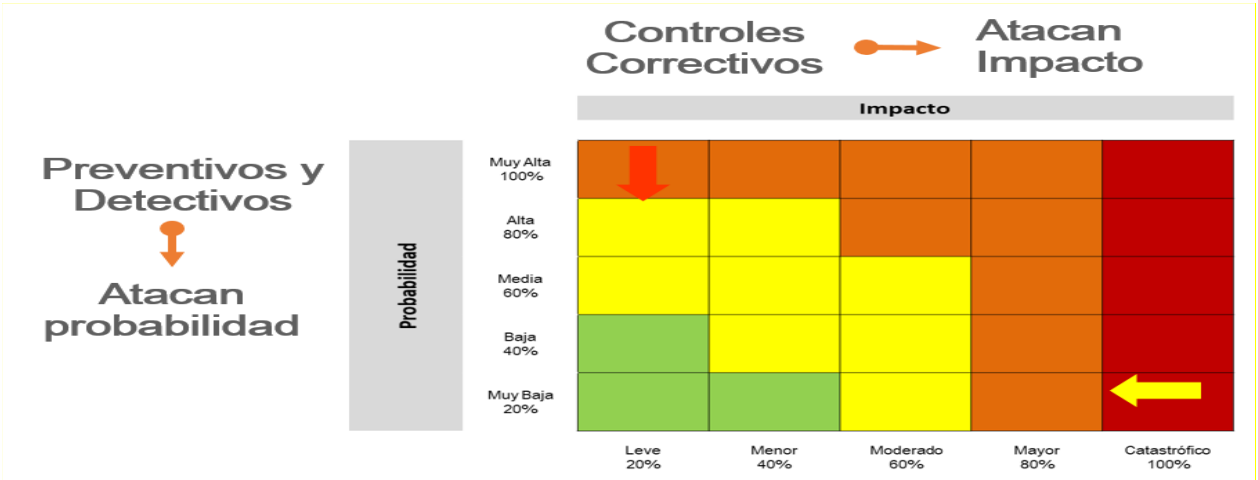
Fuente: Elaboración Dirección de Gestión y Desempeño Institucional, 2025.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

a. Aplicación de Controles en la Matriz de Severidad

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

Figura 22.
Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

El resultado obtenido a través de la valoración del riesgo, es denominado también tratamiento del riesgo, ya que se "involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales acciones" así el desplazamiento dentro de la Matriz de Evaluación y Calificación determinará finalmente la calificación del riesgo.

b. Valoración de Riesgo Residual

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

Figura 23.
Aplicación de Controles

Aplicación de controles para establecer el riesgo residual

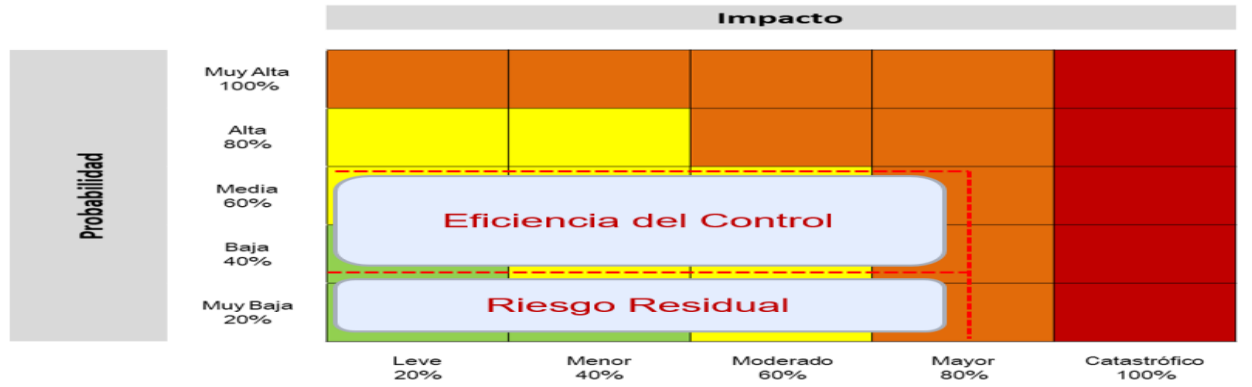
Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos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

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

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Gráficamente el movimiento en la matriz de calor se muestra

Figura 24.
Visualización Grafico



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

4.8.SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA -SIGRIP

Teniendo en cuenta la expedición de la Ley 2195 de 2022, que hace obligatorio para las entidades públicas la "prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional" (artículo 31).

4.8.1.Integridad Pública

Las organizaciones se exponen frecuentemente a que sus objetivos no se cumplan como consecuencia de los diferentes intereses que pueden confluir en la toma de decisiones, en la medida que se privilegian intereses propios sobre el interés general de la organización. En el caso del sector público, el interés general, que no es otra cosa que el interés por la consecución de los fines del Estado, también se puede ver afectado por intereses particulares, lo que termina afectando la capacidad de las entidades públicas para cumplir con las funciones que se le han encomendado.

En materia de integridad en el sector público, se espera que los servidores, y en general los colaboradores de las entidades públicas, dentro de un marco ético, se comporten de forma que privilegien el interés general del Estado en todas las decisiones que deben tomar en el ejercicio de sus funciones o del servicio que prestan.

4.8.2.Amenazas para la Integridad Pública

La Organización para la Cooperación y el Desarrollo Económico, ODCE, ha planteado la necesidad de aplicar un enfoque basado en riesgos cuando se habla de integridad pública

A. Soborno

El Soborno puede ser entendido como "ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar.

a. **Soborno Entrante:** El soborno al servidor de la Entidad

b. **Soborno Saliente:** De servidores a otros en nombre de la Entidad.

B. Fraude: corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.

a. **Fraude Interno**: Cuyo caso el fraude involucra a colaboradores.

b. **Fraude Externo**: Se realiza por terceros externos la organización es la víctima, es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.

C. Inadecuada gestión del conflicto de intereses

Un conflicto de intereses surge cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho.

D. Corrupción

La Corrupción es *"todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero.*

E. Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP

La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la capacidad del Estado para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento.

4.8.3.Sistema de Gestión del Riesgo

Teniendo en cuenta las diferentes amenazas para la integridad pública, que pueden generar peligro o daño, es necesario que, desde un enfoque basado en riesgos, se gestionen los eventos que pueden ocurrir dentro de la Entidad. La gestión implica que la Entidad debe identificar, analizar y valorar los riesgos, partiendo de la existencia de eventos que pueden convertirse en factores de riesgo. El SIGRIP busca articular la Política para la Gestión Integral de Riesgos, mediante la cual se gestionan los Riesgos Generales de la Gestión, la Gestión Preventiva de Riesgos Fiscales y los Riesgos de Seguridad de la Información, con los demás elementos que son necesarios para gestionar los riesgos para la integridad pública.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP contempla que la entidad adopte una serie de instrumentos de gestión del riesgo, que actúe con diligencia en el conocimiento de sus contrapartes y que integre en su operación una función de cumplimiento, todo esto además de la identificación y valoración de los riesgos según la metodología definida en la Política para la Gestión Integral de Riesgos que adopte. Además, permite a la entidad dar cumplimiento a los lineamientos establecidos para la gestión de riesgos en los Programas de Transparencia y Ética Pública.

A. Contexto de la organización

Dentro de los análisis de contexto se debe realizar un análisis teniendo en cuenta los siguientes aspectos.

a. La planta y estructura de la entidad, así como la delegación de autoridad o poder decisorio discrecional dentro de la organización.
b. Los grupos de valor o partes interesadas, incluidos los clientes internos y externos en especial énfasis en identificar aquellos que pueden considerarse contrapartes.
c. Si la entidad está desconcentrada en el país, identificar los lugares en qué opera, así mismo, si por su misión, opera en otras jurisdicciones o en sectores, industrias o mercados específicos, identificarlos.
d. La naturaleza, escala y complejidad de los procesos, servicios, trámites u otras operaciones administrativas de la organización.
e. Información general sobre los contratos y principales proveedores de la entidad. (Naturaleza Jurídica, Modalidad de Selección, Valores de Contratación, relación de cumplimientos e incumplimientos, tipos de supervisor, entre otras.
f. Las Entidades que tiene bajo su control y entidades que ejercen control sobre la Entidad
g. La naturaleza y alcance de las interacciones con entidades de otras Ramas del Poder Público, órganos de control o independientes.
h. Las obligaciones generales de la entidad, con independencia de la fuente: legal, reglamentaria, contractual, extracontractual u obligaciones profesionales.

B. Liderazgo del Sistema

A continuación se identifican los roles y responsabilidades respecto al componente SIGRIP:

Tabla 9.
Roles y Responsabilidades

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	**Auditor del Programa**	**Administrador del Programa**	**Ejecutores del Programa**
Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno	Oficina de Control Interno, Auditoría Interno o quien haga sus veces	Oficina Asesora de Planeación e Innovación Institucional Secretaria General	Directivos, líderes de proceso, servidores y colaboradores
Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.	Responsables de la formulación del Programa de Transparencia y ética Publica y de asesorar la formulación de riesgos SIGRIP	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, ejecución de controles y su seguimiento

Fuente: Elaboración propia a partir la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

C. Planificación

El SIGRIP será un sistema conexo al sistema de gestión de calidad en la Entidad, por lo cual dentro de este se definirán los objetivos correspondientes. De igual forma su enfoque de

ejecución principal será el Programa de Transparencia y Ética Pública. De igual forma los procesos identificaran los riesgos relacionados con la integridad pública de acuerdo con las siguientes categorías

- Integridad pública de corrupción
- Integridad pública de lavado de activos, financiación del terrorismo, financiación de la proliferación de armas de destrucción masiva.

D. Apoyo

El SIGRIP, debe disponer de recursos necesarios (Financieros, Humanos, Tecnologías de la información, habilidades especializadas, infraestructura organizacional entre otras), una estrategia de formación y comunicación y documentar todas las actividades.

La Entidad debe concientizar a todo el personal de la cultura de la legalidad (Lideres, Alta Dirección, y en general todos los funcionarios).

Comunicar Interna y Externa los resultados de la operación y actualizaciones del sistema o alguno de sus elementos.

Los elementos del sistema deben estar correctamente documentado e incluirse en el Sistema de Gestión los documentos del SIGRIP, como en la gestión archivista de la Entidad.

E. Operación

Los procesos deberán formular sus riesgos asociados al SIGRIP, para lo cual derivado de esta formulación se aplicarán controles en materia de:

- La debida diligencia
- La función de cumplimiento.
- Herramientas de gestión de riesgo.

Figura 25.
Sistema de Gestión de Riesgos para la Integridad Pública

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

a. Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos.

La Entidad deberá identificar y valorar los riesgos, incluidos los riesgos de LA/FT/FP que apliquen con base en su objeto misional y operación, cuya principal amenaza para la integridad es la corrupción, por lo cual se requiere que se identifiquen y valore individualmente aspectos como el soborno, el fraude, la inadecuada gestión del conflicto de intereses y conductas que permiten o favorecen el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva.

Los riesgos para la integridad pública deben ser gestionados en conjunto con los riesgos generales de gestión, la gestión preventiva del riesgo fiscal y los riesgos de seguridad de la información.

- ***Identificación y descripción del riesgo***

En el marco del Riesgo de LA/FT/FP se refiere en las actividades (operaciones) del flujo de procesos que implican intercambio de recursos.

Respecto del riesgo de Corrupción y sus manifestaciones (soborno, fraude e inadecuada gestión del conflicto de intereses), los puntos de riesgos pueden ser cualquier actividad dentro del flujo de proceso y no solo las operaciones.

- ***Identificación de áreas de impacto***

La gestión de los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

  - **La consecuencia legal:** Incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños y surge a partir en que una contraparte es vinculada a procesos judiciales o administrativos sancionatorios o que busquen declarar un incumplimiento.
  - **El contagio:** a partir de que la entidad pueda sufrir una afectación económica, reputacional o legal a causa de la acción propia de una entidad o de un individuo relacionado. Y se expresa cuando a partes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar a la entidad.
    Las consecuencias de ambas para de determinar el impacto del riesgo se deben analizar en términos de afectación económica se pueda aplicar la **Tabla 8** *Criterios para definir el nivel de impacto Gestión de Riesgos Generales.*
  - **La consecuencia reputacional:** Surge cuando la organización se ve involucrada en denuncias o reportajes que la vinculan con prácticas poco íntegras, incumplimientos normativos o corrupción en general.
  - **La consecuencia operativa:** Corresponde a los escenarios en que la conducta contraria a la integridad termina afectando el desarrollo de los procesos.
  - **la consecuencia económica** Desde el mismo momento en que hay retrasos en la ejecución del recurso, por conductas poco íntegras del ejecutor.

La gestión del riesgo de LA/FT/FP está centrada en prevenir la utilización de la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas, aun cuando no haya consecuencias, **toda operación sospechosa, incluso la intentada, debe ser objeto de reporte, al margen de la materialización del delito de lavado de activos**.

La materialización del riesgo no debe confundirse con la ocurrencia del delito, falta o conducta generadora de responsabilidad fiscal; los riesgos para la integridad no deben entenderse como tipos penales o disciplinarios, ni la materialización del riesgo implica un prejuzgamiento.

Toda la gestión del riesgo tiene como principales objetivos la identificación, medición, control y el monitoreo, con el propósito de prevenir, detectar y corregir. En ningún caso podrá derivar en juicios de responsabilidad o en la aplicación de sanciones.

- **Respecto de la "Identificación de factores de riesgo"**

Los factores del riesgo LA/FT/FP (contrapartes, productos, los caneles y las jurisdicciones) aspectos mínimos a contemplar en cualquier análisis que en conjunto conforman el concepto de transacción u operación, será realizada por un cliente o usuario, que accedió o entregó un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.

- **Respecto de la "Descripción del riesgo"**

La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en el Capítulo 5.7 Gestión de Riesgos Generales.

Teniendo en cuenta las amenazas, las causas inmediatas de los riesgos para la integridad pública podrán ser el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP.

- ***Análisis de Riesgo Inherente***

Respecto del "Análisis de Riesgo Inherente"

Por la naturaleza de los riesgos para la integridad pública, el objetivo fundamental es prevenirlos, detectarlos y reportarlos en términos de oportunidad y eficacia.

Para el cálculo de probabilidad e impacto, aplica lo establecido en el Capítulo 5.7 Gestión de Riesgos Generales. (**Determinar la probabilidad), (Determinar el impacto) y la matriz de severidad.**

- ***Diseño y Análisis de Controles***

Para el diseño de controles deberá tenerse en cuenta que, además de la Política para la Gestión Integral de Riesgos y su respectivo Mapa de Riesgos, el manual de debida diligencia, función de cumplimiento y formular una serie de herramientas de gestión.

- ***Valoración de Riesgo Residual***

Respecto de la "Valoración del riesgo residual puede remitirse en el Capítulo 5.7 Gestión de Riesgos Generales ***Valoración de Riesgo Residual.***

b. Debida diligencia en el conocimiento de las contrapartes

La Subdirección General de Contratación debe estructurar y actualizar el manual de debida diligencia con el cual debe llevar a cabo el conocimiento de sus contrapartes. Como mínimo debe llevar los siguientes criterios.

Identificar la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico o el contrato estatal.

Identificar (el/los) beneficiario(s) final(es) y la estructura de titularidad y control de la persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico o el contrato estatal, y tomar medidas razonables para verificar la información reportada.

Solicitar y obtener información que permita conocer el objetivo que se pretende con el negocio jurídico o el contrato estatal. Solicitar y obtener información que permita conocer el objetivo que se pretende con el negocio jurídico o el contrato estatal. Solicitar y obtener información que permita conocer el objetivo que se pretende con el negocio jurídico o el contrato estatal.

Realizar una debida diligencia de manera continua del negocio jurídico o el contrato estatal, examinando las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones sean consistentes con el conocimiento de la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se realiza el negocio jurídico o el contrato estatal, su actividad comercial, perfil de riesgo y fuente de los fondos.

c. Función de Cumplimiento

La función de cumplimiento implica velar por el efectivo, eficiente y oportuno funcionamiento del SIGRIP en su conjunto, y cada uno de sus elementos, promoviendo el cumplimiento de sus disposiciones y apoyando a los líderes de procesos y gestores de riesgo, en la gestión de los riesgos identificados.

Nota: De acuerdo con las disposiciones del Departamento de la Función Pública, no es necesario que la entidad cree cargos específicos para asumir esta función de cumplimiento. Según lo establecido en el Decreto 1083 de 2015, …*por regla general, cualquier servidor del nivel directivo, o su equivalente según el sistema de empleo público con que cuente la entidad, podría asumirla al estar relacionada con las funciones generales que tiene este tipo de cargo, en particular, la de "adelantar las gestiones necesarias para asegurar el oportuno cumplimiento de los planes, programas y proyectos y adoptar sistemas o canales de información para la ejecución y seguimiento de los planes del sector". Incluso esta función podría ser asumida por servidores del nivel asesor, que tienen, entre otras funciones, la de "absolver consultas, prestar asistencia técnica, emitir conceptos y aportar elementos de juicio para la toma de decisiones relacionadas con la adopción, la ejecución y el control de los programas propios del organismo".*

La función de cumplimiento no sustituye, elimina o restringe las funciones propias de las unidades de control interno.

Está función será determinada por la Dirección General en apoyo de la Dirección Administrativa y Talento Humano, dejando registro de asignación que corresponda.

d. Herramientas de Gestión del Riesgo.

La ALFM además de contar con la política para la Gestión Integral de Riesgos, debe definir las siguientes políticas conexas:

- Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP).
- Política Antisoborno**.**
- Política Antifraude.
- Procedimiento para la gestión de los conflictos de intereses
- Procedimiento para el reporte de operaciones sospechosas
- Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético.

Nota: La Entidad tendrá un plazo de 4 meses contados a partir de la expedición de la presente versión del manual de riesgos para definir estas herramientas.

e. Monitoreo, evaluación, auditoría y mejora

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto permanente de monitoreo, evaluación, auditoría y mejora por medio de la evaluación y mejora del programa de transparencia y ética pública, así como la gestión de riesgos.

4.9.GESTION DE RIESGOS FISCALES

El riesgo fiscal es "*Efecto dañoso sobre recursos, bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.*", este tipo de riesgo debe ser incluido en el Mapa de Riesgos Integrales de la entidad.

Efecto dañoso: Daño que se generaría sobre los recursos, en caso de ocurrir un evento.
Evento Potencial: Hechos inciertos o incertidumbres que podría generar daño sobre los recursos.

Nota: No se debe confundir el riesgo fiscal con el daño patrimonial. El riesgo fiscal se relaciona con el evento de potencial efecto perjudicial sobre los recursos bienes o intereses públicos, mientras que el daño patrimonial es la afectación real y concreta a los mismos, como resultado de una acción u omisión.

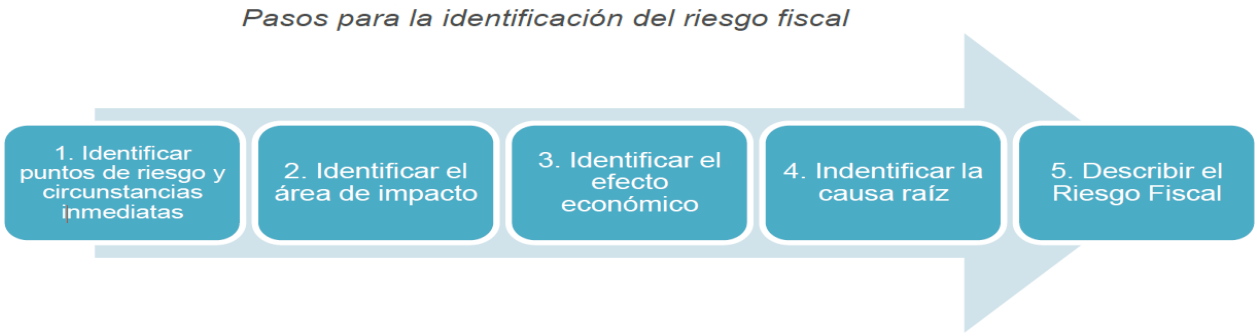
El control fiscal adquiere un enfoque preventivo que se potencia con el control interno. Donde se denomina **gestor fiscal a** los jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores de proyectos, responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros roles cuyas funciones u obligaciones incidan en la gestión fiscal. Bajo este parámetro se define un modelo control fiscal multinivel que es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

Figura 26.
Articulación modelo constitucional control fiscal y sistema de control interno

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

4.9.1.Identificación de Riesgos Fiscales

Figura 27.
Identificación Riesgo Fiscal



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Los **puntos de riesgo fiscal** son eventos en los que potencialmente se genera riesgo fiscal, es decir, son las actividades propias de la gestión fiscal.

las **circunstancias inmediatas** son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo.

Tabla 11.
Identificación de riesgos fiscales.

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal?
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas", son aplicables a la entidad?
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI- **Nota 1:** Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. **Nota 2:** Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. **Nota 3:** Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. **Nota 4:** La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? **Nota:** Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

4.9.2. Identificación de Áreas de Impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo. El concepto de patrimonio público a partir de las tres expresiones que se derivan del artículo 6 de la Ley 610 de 2000:

A. **Bienes públicos:** Son todos aquellos muebles e inmuebles de propiedad pública (bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de

particulares). Estos se clasifican en bienes de uso público (aquellos cuyo uso pertenece a todos los habitantes del territorio nacional) y bienes fiscales (aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos).

B. Recursos públicos: Son los dineros comprometidos y ejecutados en ejercicio de la función pública.

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

4.9.3.Identificar el Efecto Económico

El efecto económico del riesgo fiscal es el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público.

Nota: No todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

A. Riesgos de daño antijurídico: Los montos que se reconocen como pago de condenas y conciliaciones.

B. Efectos económicos generados por causas exógenas: No relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público.

C. Multas: Impuestas por hechos que no comportan gestión fiscal.

D. Existencia de actuación de cobro coactivo por parte de la entidad.

E. Pérdida de Bienes: Cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.

F. Perdida de bienes cuando se presenta el daño: El riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su "normal uso" (máquinas eléctricas, computadores, celulares, etc.).

4.9.4.Identificación de la Causa Raíz o Potencial Hecho Generador

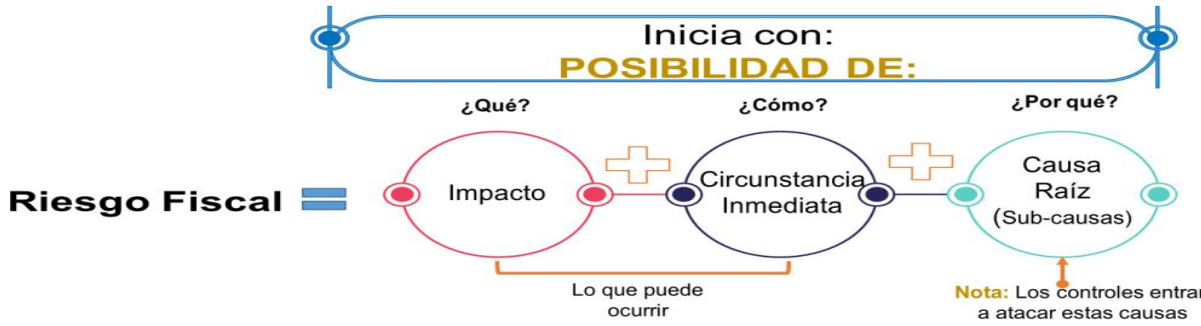
La **causa raíz** sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro.
La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal (efecto dañoso).

4.9.5. Descripción del Riesgo Fiscal

Para redactar un riesgo fiscal se debe tener en cuenta:

A. **Iniciar con la oración.** Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
B. **Impacto.** Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.
C. **Circunstancia inmediata**. Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal que lo genera.
D. **Causa Raíz.** Corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño.

Figura 28.
Descripción Riesgo Fiscal



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Tabla 12.
Aplicación pasos descripción Riesgo Fiscal

Paso	Identificación
Punto de Riesgo: (Actividad de la Gestión Fiscal)	Gestión de cobro a contribuyentes en mora del pago de sus obligaciones tributarias.
Circunstancia inmediata: (Situación en la que se presenta el Riesgo)	Prescripción de los términos para la exigibilidad de las obligaciones tributarias.
Área de Impacto: (Patrimonio Público Afectado)	Intereses patrimoniales de la entidad
Efecto económico: (Potencial daño al Patrimonio)	Menor recaudo de ingresos tributarios establecidos a favor de la entidad
Causa raíz: (Potencial Acción u Omisión)	Errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Figura 29.
Redacción de riesgos fiscales.

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efecto dañoso sobre los **intereses patrimoniales**	Por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora.	A causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Conclusión: El riesgo fiscal existe desde el momento en que, existiendo obligaciones en mora, los procedimientos de cobro no se ejecutan de manera oportuna y correcta, pues allí surge la potencial reducción del recaudo. En esta etapa, el sistema de control interno debe ser capaz de tomar los correctivos necesarios, pues una vez se materialice la prescripción, se configura el daño patrimonial (hallazgo fiscal) a partir del cual el órgano de control fiscal procede a establecer y exigir la responsabilidad del gestor fiscal.

4.9.6. Valoración del Riesgo Fiscal

En este paso se realiza la Evaluación de Riesgos donde que busca establecer el nivel de riesgo inherente, entendido como la probabilidad de ocurrencia del riesgo, así como su impacto en la gestión fiscal.

La probabilidad, el impacto, la determinación del nivel del riesgo inherente: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad. Para la evaluación del Riesgo Fiscal, se aplicara las tablas de frecuencia e impacto, así como la matriz de severidad en el Capítulo 5.7 Gestión de Riesgos Generales

4.9.7. Valoración de Controles

Los controles pueden ser preventivos, detectivos o correctivos dependiendo el momento (antes, durante o después) en que se accionen respecto a la actividad que origina el riesgo fiscal (punto de riesgo). Para el análisis y evaluación de los controles se aplican los lineamientos para la redacción del control establecidos en el Capítulo 5.7 Gestión de Riesgos Generales

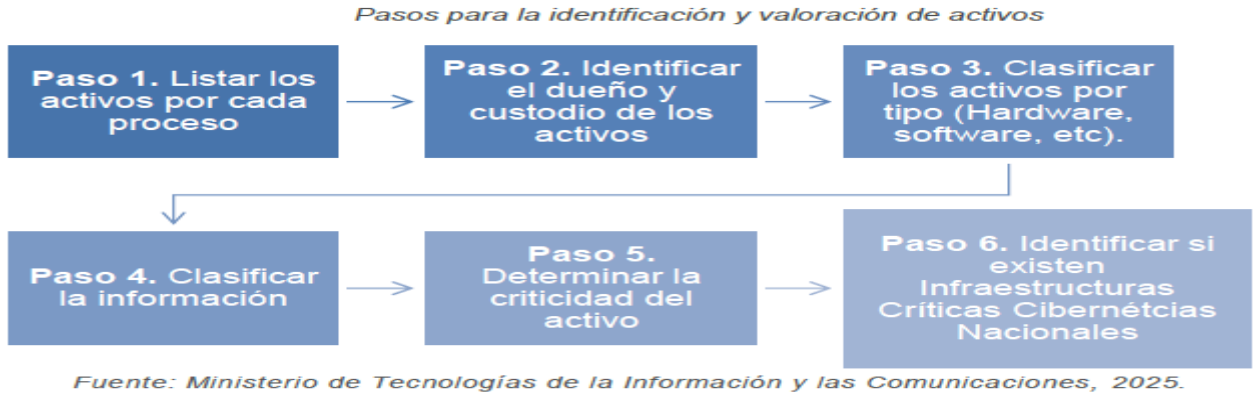
Los elementos relacionados con la evaluación, establecimiento de controles y monitoreos se realizan con la misma metodología descrita para los riesgos organizacionales. Como complemento a este capítulo, y para mejorar la identificación de puntos de riesgo fiscal, se recomienda revisar el anexo I de la guía de administración de riesgos del DAFP "*CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS*"

4.10. GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

4.10.1. Identificación y Descripción de Riesgos de Seguridad de la Información

En primer lugar, se deben identificar los activos de Información mediante las actividades descritas en los "*Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional*" del MSPI *Modelo de Seguridad y Privacidad de la Información*

Figura 30.
Identificación y Valoración



Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Se deben listar cada uno de los activos de información de la entidad que corresponden al alcance del proyecto, luego, para cada activo se deben registrar los siguientes datos:

A. Datos para cada activo de Información

Macroproceso, Proceso, Identificador, Tipo (Información y datos Entidad, Sistemas de información y aplicaciones de Software, Dispositivos de Tecnologías de Información-Hardware, Soporte para almacenamiento de Información, Servicios, Recursos Humanos, Instalaciones, Redes), Oficina, Serie documental, Nombre, Descripción, Nombre del responsable de la producción de la información (Propietario del activo), Fecha de generación de la información, Nombre del responsable de la información (Custodio del activo), Fecha de ingreso del activo al archivo, Soporte de registro *((Físico (análogo), Digital (electrónico) y N/A (Demas tipos de activos))*, Medio de conservación, Formato e idioma.

Se realiza la Clasificación de Activos de Información de acuerdo con la propiedad correspondiente: Disponibilidad, Integridad y Confidencialidad; para cada uno de los activos se define un nivel de criticidad de la propiedad especifica y se define tres niveles que permiten el valor general o criticidad del activo de la entidad.

Figura 31.
Criterios de Clasificación

Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Tabla 13.
Niveles de Confidencialidad

Tipo de Información	Descripción
INFORMACIÓN PUBLICA RESERVADA	Es la información que no debe ser divulgada debido a que esto puede causar daño a intereses públicos. Solamente la Constitución o la ley pueden definir qué información es de carácter reservado.
INFORMACIÓN PUBLICA CLASIFICADA	Es la información que no debe ser divulgada debido a que se pueden vulnerar los derechos de las personas naturales o jurídicas, tales como: derecho de las personas a la intimidad, derecho a la vida, salud o seguridad y los secretos comerciales, industriales y profesionales.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Nota. Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional (MSPI)2025

Figura 32.
Criterios de Clasificación

Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Tabla 14.
Clasificación de la Integridad

Clasificación	Descripción
A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Nota. Tomada de Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional (MSPI) 2025

Tabla 15.
Clasificación de la Disponibilidad

Clasificación	Descripción
1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Tomada de Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional (MSPI) 2025

B. Nivel de Criticidad del activo de Información.

Infraestructura Critica Cibernética Nacional, Información publicada (Interna, externa, ambas o no publicada) y Lugar de consulta o ubicación.

C. Índice de información clasificada y reservada

Objeto legítimo de la excepción, Fundamento constitucional o legal, Fundamento jurídico de la excepción, Excepción total o parcial, Fecha de clasificación (DD/MM/AAAA) y Tiempo de clasificación.

D. Los activos de información que contienen datos personales.

¿Contiene datos personales?, ¿Contiene datos personales de niños, niñas o adolescentes?, Tipos de datos personales (públicos, privados, semiprivado), Finalidad de la recolección de los datos personales, Existe la autorización para el tratamiento de los datos personales.
Todas las definiciones anteriormente mencionadas se encuentran se Guía para la Gestión del Inventario y Clasificación de Activos de Información e Infraestructura Crítica - GTI-GU-02- que se encuentre vigente a la fecha para la Entidad, en relación a en el capítulo de Riesgos de Seguridad de la Información

4.10.2.Lineamientos Riesgos de Seguridad de la Información

Son directrices y recomendaciones establecidas para identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información en la Entidad. Estos lineamientos están diseñados para ayudar a proteger los activos de información y garantizar la confidencialidad, integridad y disponibilidad de la información.

La gestión de estos lineamientos será acompañada por la Oficina TIC. Sin embargo, la responsabilidad de identificar las acciones descritas será de cada proceso al ser conocedor de la diferente información que se maneja y las mejoras prácticas para salvaguardarla.

NOTA: Los ejemplos que se presentan por cada paso son a manera de orientación y no necesariamente representaran la manera en que se debe tomar la información.

A. Paso 1: Listar los Activos por cada Proceso

En cada proceso, se deberán listar los activos de información, indicando su consecutivo, de acuerdo al identificador definido mediante la Guía para la Gestión del Inventario y Clasificación de Activos de Información e Infraestructura Crítica - GTI-GU-02. Ejemplo:

Figura 33.
Ejemplos de activos de información

PROCESO	ACTIVO	DESCRIPCION
Gestión Talento Humano	Base de datos de nómina	Base de datos con información de nómina de la entidad
Gestión Talento Humano	Aplicativo de Nómina	Servidor web que contiene el front office de la entidad
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

B. Paso 2: Identificar el Propietario y Custodios de los Activos

Cada uno de los activos identificados deberá tener establecido un propietario y custodios responsables de la información designados, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente; deberá quedar de acuerdo a la Guía para la Gestión del Inventario y Clasificación de Activos de Información e Infraestructura Crítica - GTI-GU-02.

Figura 34.
Ejemplos de definición de responsables para los activos de información

ACTIVO	DESCRIPCION	PROPIETARIO DEL ACTIVO	CUSTODIOS DEL ACTIVO
Base de datos de nómina	Base de datos con información de nómina de la entidad	Director Dirección Administrativa y de Talento Humano	Coordinador Grupo Talento Humano
Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos	Jefe Oficina TIC	Coordinador Grupo informática
Cuentas de Cobro	Formatos de cobro diligenciados	Director Dirección Financiera	Coordinador Cartera

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

C. Paso 3: Clasificar los activos

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red, entre otros.

Tabla 16.
Descripción de los tipos de activos de información

Tipo de activo	Descripción
Información y datos de la Entidad.	Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
Sistemas de información y aplicaciones de Software.	Se refieren a los componentes tecnológicos utilizados para gestionar, almacenar, procesar y transmitir información en la Entidad. Estos sistemas y aplicaciones están diseñados para ayudar a recopilar, organizar y analizar datos para apoyar las operaciones y la toma de decisiones, tales como: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
Dispositivos de Tecnologías de información – Hardware.	Equipos físicos de cómputo y de comunicaciones como servidores, biométricos, (PaaS) Plataformas como servicios, que por su criticidad son considerados activos de información.
Soporte para almacenamiento de información.	El soporte para almacenamiento de información se refiere a los medios físicos o digitales utilizados para guardar y conservar datos de manera segura y accesible. Estos soportes pueden variar según el tipo de información y las necesidades de almacenamiento de la Entidad, tales como: USB, Discos Duros, Unidades de estado sólido, CDs, SAN, NAS, Nubes de almacenamiento.
Servicios	Los servicios de computación y comunicaciones se refieren a las soluciones tecnológicas y servicios que permiten el procesamiento, almacenamiento y transmisión de información a través de sistemas informáticos y redes de comunicación, tales como: Internet, páginas de consulta, directorios compartidos e Intranet.
Recurso Humano	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Conjunto de infraestructuras físicas, redes, hardware y software necesarias para la operatividad, conectividad y seguridad de una organización, incluyendo servidores, cableado, sistemas de datos y equipos de usuario final
Redes	Conjunto de infraestructuras físicas, redes, hardware y software necesarias para la operatividad, conectividad y seguridad de una organización, incluyendo servidores, cableado, sistemas de datos y equipos de usuario final

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Figura 35.
Ejemplo de identificación de activos

ACTIVO	TIPO DE ACTIVO
Base de datos de nómina	Sistemas de Información y aplicaciones de software.
Aplicativo de Nómina	Sistemas de Información y aplicaciones de Software.
Cuentas de Cobro	Información y datos de la Entidad.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

D. Paso 4. Clasificar la información

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía para la Gestión del Inventario y Clasificación de Activos de Información e Infraestructura Crítica - GTI-GU-02 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

Figura 36.
Ejemplos de clasificación de la información

ACTIVO	TIPO DE ACTIVO	Ley 1712 de 2014	Ley 1581 de 2012
Base de datos de nómina	Sistema de Información y aplicaciones de software.	Información Reservada	No Contiene datos personales
Aplicativo de Nómina	Sistemas de Información y aplicaciones de Software	N/A	N/A
Cuentas de Cobro	Información y datos de la Entidad.	Información Pública	No contiene datos personales

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

E. Paso 5. Determinar la Criticidad del Activo (Valoración del Activo)

Ahora la entidad pública debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso. Para mayor claridad a continuación se presenta un ejemplo.

Figura 37.
Evaluación de criticidad

ACTIVO	TIPO DE ACTIVO	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de Criticidad
Base de datos de nómina	Sistema de Información y aplicaciones de software.	ALTA	ALTA	ALTA	ALTA
Aplicativo de Nómina	Sistemas de Información y aplicaciones de Software	BAJA	MEDIA	BAJA	BAJA
Cuentas de Cobro	Información y datos de la Entidad.	BAJA	MEDIA	BAJA	BAJA

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

Una vez se encuentren clasificados los activos de acuerdo con su criticidad, se procederá a realizar el análisis de sus correspondientes vulnerabilidades y amenazas según aquellos activos que se encuentren en un nivel alto o medio de criticidad según se establezca en documentos relacionados al tratamiento en términos de seguridad de la Información.

4.10.3.Identificación de Areas de Impacto

El área de impacto es la consecuencia negativa en los objetivos de la organización en caso de materializarse un riesgo o las que por causa de incidentes de seguridad de la información tenga consecuencias en la gestión de la entidad.

Una vez identificados cada uno de los elementos de una matriz de seguridad de información, tales como el proceso, referencia, activo de información, tipo de activo y la identificación del área de impacto, se procederá a identificar las áreas de factores de riesgo.

Tipo de Riesgo

La descripción del riesgo es la situación especifica que da como resultado el correspondiente riesgo y en el tipo de riesgos solo se admite uno de estos riesgos:

a. Perdida de Disponibilidad
b. Perdida de Integridad
c. Perdida de Confidencialidad

Su clasificación identifica la situación que podría presentarse o posible incidente de seguridad.

4.10.4.Análisis de Riesgo Inherente

Remitirse al capítulo de Riesgos Generales en el numeral 5.6.5 Análisis de Riesgo Inherente

A. Determinar la probabilidad: En esta actividad se debe realizar el análisis de probabilidad de la materialización de estos riesgos.

B. Frecuencia: Corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.

C. Probabilidad: Posibilidad de ocurrencia de riesgo en un proceso, para valorar la probabilidad de ocurrencia se establece un análisis de la exposición al riesgo dentro del proceso, por lo que la forma de medición se establece en cuantas veces se pasa por el punto de riesgo durante el desarrollo del proceso. Para ello se utilizan los siguientes criterios, los mismos se encuentran en la herramienta SVE.

D. % Probabilidad Inherente: Porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa.

E. Probabilidad inherente: Corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa.

4.10.5.Determinar el Impacto

Remitirse al capítulo de Riesgos Generales en el numeral 5.6.5 Análisis de Riesgo Inherente

A. Impacto: Consecuencias que se pueden producir por la materialización del riesgo en la organización, dicho impacto comprende dos grandes áreas, el área reputacional y la afectación económica de la entidad y según el tipo de riesgo se determina el grado de afectación.

B. % Impacto Inherente: Medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa.

C. Impacto Inherente: Medida del impacto económico o reputacional sobre la entidad de manera cualitativa.

4.10.6.Análisis de Severidad

Remitirse al capítulo de Riesgos Generales en el numeral **5.6.5 Análisis de Riesgo Inherente**
Zona de riesgo inherente: Determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto.

4.10.7.Diseño y Análisis de Controles

A. Valoración de Controles

Remitirse al capítulo en el numeral **5.6 Riesgos Generales de la Gestión**

a. Afectación: En esta actividad se establece la afectación que tendrá la implementación del control sobre la Probabilidad o el Impacto del riesgo.
b. Probabilidad: En este campo se especifica si el control pretende modificar la probabilidad de ocurrencia de riesgo.
c. Atributos: En esta actividad se establecen los Atributos de la implementación del control, donde se consideran atributos de eficiencia y los de formalización del control.

B. Valoración de Riesgo Residual

Remitirse al capítulo en el numeral **5.6 Riesgos Generales de la Gestión**

En esta etapa se revisa la efectividad de los controles**,** para establecer el riesgo residual.

C. Plan de implementación de controles

a. Tratamiento: En esta etapa se hace teniendo en cuenta los resultados obtenidos de la valoración de los riesgos después de controles. Las políticas identifican las opciones para tratar y manejar los riesgos con base en su valoración y permiten tomar decisiones adecuadas para evitar, reducir, compartir, transferir o asumir riesgos. En este campo se especifica el tipo de tratamiento que se realizará entre 4 opciones disponibles.

Figura 38.
Tipos de Tratamiento

Tratamiento	Descripción
Reducir el Riesgo	Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.

Compartir Riesgo	Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.
Aceptar un Riesgo	Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.
Evitar el Riesgo	Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por Ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

Nota. Opciones de tratamiento de riesgos – Elaborado por Grupo DOGI -2026

b. Plan de Acción: Se especifica la identificación del Plan de acción con el cual se realizará la implementación de dicho control.
c. Responsable: Se especifica el cargo de quien implementa el control.
d. Fecha de Implementación: Se especifica la Fecha máxima de implementación del control.
e. Seguimiento: Se especifica la periodicidad del seguimiento a la implementación del control.
f. Estado: Se especifica el estado de la implementación del control.

4.11. SEGUIMIENTO, MONITOREO Y REVISIÓN EN EL MARCO DEL ESQUEMA DE LÍNEAS DEL MODELO ESTÁNDAR DE CONTROL INTERNO MECI

De acuerdo al desarrollo de la Metodología COSO-ERM detallada en Capitulo 5.2 SOPORTE METODOLÓGICO para la política de la Gestión Integral de Riesgos y alineada con el Modelo Integrado de Planeación y Gestión (MIPG), el cual a través de la Dimensión 7 despliega los componentes de evaluación del riesgo y actividades de control en articulación con el esquema de líneas, se precisa que dicho esquema atiende de manera íntegra la gestión del riesgo al interior de la entidad, comprometiendo todos los niveles de la organización, al definir los niveles de autoridad y responsabilidad en la aplicación de controles como eje para materializar el seguimiento y monitoreo a los riesgos que enfrenta la entidad.

En ese contexto surgen los indicadores los Indicadores Clave de Riesgo (KRI), surgen como herramienta para la toma de decisiones de cara a la mitigación de riesgos.

4.11.1. Tipologías de Indicadores para el Seguimiento

Para definir adecuadamente los Indicadores (KRI) es necesario enmarcarlos en la línea estratégica de la Entidad la cual parte desde la Misión, Vision y valores Institucionales, base para la formulación de los objetivos estratégicos, los cuales, a su vez, no solamente orientan la planeación institucional, sino que también, permiten tener un despliegue hacia los objetivos de los procesos y se constituyen en la base para la identificación y formulación de

Indicadores Clave de Desempeño (KPI). Estos últimos están diseñados para medir el cumplimiento misional desde lo estratégico hasta lo operativo

Todos los indicadores se formularán con base en la metodología Guia para la Administración, Control y Seguimiento de Indicadores de Desempeño de Proceso GI-GU-01

Figura 39.
Articulación Indicadores

Fuente: Adaptado documento PricewaterhouseCoopers International Limited, Indicadores clave de riesgo por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2025.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

4.11.2.Alcance de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI)

Tabla 17.
Indicadores KPI vs Indicadores KRI

Indicadores Clave de Proceso *(KPI)*	Indicadores Clave de Riesgo (KRI)
Permiten medir periódicamente el desempeño general de la entidad y sus principales unidades operativas.	Complementan el seguimiento a los resultados de la entidad.
Se definen tomando como referencia las metas establecidas, por procesos, unidades u operaciones clave.	Proporcionan una señal temprana y oportuna de una exposición al riesgo en diversas áreas de la entidad.
Mide el rendimiento pasado, proporcionando información sobre qué tan bien se están logrando los objetivos estratégicos y operativos.	Proporcionan información útil sobre los riesgos emergentes y potenciales que pueden impactar en los objetivos estratégicos de la organización.
Ofrecen información sobre aquellos aspectos críticos de la operación que requieren mayores recursos y atención.	Ayudan a identificar y anticipar problemas que se pueden presentar interna o externamente, así como oportunidades futuras.
Permiten medir los resultados que se obtienen de la ejecución de los programas, planes y proyectos, en los diferentes momentos o etapas de su desarrollo.	Permiten realizar un monitoreo constante y mitigar los posibles eventos de riesgo que se presenten al aplicar medidas oportunas para disminuir su impacto.
Permiten mejorar la planificación, entender con mayor precisión las oportunidades de mejora de determinados procesos y analizar el desempeño de las acciones, logrando tomar decisiones con mayor certeza y confiabilidad.	Facilitan el proceso de generación de informes y el escalamiento de los riesgos

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

4.11.3.Lineamientos Generales para el Establecimiento de Indicadores Clave de Riesgo (KRI)

Lograr una adecuada comprensión de la tipología de indicadores bajo los parámetros del COSO a través del COSO-ERM donde precisa métricas utilizada por la Entidad para proporcionar una señal temprana de exposiciones al riesgo, también se identifican como métricas diseñadas con el propósito de identificar y monitorear posibles amenazas que puedan afectar el cumplimiento de los objetivos de la Entidad.

Construcción de Indicadores KRI en la ALFM

Una vez los procesos definan su mapa de riesgos institucional, identificarán con base en los lineamientos de la Guia para la Administracion, Control y Seguimiento de Indicadores de Desempeño de Proceso GI-GU-01, aquellos indicadores que se van a relacionar en el modulo de Riesgos en la herramienta SVE y harán parte del seguimiento del Riesgo definido. Estos indicadores se entenderán como los KRI del Proceso y podrán corresponder en un factor multipropósito a indicadores de gestión y de riesgos.

Tabla 18.
Ejemplo Indicadores Clave Riesgo (KRI)

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos
		% solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

4.11.4.Comunicación y Reporte KRI en el Marco del Esquema de Líneas de Aseguramiento

La asignación de roles y responsabilidades que se distribuyen en diversos servidores de la entidad y mantiene la dinámica que ha propuesto para el esquema de líneas de aseguramiento.

Tabla 19.

Seguimiento y monitoreo Indicadores Clave de Riesgo (KRI)en el marco del Esquema de Líneas de Aseguramiento

Líneas de aseguramiento	Responsable	Responsabilidad frente a los Indicadores Clave de Riesgo (KRI)
Línea Estratégica	**Alta Dirección Comité institucional de coordinación de control interno**	Incorporar en la política para la gestión integral de riesgos lineamientos sobre los Indicadores Clave de Riesgo (KRI)
		Realizar seguimiento y análisis periódico a los indicadores claves de riesgos institucionales y proponer mejoras a su estructura.
		Analizar los umbrales definidos para los Indicadores Clave de Riesgo (KRI) y sugerir ajustes de ser necesario, de tal forma que estos se alineen con los niveles aceptables para la entidad.
		Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a los indicadores claves de riesgo, así como a los indicadores clave de proceso asociados.
	Comité de Gestión y Desempeño Institucional	Realizar seguimiento y análisis periódico a los indicadores claves de desempeño de manera articulada con los indicadores clave de riesgo.
		Generar las alertas que correspondan, de acuerdo con los umbrales definidos para los Indicadores Clave de Riesgo (KRI)
1ª Línea de Aseguramiento	**Líderes de Procesos Servidores en general Responsable de las tareas del plan de mitigación, indicador, u otro plan asociado a los controles de riesgo.**	Identificar y formular los indicadores clave de riesgos que pueden alertar sobre la exposición al riesgo para los procesos, bajo su responsabilidad.
		Aplicar, medir y hacer seguimiento a los indicadores clave de riesgos, asociados en la herramienta SVE con los riesgos identificados.
		Reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos. (Plan de Mitigación)
		Informar a la Oficina Asesora de Planeación e Innovación Institucional sobre las alertas críticas resultado de la medición de los indicadores bajo su responsabilidad, por medio de la herramienta SVE modulo de Indicadores registrando la medición correspondiente.
		Si se identifica que un indicador asociado a un riesgo institucional presenta reiteratividad en el cumplimiento de su meta se aplicara las disposiciones establecidas en la Guia para la Administracion, Control y Seguimiento de Indicadores de Desempeño de Proceso GI-GU-01.
2ª Línea de Aseguramiento	**Oficina Asesora de Planeación, Líder o responsable del proceso**	Construir los tableros estratégicos que correspondan con base en la planeación institucional.
		Proponer la inclusión de los lineamientos en materia de indicadores claves de riesgo en la estructura de la política para la gestión integral de riesgos, para aprobación por parte de la Alta Dirección.
		Establecer las metodologías que guíen la medición, seguimiento y monitoreo de los indicadores claves de riesgo, asegurando que se utilicen las mejores prácticas y se implementen de manera efectiva.
		Consolidar los indicadores con mayor criticidad frente al logro de los objetivos y presentarlos a la Dirección General mediante informe.
		Asesorar a la 1ª línea para la correcta identificación, formulación e implementación de los indicadores.
3ª Línea de Aseguramiento	**Jefe Oficina Asesora de Control Interno**	Evaluar si los indicadores asociados a los riesgos son pertinentes y eficaces para la oportuna generación de alertas y/o implementación de correctivos.
		Incorporar en los seguimientos que se adelante a los riesgos la validación de los indicadores asociados a estos.

Fuente: Tomada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7.

4.11.5.Monitoreo a Riesgos.

La herramienta Suite Visión Empresarial presenta varias funcionalidades para la gestión de riesgos. En este capítulo presentaremos el monitoreo a los riesgos que no es más que una medida de autocontrol y autodetección de cualquier materialización que se pueda presentar. Esta medida es adicional a las actividades que regularmente son cargadas dentro de los planes de mitigación diseñados.

Tabla 20.
Responsabilidades y periodos de monitoreo

Línea de Defensa	Actor	Periodicidad
Primera línea de defensa	Líder o responsable del Proceso	Se realizará dos veces al año a través del plan de mitigación asociado a la gestión de riesgo dentro de la herramienta SVE. **Contenido mínimo del monitoreo:** Análisis de cambios en el contexto del proceso, Seguimiento a la ejecución de controles, Seguimiento a indicadores asociados al riesgo, Materializaciones de riesgos, validación de documentación de controles en los procedimientos, guías, manuales etc.
Segunda línea de defensa	Oficina Asesora de Planeación e Innovación Institucional	Se realizará dentro de la herramienta SVE en una actividad definida en el plan de mitigación como mínimo una vez al año **Contenido mínimo del monitoreo:** Cambios en el contexto de la organización, recomendaciones sobre el diseño de controles, perfil de riesgo, riesgos materializados y planes de mejoramiento asociados.
Tercera línea de defensa	Oficina de Control Interno	Se realizará según el plan de trabajo establecido para los ejercicios de auditoría. Adicionalmente, se realizará de forma cuatrimestral a según lo disponga la normatividad en materia de riesgos.

Nota. Responsabilidades y periodos de monitoreo– Elaborado por Grupo DOGI -2026

4.11.6.Divulgación y Ajustes de Riesgos

A. Divulgación

El Manual de administración del riesgo y el mapa de riesgos se divulgarán a todos los servidores públicos de la Agencia Logística de las Fuerzas Militares a través de herramienta SVE. De igual forma se publicará en la página web institucional en el banner del SIG.

B. Ajustes de Riesgos

Como resultado del autocontrol y la evaluación realizada por la Oficina de Control Interno o revisión de los responsables o líderes de proceso, se pueden generar circunstancias que conlleven a ajustar el riesgo. Para esto se debe solicitar por parte de los lideres de proceso, la actualización mediante el diligenciamiento del Mapa de Riesgos Integrales debidamente firmada de manera electrónica.

La Oficina Asesora de Planeación una vez recibido el mapa de riesgos integrales actualizado, realizará los ajustes en la SVE y página web en un plazo no mayor a 10 días hábiles.

De acuerdo con las normas ISO 9001:2015, 14001:2015 y 45001:2018, derivadas de las actividades de auditoría, se establece que será responsabilidad del auditor principal o de

quien proponga una acción de mejora en la herramienta SVE (Suite Vision Empresarial) definir y documentar la necesidad de revisión de los riesgos y/o controles, una vez concluido el ejercicio de seguimiento. Es importante señalar que esta revisión no necesariamente implica la materialización de los riesgos; más bien, representa la posibilidad de una falla en los controles o debilidades en la definición del riesgo identificadas durante la auditoría, las cuales deben ser evaluadas en el marco de los planes de mejora por los procesos involucrados.

Adicionalmente, se resalta la importancia de integrar este proceso de revisión en los planes de mejora, garantizando así una gestión proactiva de los riesgos y una constante optimización de los controles, lo cual contribuye significativamente a la mejora continua del sistema. En caso de ser necesario, el equipo auditor deberá colaborar estrechamente con las áreas correspondientes para implementar las acciones correctivas pertinentes y fortalecer la capacidad de la organización para gestionar eficientemente los riesgos y controles asociados.

La Oficina Asesora de Planeación e innovación institucional, definirá dentro del plan de mitigación una actividad de actualización a cada uno de los procesos, la cual debe ser ejecutada en el último trimestre del año, con el fin de actualizar los riesgos para la siguiente vigencia, ejercicio que normativamente debe quedar publicado en el portal web de la ALFM, a más tardar el 31 de enero de cada año. Este ejercicio de actualización será asesorado por el Grupo de Desarrollo Organizacional y Gestión Integral.

4.11.7.Materialización de los Riesgos

La Oficina de Control Interno podrá materializar riesgos institucionales, producto del ejercicio de las auditorías o monitoreos que realice, para ello, deberá indicar mediante informe o comunicación al líder del proceso de la novedad para que se realice la formulación del plan de mejoramiento correspondiente.
La Oficina Asesora de Planeación e Innovación Institucional, podrá materializar riesgos institucionales, producto de la aplicación del monitoreo de segunda línea de defensa informando al líder de proceso la novedad para que registre el plan de mejoramiento correspondiente

Los procesos de forma consciente de los fallos que se puedan presentar en sus procesos, podrán indicar a la Oficina asesora de Planeación mediante los monitoreos de primera línea de defensa, los riesgos materializados, para que dicha dependencia registre en la SVE la solicitud de plan de mejoramiento.

En caso de reportarse una posible materialización de un riesgo se procederá a:

A. Se realizará la solicitud de plan de mejoramiento por parte de la Oficina de Control Interno y/o la Oficina Asesora de Planeación e Innovación Institucional.
B. Cuando se indique una materialización, se deberá ajustar la probabilidad del riesgo afectado a la máxima calificación en su riesgo inherente y se evaluará el impacto de acuerdo con los efectos potenciales de afectación.

Nota: Los planes de mejoramiento deberán integrar actividades de evaluación de controles y mejora sobre estos.

5. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
00	Versión Inicial
01	Se cambió al nuevo formato
02	Se rediseñó el objetivo general y específico del Manual de Administración del Riesgo
03	Se ajustaron las responsabilidades y roles
04	Se actualizó la normatividad
05	Se incorporaron directrices de Administración de Riesgos de Fraude o corrupción.
06	Se dieron instrucciones particulares frente a la gestión de administración del riesgo por parte de las Direcciones Regionales.
07	Se cambió al nuevo formato, cambios en los formatos anexos, se incluyen los cambios correspondientes al nuevo modelo de operación.
08	Se cambia parte de la metodología por modificaciones introducidas por las guías del DAFP respecto al tema de riesgos, se adiciona metodología para la identificación y valoración de las oportunidades
09	Se incluyen disposiciones referentes a los riesgos de seguridad digital, se actualizan las imágenes según la SVE 8, se añaden actividades referentes a la materialización de los riesgos.
10	Ajuste de responsabilidades y elementos de la política de administración del riesgo consolidando un único documento, inclusión de elementos propios de la actualización metodológica establecida por el DAFP.
11	Ajuste de actividades, definición de responsabilidades en el tema de análisis de amenazas y vulnerabilidades de los activos de información. Ajuste de responsabilidades, inclusión de elementos propios de la actualización metodológica establecida por el DAFP. Inclusión de los riesgos ficales según la guía de administración de riesgos del DAFP, se modifica el flujo de administración de riesgos en temas de materialización, se ajustan las responsabilidades alineándolas al modelo de líneas de defensa del MIPG.
12	Se ajustan conceptos referentes a seguridad de la información y se añaden nuevas definiciones.
13	Se actualiza de acuerdo a la Guia No 7 de Función Pública – incluido lo del SIGRIP