AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

MANUAL DE ADMINISTRACIÓN DE RIESGOS Y OPORTUNIDADES

ELABORÓ	REVISÓ	APROBÓ
NOMBRE Fabián Ernesto Pongutá Castro	NOMBRE Ing. Sis. Cesar Adolfo Gonzalez Peña Adm. Emp. Jaime Rafael Morón Barros	NOMBRE Abo. Martha Eugenia Cortes Baquero
CARGO Coordinador Grupo Desarrollo Organizacional y Gestión Integral	CARGO Coordinador Grupo Redes e Infraestructura Oficina TIC Jefe Oficina Asesora de Planeación e Innovación Institucional	CARGO Jefe Oficina Asesora Jurídica encargada de las funciones de la Dirección General de la Agencia Logística de las Fuerzas Militares
FIRMA	FIRMA FIRMA	FIRMA

TABLA DE CONTENIDO

INTRODUCCIÓN 4
OBJETIVO DEL MANUAL 5
1. ALCANCE 5
2. REFERENCIA NORMATIVA 5
3. DEFINICIONES 7
4. CUERPO DEL MANUAL 10
4.1. OBJETIVOS ESPECÍFICOS 10
4.2. SOPORTE METODOLÓGICO 10
4.3. PARA ESTE PROCESO SE TIENEN LOS SIGUIENTES DOCUMENTOS: 10
4.3.1. Mapa de riesgos por procesos: 10
4.3.2. *Identificación de activos de información por proceso:* 11
4.3.3. La información consolidada resultado de la administración de riesgo: 11
4.4. CONTEXTO 11
4.5. CLASIFICACIÓN DE LOS RIESGOS Y OPORTUNIDADES 13
4.6. RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS 14
4.6.1. Línea estratégica 14
4.6.2. Primera línea de defensa 14
4.6.3. Tercera línea de defensa 19
4.7. RESPONSABILIDADES PARA LAS OPORTUNIDADES 19
4.8. MAPA DE RIESGOS Y OPORTUNIDADES 20
4.9. IDENTIFICACIÓN DE RIESGOS Y OPORTUNIDADES 23
4.9.1. *Proceso* 23
4.9.2. *Objetivo del proceso* 23
4.9.3. *Riesgo* 23
4.9.4. Oportunidad 24
4.9.5. Detalle 24
4.10. RIESGOS INHERENTES DE SEGURIDAD DIGITAL. 25
4.11. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 25
4.11.1. Paso 1: Listar los activos por cada proceso 25
4.11.2. Paso 2: Identificar el propietario y custodios de los activos 26
4.11.3. Paso 3: Clasificar los activos 26
4.11.4. Paso 4. Clasificar la información 27
4.11.5. Paso 5. Determinar la criticidad del activo (valoración del activo) 27

A. *Clasificación de acuerdo con la confidencialidad.* 28

B. *Clasificación de acuerdo con la integridad* 28

C. *Clasificación de acuerdo con la disponibilidad* 29

4.12. ANÁLISIS DE LOS RIESGOS 29

4.12.1 Análisis del riesgo 29

4.12.2 Clasificación de riesgos 33

4.12.3 Valoración del riesgo 34

A. Identificación de Controles. 34

B. Valoración de Controles 35

C. Plan o acciones de contingencia 38

D. Tratamiento del Riesgo 39

4.13. ANALISIS DEL RIESGO FISCAL 40

4.13.1 Identificación de riesgos fiscales 40

4.13.2 Identificación de áreas de impacto 42

A. Riesgos de daño antijurídico. 42

B. Efectos económicos generados por causas externas. 42

4.13.3 Identificación de la causa raíz o potencial hecho generador 42

4.13.4 Descripción del riesgo fiscal 42

4.14. ANÁLISIS DE LAS OPORTUNIDADES 43

4.14.1 Análisis de la Oportunidad 43

4.14.2 Valoración de las oportunidades 44

A. Identificación de controles o actividades para la gestión de la oportunidad 45

B. Valoración de Controles 45

C. Tratamiento de la oportunidad. 46

4.15. MAPA DE RIESGOS INSTITUCIONAL, DE FRAUDE O CORRUPCIÓN Y DE OPORTUNIDADES. 47

4.16. SEGUIMIENTO 47

4.17. MONITOREO A RIESGOS Y OPORTUNIDADES 48

4.18. DIVULGACIÓN Y AJUSTES DE UN RIESGO 49

4.18.1. Divulgación 49

4.18.2 Ajustes del Riesgo 49

4.18.3 Materialización de los riesgos 50

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 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. El Mapa de Riesgos presentado en este manual, estructurado en un enfoque por procesos, refleja un esfuerzo conjunto de todos los servidores públicos vinculados a la Entidad. La gestión del riesgo establece pautas precisas para el tratamiento, manejo y seguimiento de los riesgos.

OBJETIVO DEL MANUAL

Establecer la política y orientar 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, y a su vez potenciar las actividades que favorezcan las oportunidades que se presenten dentro de la entidad, a través de los elementos como contexto estratégico, identificación de riesgos y oportunidades, análisis y valoración de las mismas, su trazabilidad, registro y monitoreo.

1. ALCANCE

La administración de riesgos y oportunidades 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 de los procesos 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.

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 V5 marzo de 2023	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 V5 Diciembre de 2020	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 la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea 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.
Capacidad de riesgo	Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
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.
Causa Raíz	Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
Cliente	Organización, entidad o persona que recibe un producto y/o servicio.
Confidencialidad	Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
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.
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
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.
Frecuencia	Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
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.
Integridad	Propiedad de exactitud y completitud.
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.
No repudio	Permite probar la participación de las diferentes partes en la interacción de la información y la comunicación.

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.
Reducción del riesgo	Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia
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)
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.
Sistema de Administración de Riesgo	Conjunto de elementos del direccionamiento estratégico de una entidad concerniente a la Administración del Riesgo.
SIG	Sistema Integrado de Gestión
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.
Valoración del riesgo:	Es el resultado de confrontar la evaluación del riesgo con los controles existentes.
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. OBJETIVOS ESPECÍFICOS

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

Identificar en los procesos y actividades los eventos que afecten el logro de los objetivos.

Identificar los riesgos críticos, a fin de implementar el mapa de riesgos institucional y las acciones de mitigación sobre aquellos que puedan causar mayor daño al momento de materializarse.
Identificar las oportunidades potenciales, a fin de implementar el mapa de riesgos y oportunidades al igual que las acciones para abordar las más importantes que puedan causar mayor beneficio al momento de materializarse.

Reducir la vulnerabilidad y fortalecer la prevención y mitigación de los efectos de los riesgos.

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

Construir el mapa de riesgos y oportunidades por proceso de manera coherente y ordenada para proceder a identificar y definir los correspondientes controles.

Involucrar y comprometer a los funcionarios de la ALFM en el proceso de administración del riesgo y oportunidades de la entidad, y en la búsqueda de acciones encaminadas a prevenir y mitigar el riesgo al igual que a potenciar las oportunidades.

4.2. SOPORTE METODOLÓGICO

Para la elaboración del Mapa de riesgos y oportunidades institucionales 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- y los requisitos de las normas ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 27001:2022.

4.3. PARA ESTE PROCESO SE TIENEN LOS SIGUIENTES DOCUMENTOS:

4.3.1. Mapa de riesgos por procesos:

En el cual se elevan todos los riesgos que afecten a la entidad en su conjunto y los riesgos identificados de los procesos Misionales y se incluirán los riesgos de fraude o corrupción de los que trata la Ley 1474 de 2011.

4.3.2. *Identificación 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.

4.3.3. La información consolidada resultado de la administración de riesgo:

Se podrá consultar en la herramienta Suite Visión Empresarial (SVE), en la cual se hará la gestión de las acciones propuestas para los riesgos y las oportunidades.

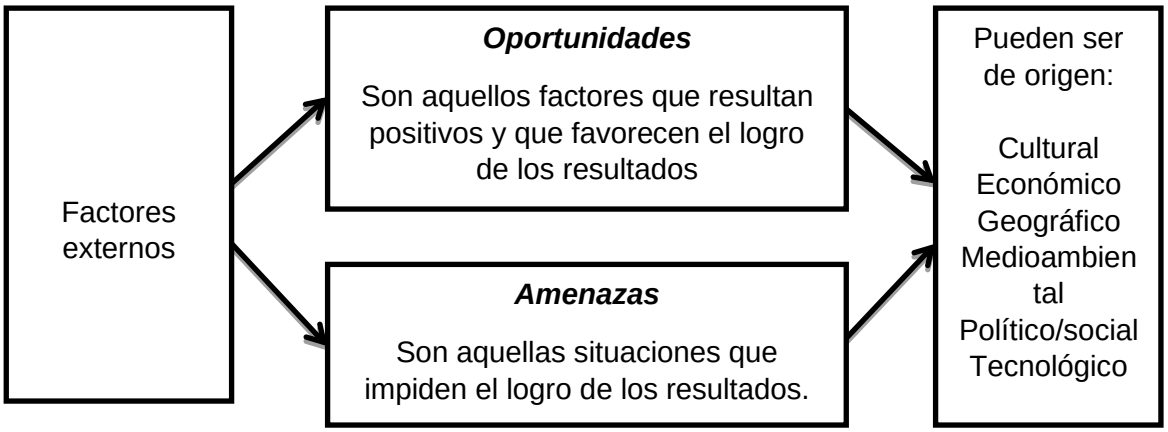
4.4. CONTEXTO

Son las condiciones internas y del entorno, que pueden generar efectos positivos originando oportunidades o afectando negativamente el cumplimiento de la misión y los objetivos de una institución o a cada uno de los procesos definidos. Para determinar los diferentes factores internos y externos se aplica la herramienta de gestión denominada matriz DOFA. Con el fin de mantener la información documentada la Oficina Asesora de Planeación e Innovación Institucional definirá el formato necesario para los análisis, este análisis se revisará de manera anual junto con los riesgos de los procesos y se ajustará en caso de considerarse necesario en las revisiones.

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

Figura 1.

Establecimiento del contexto



Nota: Factores externos del entorno – Creado por Grupo DOGI -2024

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 2.

Determinación de fortalezas y debilidades

Nota: Determinación de fortalezas y debilidades – Elaborado por Grupo DOGI -2024

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

Tabla 3.

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.	
SOCIALES: Demografía, responsabilidad social, terrorismo.	**TECNOLOGÍA**: Integridad, disponibilidad y accesibilidad a los datos, aplicativos y sistemas de información, desarrollo, producción, mantenimiento.
TECNOLÓGICOS: Interrupciones comercio electrónico, datos externos, tecnología emergente.	

Nota: Ejemplos de factores internos y externos – Elaborado por Grupo DOGI –2024

Esta etapa se documenta mediante análisis de contexto interno y externo, se recomienda el uso de la metodología DOFA, sin embargo, podrá realizarse con la herramienta que la entidad considere pertinente.

4.5. CLASIFICACIÓN DE LOS RIESGOS Y OPORTUNIDADES

Teniendo claro el contexto de los riesgos se deben clasificar en las siguientes clases:

Tabla 4.

Definición de tipos de riesgo

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude o corrupción externo	Pérdida derivada de actos de fraude o corrupción por personas ajenas a la organización (no participa personal de la entidad).
Fraude o corrupción interno	Pérdida debido a actos de fraude o corrupción, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Nota: Definición de tipos de riesgos – Elaborado por Grupo DOGI –2024

Dentro del mismo análisis de riesgos es posible identificar las oportunidades que se presentan en cada uno de los procesos de la entidad, estas oportunidades presentan una clasificación propia, sin embargo, se debe tener en cuenta que las mismas representan efectos positivos para la Entidad, en este orden de ideas, se deberá entender la definición en términos positivos de los riesgos, las oportunidades serán clasificadas en:

Oportunidades Estratégicas
Oportunidades Operativas
Oportunidades Financieras

Oportunidades de Cumplimiento
Oportunidades de Tecnología
Oportunidades de Imagen

4.6. 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).

4.6.1. 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.

4.6.2. 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.

En resumen, la primera línea de defensa tiene la responsabilidad de identificar, evaluar, implementar controles, monitorear y reportar los riesgos asociados con las actividades y procesos que ejecutan. Su enfoque principal es la gestión cotidiana de los riesgos y la implementación efectiva de controles.

4.6.3 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.

Entre los parámetros a tener en cuenta, para definir esta línea son los siguientes:

A. **Pertenecer a la media o alta gerencia:** Dentro del Organigrama aquellos cargos que dependen del Representante Legal (Alta Gerencia), Para Media Gerencia, aquellos que se desprenden de los cargos anteriormente mencionados.
B. **Responder ante la Alta Dirección:** Aquel cargo que maneja un tema transversal para toda la entidad y responde ante el Representante Legal.
C. **Evaluar y efectuar seguimiento a los controles aplicados por la 1ª línea de defensa**.

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

1) **Gestión Estratégica de Riesgos:** La 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.

2) **Gestión Táctica de Riesgos: La 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.

3) Gestión Operacional de Riesgos: La 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.

En resumen, la gestión estratégica de riesgos se enfoca en la dirección estratégica y la toma de decisiones a largo plazo, la gestión táctica de riesgos se centra en la implementación de las estrategias establecidas, y la gestión operacional de riesgos se enfoca en la ejecución diaria de las acciones de gestión de riesgos y el cumplimiento de los controles. Cada nivel de gestión es importante y complementario en la gestión integral de riesgos en el marco del MIPG.

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. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (en orden jerárquico: jefe de oficina asesora de planeación e innovación institucional – componente estratégico – secretario general, jefes de oficina, subdirectores generales, directores nacionales, directores regionales y supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc. – componente táctico y operacional –)

El jefe de la Oficina Asesora de Planeación e Innovación Institucional, líderes de proceso o responsables que se asignen deben monitorear y revisar 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 digital 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 digital, 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 digital.
- 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 Digital.

- Elaborar y actualizar Planes de Tratamiento de Riesgos e indicadores de Seguridad Digital.
- 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 Digital.
- 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 Digital.

4.6.3. 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:

A. 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.

B. 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.

C. 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 de fraude o corrupción 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.

4.7. RESPONSABILIDADES PARA LAS OPORTUNIDADES

Tabla 5.

Funciones de las áreas organizativas

RESPONSABLE	FUNCIÓN
Alta Dirección	• Establecer la metodología para riesgos y oportunidades.

	• Realizar seguimiento y análisis de las oportunidades.
Secretario General, Subdirectores Generales, Jefes de Oficina, Directores Nacionales, Directores Regionales y Responsables de Procesos	• Identificar los riesgos, oportunidades y controles de procesos y proyectos a cargo en cada vigencia. • Realizar seguimiento y análisis a los controles y actividades asociadas de los riesgos y oportunidades según periodicidad establecida en la herramienta SVE. • Actualizar de manera oportuna el mapa de riesgos y oportunidades 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 y oportunidades. • Consolidar el Mapa de riesgos/oportunidades institucionales y de fraude o corrupción de la entidad.
Todos los funcionarios	• Participarán en la realización e implementación del Mapa de Riesgos y Oportunidades 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.

Nota: Funciones de las áreas Organizativas – Elaborado por Grupo DOGI –2024

4.8. MAPA DE RIESGOS Y OPORTUNIDADES

El mapa de riesgos y oportunidades 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.
La fecha del mapa de riesgos y oportunidades por proceso, corresponde a la fecha de actualización más reciente frente a la información consignada plataforma SVE.

Respecto al Mapa de riesgos institucionales, 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.

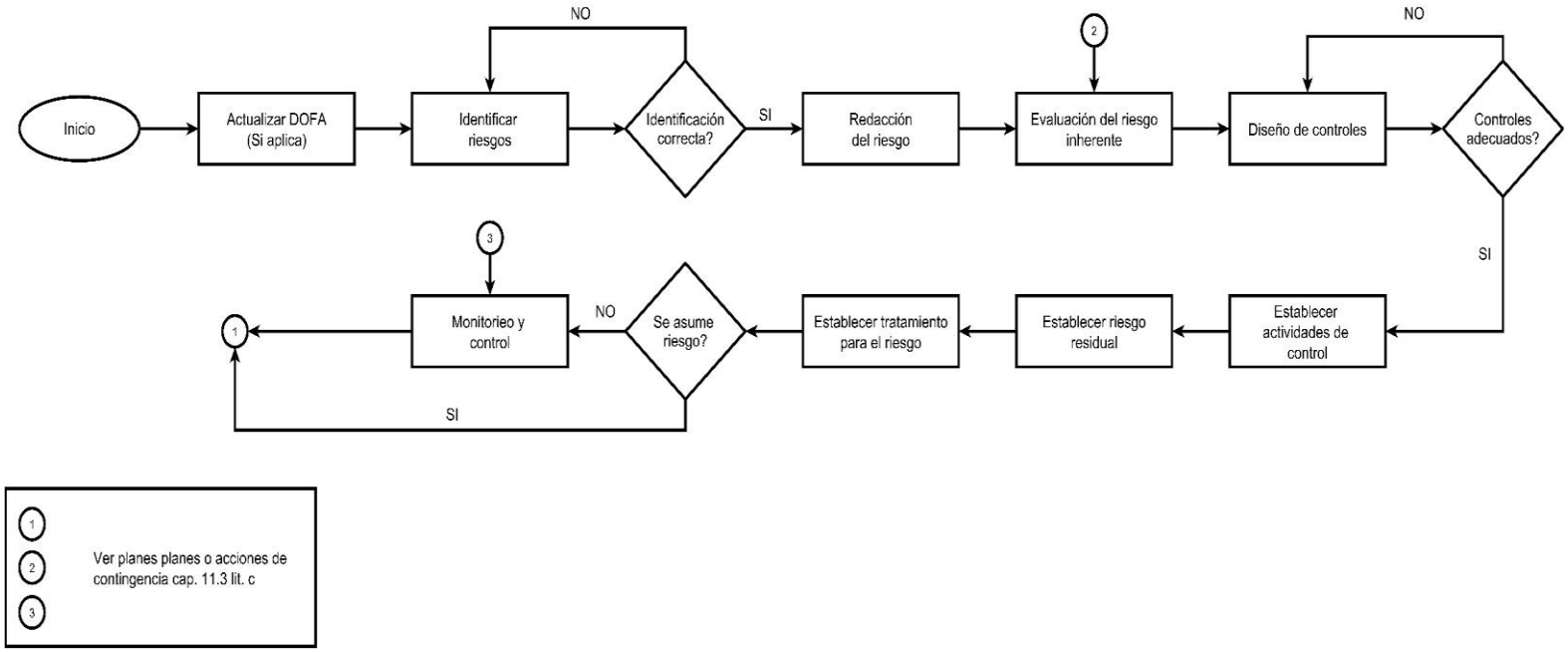
El Mapa de riesgos en la herramienta Suite Visión Empresarial – Modulo de gestión del riesgo – tiene vinculado el plan de mitigación, indicadores u otros planes que soporten la ejecución de los controles definidos para los riesgos, allí se puede consultar el avance de las acciones propuestas y esta información 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 de la matriz de riesgos 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 y el plan asociado a la gestión de las oportunidades se encuentra en el módulo “planes” de la SVE, desde allí se direccionan las actividades para las oportunidades y riesgos identificados.

En general, el despliegue de la metodología descrita en el manual sigue el flujo que se describe más adelante, cada una de las acciones contempladas para el flujo son explicadas metodológicamente en

cada una de las secciones del presente manual. Desde el siguiente grafico es posible abstraer que la gestión de riesgos es un proceso permanente que no tiene un final planificado debido a la dinámica de las organizaciones y el ciclo propio de la mejora continua.

FLUJO DE ADMINISTRACIÓN DEL RIESGO



4.9. IDENTIFICACIÓN DE RIESGOS Y OPORTUNIDADES

Para esta etapa del proceso, hay que tener en cuenta que este es permanente e interactivo, y basado tanto en el resultado del análisis del Contexto Estratégico como en el proceso de planeación. Una vez definidos los factores internos y externos, se identifican los eventos (riesgos y oportunidades) que afecten el logro de los objetivos de los procesos, siendo ésta la base del análisis de riesgos y oportunidades que permite avanzar hacia una adecuada implementación de políticas que conduzcan a su control o potencialización.

Para una fácil identificación se pueden apoyar en las amenazas y debilidades del punto "Contexto Estratégico", que contribuyen a la definición de factores de riesgo. Adicionalmente las fortalezas y las oportunidades contribuyen a la contextualización de las mismas según se explica en la gráfica siguiente.

Figura 3.

Ejemplo de análisis de contexto e identificación de riesgos y oportunidades

		ANÁLISIS INTERNO	
		DEBILIDADES	**FORTALEZAS**
ANÁLISIS EXTERNO	**OPORTUNIDADES**	**Estrategias de Reorientación:** ¿Cómo minimizar/superar debilidades para aprovechar oportunidades?	**Estrategias de Crecimiento / Ofensivas:** ¿Cómo me permiten las fortalezas aprovechar las oportunidades?
	AMENAZAS	**Estrategias de Supervivencia:** ¿Cómo evito que la debilidad refuerce la amenaza? ¿Cómo reduzco la debilidad y/o eludo la amenaza?	**Estrategias de Conservación/Defensivas:** ¿Cómo aprovecho las fortalezas para contrarrestar amenazas?
		↑ **Zona de riesgo**	↑ **Zona de oportunidades**

Nota: Ejemplo de análisis de contexto – Elaborado por Grupo DOGI –2024

En esta etapa es donde se identifican los riesgos y las oportunidades, lo cual es importante tener en cuenta las siguientes variables:

4.9.1. *Proceso*

Nombre del Proceso.

4.9.2. *Objetivo del proceso*

Se debe transcribir el objetivo que se ha definido para el proceso, al cual se le están identificando los riesgos.

4.9.3. *Riesgo*

Representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones y afectar total o parcialmente la operación y el logro de los objetivos institucionales.

4.9.4. Oportunidad

Diferencia detectada en la Entidad, entre una situación real y una situación deseada. La oportunidad puede afectar a un proceso, producto, servicio, recurso, sistema, habilidad, competencia o área de la Entidad.

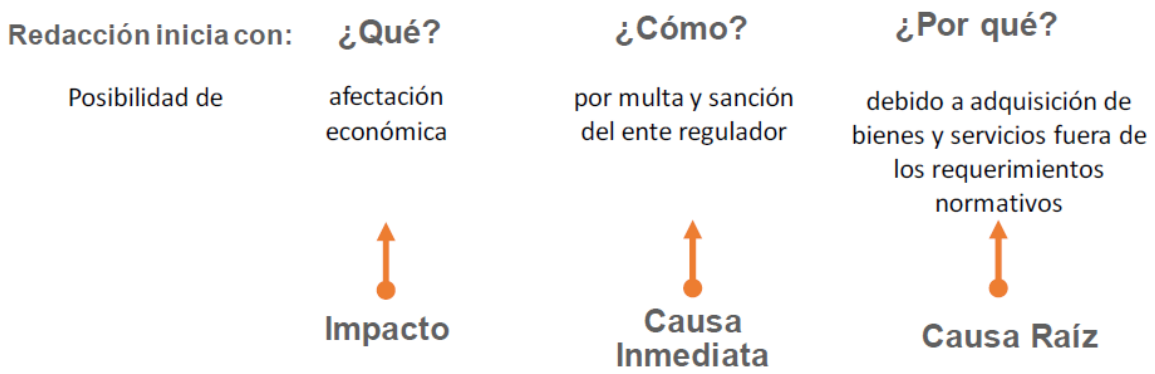
4.9.5. Detalle

Corresponde a la descripción del riesgo o la oportunidad en términos claros y comprensibles, se sugiere tener en cuenta los aspectos que se describen más adelante.

NOTA: El riesgo ya sea de Gestión o de fraude o corrupción debe estar descrito de manera clara, de la misma manera que las oportunidades que se identifiquen, sin que su redacción dé lugar a ambigüedades o confusiones con la causa generadora de los mismos. Por tal motivo para la identificación de los riesgos se ha determinado la siguiente estructura:

Figura 4.

Identificación y redacción de riesgos



Nota: Identificación y redacción de riesgos – Tomado de Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 (DAFP)

A. **Descripción de la materialización:** Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo o la oportunidad identificada.
B. ***Causas (factores internos o externos):*** Son los medios, las circunstancias y agentes generadores de riesgo o potenciadores de las oportunidades. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo o una oportunidad.
C. **Tipo de riesgo u oportunidad**: Definir la clasificación del riesgo o la oportunidad, identificando en la justificación de por qué es de gestión o de fraude o corrupción, en el caso de los riesgos, o cualquier tipología teniendo en cuenta las descripciones de situaciones no deseadas, o aquellas oportunidades que se pretendan abordar. Para definir el riesgo es necesario tener cuenta una estructura concreta que permite que la definición sea de carácter concreta y fácil de entender, dicha estructura se establece que le riesgo debe comprenderse teniendo en cuenta tres elementos concretos: el impacto, la causa inmediata y la causa raíz que representan las preguntas Que, Como y Porque, Dichos elementos permiten destacar información esencial que se requerirá a la hora de establecer los controles

D. ***Efectos (consecuencias o beneficios):*** Constituyen las consecuencias o beneficios de la ocurrencia del riesgo o de la oportunidad sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y fallecimiento, sanciones, pérdidas económicas, de información y activos, de bienes, de imagen y reputación corporativa , de credibilidad y de confianza, interrupción del servicio y daño ambiental, como es en el caso de los riesgos, o bien se pueden considerar los efectos positivos en términos de mejoramiento de las condiciones de operación para el caso de las oportunidades.

4.10. RIESGOS INHERENTES DE SEGURIDAD DIGITAL.

Para efectos del presente manual y según lo establecido en las diferentes guías del DAFP se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital de ellos se pueden establecer cualquiera que se considere relacionado con ellos.

Pérdida de la confidencialidad

Pérdida de la integridad

Pérdida de la disponibilidad

Para dar alcance a este tipo de riesgos, se dedicará un capítulo del presente manual para describir la metodología por usar.

4.11. 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 y la Oficina Asesora de Planeación e Innovación Institucional, esta última cuando se requiera. 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.

4.11.1. 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 y clasificación de activos de información, nombre y descripción breve de cada uno.

Ejemplo:

Tabla 6.

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

Nota: Ejemplos de activos de información – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

4.11.2. 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.

Ejemplo:

Tabla 7.

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

Nota. Ejemplos de definición de responsables para activos de infomación – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

4.11.3. 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 8.

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 –	Equipos físicos de cómputo y de comunicaciones como servidores, biométricos, (PaaS) Plataformas como servicios, que por su criticidad son considerados activos de información.

Hardware.	
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.

NTA. Descripción tipos de activos de información – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

Ejemplo:

Tabla 9.

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.

Nota Ejemplo identificación activos – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

4.11.4. 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 de Gestión de Activos y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

Tabla 10.

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

Nota. Ejemplo clasificación de información – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

4.11.5. 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.

Tabla 11.

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

Nota. Evaluación de criticidad – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

A. *Clasificación de acuerdo con la confidencialidad.*

Tabla 12.

Niveles de confidencialidad

INFORMACIÓN PUBLICA RESERVADA/CONFIDENCIAL (Alto)	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBLICA CLASIFICADA/USO INTERNO (Medio)	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA (Bajo)	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. Niveles de criticidad – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

B. *Clasificación de acuerdo con la integridad*

Tabla 13.

Clasificación de la integridad

Alto	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.
Medio	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.
Bajo	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. Clasificación de la Integridad – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

C. ***Clasificación de acuerdo con la disponibilidad***

Tabla 14.

Clasificación de la disponibilidad

Alto	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.
Medio	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.
Bajo	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.

Nota. Clasificación de la Disponibilidad – Tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

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 digital.

4.12. ANÁLISIS DE LOS RIESGOS

En este capítulo se explorará la metodología para el análisis de los riesgos ya identificados, las oportunidades serán abordadas en el capítulo 12 del presente manual, ya que, aunque se trata de una metodología similar, algunas diferencias deben ser detalladas.

4.12.1. Análisis del riesgo

El análisis del riesgo tiene como principal objetivo, establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias que genera en los procesos de la entidad, al igual que calificarlos y evaluarlos, con el fin de obtener la información necesaria para establecer el nivel del riesgo y las acciones que se deben emprender para el manejo del mismo.

Hay que tener en cuenta que, el cumplimiento del objetivo de esta etapa será posible, dependiendo de la información que se obtenga en el formato de identificación de riesgos y de la disponibilidad de datos históricos, sumado del aporte de los funcionarios de la Agencia Logística de las Fuerzas Militares.

La probabilidad, que hace referencia a la 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.

Tabla 15.

Ejemplos de factores internos y externos

	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%

Nota. Ejemplos de Factores Internos y Externos – Tomado Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

A continuación, se presenta un ejemplo del análisis realizado frente a diferentes actividades de los procesos:

Tabla 16.

Ejemplo de establecimiento de la probabilidad

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	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

Nota. Ejemplos de establecimiento de la probabilidad – Tomado Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

El impacto tiene que ver con las 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.

Tabla 17.

Criterios de impacto para riesgos de gestión

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, 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

Nota Ejemplos de establecimiento de la probabilidad– Tomado Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Tabla 18.

Criterios de impacto para riesgos de seguridad digital

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		Impacto (consecuencias) Cuantitativo	**Impacto (consecuencias) Cualitativo**
Leve	**20%**	Afectación ≥X% de la **población.** Afectación ≥X% del presupuesto anual de la entidad No hay Afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad Sin afectación de la confidencialidad.
MENOR	**40%**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del Medio Ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad Afectación leve de la disponibilidad Afectación leve de la confidencialidad.
MODERADO	**60%**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del Medio Ambiente requiere de ≥X semanas de recuperación	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.

			Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	**80%**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del Medio Ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	**100%**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del Medio Ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros.

Nota Criterios de impacto para riesgos de seguridad digital – Tomado del DAFP -2020

<u>Tratándose de riesgos de fraude o corrupción el impacto siempre será negativo; en este orden de ideas, y como regla general no aplica la descripción de riesgos insignificante o menores señalados en la Guía de Función Pública por lo tanto no será procedente calificarlos con esos niveles de impacto en el formato de matriz de riesgos.</u>

Adicionalmente, para la calificación del impacto de los riesgos de fraude o corrupción deberá usarse la lista de verificación que se expone a continuación:

Tabla 19.

Formato para determinar el Impacto en los Riesgos de Fraude o corrupción

N°	**Pregunta riesgo de fraude o corrupción se materializa podría...**	**Respuesta**	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad?		

4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos Penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
Total preguntas afirmativas_____ **Total, preguntas negativas**_____			
Clasificación del Riesgo:			

Nota Formato para determinar el impacto en los riesgos de Fraude o de corrupción – Elaborado por Grupo DOGI -2024

Respuestas:

Responder afirmativamente de UNO a CINCO preguntas(s) genera un impacto **Moderado**.

Responder afirmativamente de SEIS a ONCE preguntas genera un impacto **Mayor.**

Responder afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto **Catastrófico**.

4.12.2. Clasificación de riesgos

Esta se da a través de la estimación de la probabilidad de la ocurrencia, que expresa cuantas veces se pasa por el punto de riesgo durante el desarrollo de determinado proceso; y el impacto, que se califica según la magnitud de los efectos, todo lo anterior, por la materialización del riesgo.

Tabla 20.

Calificación de Riesgos de Fraude o corrupción Impacto

NIVEL	RESPUESTA	DESCRIPCIÓN
1	1-5	Moderado
2	6-11	Mayor
3	12-18	Catastrófico

Nota. Clasificación de Riegos de fraude o de Corrupción – Tomado del DAFP-2020

4.12.3. Valoración del riesgo

La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

Figura 5.

Mapa de calor.

Probabilidad	Zonas de Riesgo				
Muy alta 100%					
Alta 80%					
Media 60%					
Baja 40%					
Muy baja 20%					
Impacto	**Leve 20%**	**Menor 40%**	**Moderado 60%**	**Mayor 80%**	**Catastrófico 100%**

Extremo

Alto

Moderado

Bajo

Nota. Mapa de calor – Tomado Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

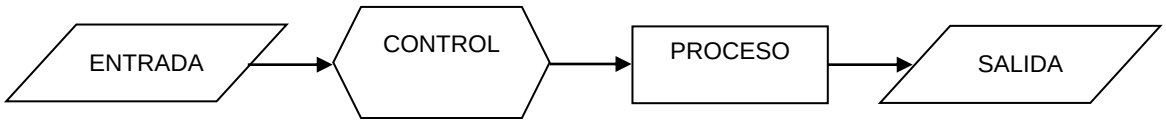
A. Identificación de Controles.

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

1) **Preventivos:** 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 6.

Controles preventivos

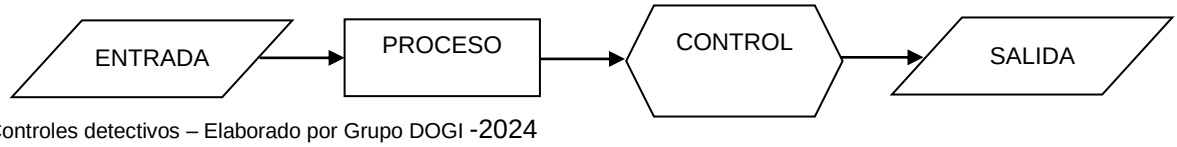


Nota. Controles preventivos – Elaborado por Grupo DOGI -2024

2) **Detectivos:** 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 7.

Controles detectivos

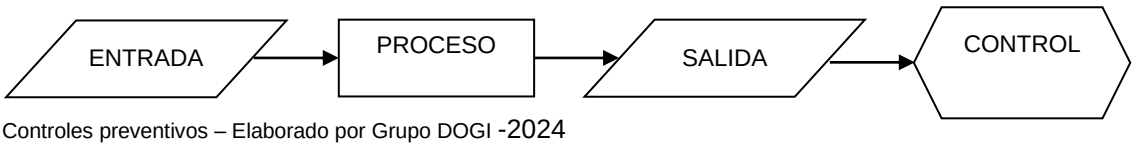


Nota. Controles detectivos – Elaborado por Grupo DOGI -2024

3) **Correctivos:** 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 8.

Controles correctivos



Nota. Controles preventivos – Elaborado por Grupo DOGI -2024

- **Control manual**: Controles que son ejecutados directamente por el funcionario.
- **Control automático**: Son aquellos ejecutados por sistemas de información o automatizados.

B. 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.

Tabla 21.

Calificación de atributos.

Características			Descripción	Peso
Atributos de eficiencia		Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Nota. Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente- Tomado del DNP -2020.

Para la aplicación de los controles se debe tener en cuenta que los 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.

El siguiente ejemplo muestra de forma adecuada como se realiza el proceso descrito.

Tabla 22.

Tabla de evaluación de controles.

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25.2%
	Probabilidad Residual	**25.2%**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Nota. En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto. – Tomado Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que se muestra 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 9.

Mapa de calor.

Preventivos detectivos

Atacan Probabilidad

Probabilidad	Zonas de Riesgo				
Muy alta 100%					
Alta 80%					
Media 60%					
Baja 40%					
Muy baja 20%					
Impacto	**Leve 20%**	**Menor 40%**	**Moderado 60%**	**Mayor 80%**	**Catastrófico 100%**

Controles correctivos

Atacan impacto

Nota. Mapa de Calor – Elaborado por Grupo DOGI -2024

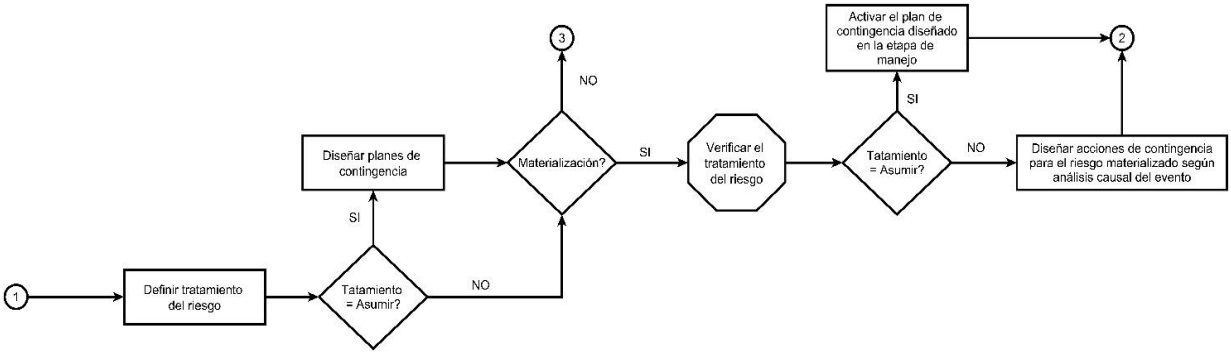
El resultado obtenido a través de la valoración del riesgo, es denominado también tratamiento del riesgo, ya que se “involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales acciones” así el desplazamiento dentro de la Matriz de Evaluación y Calificación determinará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

C. Plan o acciones de contingencia

Es una forma de organizarse para actuar frente a un evento posible. El plan o acciones de contingencia establece las medidas a tomar, las tareas a realizar, los recursos que se necesitan, las indicaciones y las competencias del equipo indispensable para actuar en caso de materialización de un riesgo. La formulación de planes de contingencia es aplicable para aquellos riesgos en los cuales se decidió “Asumir el riesgo”. Así mismo, se deberán diseñar acciones de contingencia basadas en análisis causal una vez se haya materializado un riesgo siempre y cuando este evento sea informado al componente estratégico de la segunda línea de defensa por cualquiera de los canales de comunicación dispuestos (monitoreo a través de SVE o informes de auditoría). En el caso de tratamiento “asumir” este tipo de planes estarán asociados a los controles de tipo correctivo. Para eventos de materialización las acciones serán analizadas y diseñadas una vez el evento de materialización sea informado.

Figura 10.

Proceso de gestión de riesgos ALFM.



Nota. Proceso Gestión de Riesgos – Elaborado por Grupo DOGI -2024

D. Tratamiento del Riesgo

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.

Tabla 23.

Opciones de tratamiento de riesgos.

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.
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 o Transferir el 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.
Asumir 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.

Nota. Opciones de tratamiento de riesgos – Elaborado por Grupo DOGI -2024

Una vez implantadas las acciones para el manejo de los riesgos, la valoración después de controles se denomina riesgo residual, éste se define como aquel que permanece después que la dirección desarrolle sus respuestas a los riesgos.

Tabla 24.

Posibilidades de tratamiento de riesgo según zona de riesgo.

ZONA DE RIESGO	COLOR	DESCRIPCIÓN
Baja		Asumir el riesgo.
Moderada		Asumir el riesgo, Reducir el riesgo.
Alta		Reducir el riesgo, Evitar el riesgo, Compartir o transferir.
Extrema		Evitar el riesgo, reducir el riesgo, Compartir o transferir.

Nota. Probabilidad de tratamiento de riesgos según zona de riesgos – Elaborado por Grupo DOGI -2024

4.13. ANALISIS DEL RIESGO FISCAL

El riesgo fiscal puede ser definido como "*Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.*", este tipo de riesgo debe ser incluido en la matriz de riesgos institucionales y de corrupción de la entidad. Este tipo de riesgos tienen pasos diferentes para su identificación y posible tratamiento.

4.13.1. Identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

Para la identificación del riesgo fiscal se sigue la misma estructura presentada en el capítulo 9 del presente manual. Sin embargo, es necesario tener en cuenta que existen herramientas para la correcta identificación de esta clase de riesgos, a continuación, se presentan las preguntas orientadoras sugeridas por el DAFP.

Tabla 25.

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	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 **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.
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" (anexo1), son aplicables a la entidad?

Nota. Identificación de riesgos fiscales – Tomado Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

4.13.2. Identificación de áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre se refiere a las consecuencias económicas que afectarían el patrimonio público si el riesgo se materializara. Es importante destacar que no todos los efectos económicos están relacionados con riesgos fiscales, pero todos los riesgos fiscales representan un efecto económico perjudicial para los bienes, recursos o intereses patrimoniales de naturaleza pública.
Algunos ejemplos de efectos económicos que no son riesgos fiscales son los siguientes:

A. Riesgos de daño antijurídico.

Estos implican el riesgo de tener que realizar pagos por condenas o acuerdos legales.

B. Efectos económicos generados por causas externas.

Estos no están relacionados con las acciones u omisiones de los funcionarios públicos. Incluyen situaciones de fuerza mayor, eventos fortuitos o acciones de terceros que no sean funcionarios públicos.

4.13.3. Identificación de la causa raíz o potencial hecho generador

Existe una relación de causa y efecto entre la causa raíz o potencial evento generador y el daño resultante. Por lo tanto, para determinar la causa raíz o evento generador potencial, es necesario identificar la acción u omisión que perjudica el patrimonio estatal.
Es fundamental llevar a cabo una gestión adecuada de los riesgos fiscales, lo que implica una identificación de las causas de manera objetiva y rigurosa. Los controles diseñados e implementados deben dirigirse a abordar estas causas, con el objetivo de prevenir la ocurrencia de daños fiscales.

4.13.4. 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 (área de impacto).*

C. ***Circunstancia inmediata.*** *Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.*

D. ***Causa Raíz.*** *Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.*

A continuación, se presenta un ejemplo de redacción para riesgo fiscal:

Tabla 26.

Redacción de riesgos fiscales.

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre bienes públicos	por pérdida, extravío o hurto de bienes muebles de la entidad.	A causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Nota. Redacción de riesgos fiscales – Elaborado por Grupo DOGI -2024

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*"

4.14. ANÁLISIS DE LAS OPORTUNIDADES

4.14.1. Análisis de la Oportunidad

El análisis de las oportunidades tiene como objetivo establecer la posibilidad de materializar las mismas y los beneficios potenciales que puedan tener para la Entidad, al igual que calificarlas y evaluarlas con el fin de obtener la información necesaria para establecer la posibilidad de la oportunidad y las acciones para potencializarla.

La probabilidad, que hace referencia a la posibilidad para la toma de la oportunidad. Para valorar la probabilidad de ocurrencia se utilizan los siguientes criterios, que en esencia son parecidos a los que se manejan para los riesgos:

Tabla 27.

Probabilidad de oportunidades.

NIVEL	CONCEPTO	DESCRIPCIÓN	FRECUENCIA
1	Raro	Excepcional La oportunidad se puede tomar solo en circunstancias excepcionales.	No se estima tomarla en los próximos 5 años
2	Improbable	Improbable La oportunidad se podrá tomar en algún Momento.	Al menos de 1 vez en los próximos 5 años
3	Moderada	Posible La oportunidad se podrá tomar en algún Momento.	Al menos de 1 vez en los próximos 2 años
4	Probable	Es probable La oportunidad probablemente se tomará en la mayoría de las circunstancias.	Al menos de 1 vez en el último año
5	Casi certeza	Es muy seguro Se espera que la oportunidad se pueda tomar en la mayoría de las circunstancias.	Más de 1 vez al año

Nota. Probabilidad de Oportunidades – Elaborado por Grupo DOGI -2024

El impacto tiene que ver con los beneficios que se pueden producir por la toma de la oportunidad en la organización.

Tabla 28.

Impacto de oportunidades.

NIVEL	CONCEPTO	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, generaría beneficios mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría beneficios bajos sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría beneficios medianos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría beneficios potenciales altos sobre la entidad.
5	Favorable	Si el hecho llegara a presentarse, tendría grandes beneficios sobre la entidad.

Nota. Impacto de Oportunidades – Elaborado por Grupo DOGI -2024

4.14.2. Valoración de las oportunidades

La valoración de las oportunidades es el producto de confrontar los resultados de la evaluación de las mimas con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

Figura 11.

Mapa de calor oportunidades.

Probabilidad	Puntaje	Zonas de Riesgo				
Casi seguro	**5**	**Alta 5**	**Alta 10**	**Extrema 15**	**Extrema 20**	**Extrema 25**
Frecuente	**4**	**Media 4**	**Alta 8**	**Alta 12**	**Extrema 16**	**Extrema 20**
Posible	**3**	**Baja 3**	**Media 6**	**Alta 9**	**Extrema 12**	**Extrema 15**
Ocasional	**2**	**Baja 2**	**Baja 4**	**Media 6**	**Alta 8**	**Extrema 10**
Rara vez	**1**	**Baja 1**	**Baja 2**	**Media 3**	**Alta 4**	**Alta 5**

Impacto	Insignificante	Menor	Moderado	Mayor	Favorable
Puntaje	**1**	**2**	**3**	**4**	**5**

Nota. Mapa de calor de oportunidades – Elaborado por Grupo DOGI -2024

A. Identificación de controles o actividades para la gestión de la oportunidad

Para el caso de las oportunidades, los controles deberán ser tomados en el sentido de: actividades cíclicas y repetibles en el tiempo, cuyo objetivo sea aumentar la probabilidad de ocurrencia de las oportunidades o bien aumentar el impacto en el sentido de los beneficios que las mismas puedan traer.

B. Valoración de Controles

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

Describirlos.
Revisarlos para determinar si los controles están documentados en los procedimientos, y si se están aplicando en la actualidad y si han sido efectivos para mejorar las posibilidades de las oportunidades.

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 es posible desplazarse, a fin de aumentar el nivel de oportunidad al que está expuesto el proceso analizado.
Para valorar los controles y determinar lo desplazamientos dentro de la Matriz de Calificación, Evaluación y Respuesta, se puede hacer utilizando las matrices que a continuación se presentan, los cuales permiten de manera objetiva determinar dicho desplazamiento.

Tabla 29.

Evaluación de acciones para las oportunidades.

CRITERIOS PARA LA EVALUACIÓN	EVALUACIÓN	
CRITERIO DE MEDICIÓN	**SI**	**NO**
¿Existen Documentados casos de éxito acerca del control establecido?	20	
¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5	
¿La frecuencia de ejecución del control y seguimiento es adecuada?	20	
¿Se cuenta con evidencias de la ejecución y seguimiento del control?	20	
¿En el tiempo que se lleva trabajando se ha visto mejorada la oportunidad?	30	
TOTAL	**100**	

Nota. Evaluación de acciones de las oportunidades – Elaborado por Grupo DOGI -2024

De acuerdo a los resultados obtenidos de la calificación dada a cada uno de los criterios descritos en la tabla anterior, se tendrá en cuenta los siguientes rangos de calificación:

Tabla 30.

Evaluación de impacto oportunidades.

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA	
	Cuadrantes a aumentar en la Probabilidad	**Cuadrantes a aumentar en el Impacto**
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

Nota. Evaluación de impacto de las oportunidades – Elaborado por Grupo DOGI -2024

Para adelantar esta etapa se hace necesario tener claridad sobre los controles aplicados al proceso.

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

Si el control afecta la probabilidad se avanza hacia arriba. Si afecta el impacto se avanza a la derecha.

Figura 12.

Movimiento de oportunidades según evaluación

Probabilidad	Puntaje	Zonas de Oportunidad				
Casi seguro	**5**	**Alta 5**	**Alta 10**	**Extrema 15**	**Extrema 20**	**Extrema 25**
Frecuente	**4**	**Media 4**	**Alta 8**	**Alta 12**	**Extrema 16**	**Extrema 20**
Posible	**3**	**Baja 3**	**Media 6**	**Alta 9**	**Extrema 12**	**Extrema 15**
Ocasional	**2**	**Baja 2**	**Baja 4**	**Media 6**	**Alta 8**	**Extrema 10**
Rara vez	**1**	**Baja 1**	**Baja 2**	**Media 3**	**Alta 4**	**Alta 5**
Impacto		**Insignificante**	**Menor**	**Moderado**	**Mayor**	**Favorable**
Puntaje		**1**	**2**	**3**	**4**	**5**

Nota. Movimientos de oportunidades según evaluación – Elaborado por Grupo DOGI -2024

C. Tratamiento de la oportunidad.

Esta etapa se hace teniendo en cuenta los resultados obtenidos de la valoración de las oportunidades después de controles.

Una vez implantadas las acciones para el manejo de las oportunidades, la valoración después de controles se denomina oportunidad potencial, éste se define como aquel que permanece después que la dirección desarrolle sus respuestas a los riesgos.

Tabla 31.

Opciones de manejo para oportunidades

ZONA DE OPORTUNIDAD	COLOR	DESCRIPCIÓN
Baja		Potenciar la oportunidad
Moderada		Potenciar la oportunidad, Gestionar la oportunidad
Alta		Gestionar la oportunidad
Extrema		Gestionar la oportunidad

Nota. Opciones de manejo de oportunidades– Elaborado por Grupo DOGI -2024

4.15. MAPA DE RIESGOS INSTITUCIONAL, DE FRAUDE O CORRUPCIÓN Y DE OPORTUNIDADES.

Contiene riesgos y oportunidades de un proceso, al igual que la aplicación de la política institucional en cuanto al tratamiento del riesgo asociado a cada uno.

En el caso de las oportunidades las mismas se encuentran en el formato mencionado, están identificadas por proceso o de manera organizacional según sea el caso y llevan asociadas acciones que potencian su posibilidad de ocurrencia.

4.16. SEGUIMIENTO

Se debe monitorear el Mapa de Riesgos y oportunidades, con el fin de actualizarlo permanentemente, basado en los objetivos, controles existentes, cambios en el proceso o materializaciones.

Teniendo en cuenta la dinámica de la Agencia Logística de las Fuerzas Militares, es necesario que se revisen los mapas de riesgo y oportunidades incluyendo la efectividad de las acciones y controles implementados.

Se define el insumo para realizar el seguimiento a los riesgos y oportunidades identificados, donde se pueden encontrar entre otros:
Indicadores de gestión del proceso.

Herramientas de seguimiento del proceso (aplicativos, cronogramas, informes, reportes, entre otros).

Para el seguimiento a los riesgos se tiene en cuenta dos factores fundamentales los cuales son el AUTOCONTROL y la EVALUACIÓN. Esta última realizada por la tercera línea de defensa según lo establezca la normatividad en materia de riesgos, se realizará evaluación cuatrimestral frente a riesgos de fraude o corrupción y mínimo anual para los institucionales y de seguridad digital.

En cuanto al autocontrol, los responsables o líderes de proceso, de conformidad con la estructura organizacional vigente, son los responsables de mantener actualizados los mapas de riesgos tanto institucionales como de fraude o corrupción, implementar los controles y las acciones preventivas, verificar su efectividad, proponer cambios, velar por su adecuada documentación, por su socialización y aplicación al interior de su proceso.

En cuanto a las oportunidades, cada proceso será responsable de realizar el cargue de las evidencias fruto de las acciones planeadas a la herramienta SVE, la Oficina Asesora de Planeación e Innovación Institucional realizará el seguimiento y correspondientes reportes, esto con el fin de generar evidencia de cumplimiento a la gestión de oportunidades según lo establecido en la norma ISO 9001:2015, ISO 14001:2015, ISO 45001:2018 e ISO 27001:2022.

Para esta actividad cada uno de los procesos cargará la información al plan de mitigación de riesgos y gestión de las oportunidades de manera periódica según lo planificado por el proceso, con el fin de generar los seguimientos correspondientes para la gestión de riesgo y oportunidades en la Entidad.

4.17. MONITOREO A RIESGOS Y OPORTUNIDADES

La herramienta Suite Visión Empresarial presenta varias funcionalidades para la gestión de la entidad. 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 32.

Responsabilidades y periodos de monitoreo

Línea de defensa	Actor	Periodicidad
Primera línea de defensa	Responsable de las tareas del plan de mitigación, indicador, u otro plan asociado a los controles de riesgo.	Cuando fruto de la ejecución del control detecte una desviación que pueda generar materialización de riesgo o el riesgo se evidencia materializado. Este monitoreo deberá informarse a la segunda línea de defensa por cualquiera de los canales disponibles o debe ser cargado a la herramienta SVE en el plan de mitigación, indicador u otro plan asociado a los controles.
Segunda línea de defensa	Oficina Asesora de Planeación e Innovación Institucional	Se realizará dentro de la herramienta SVE en el módulo de riesgos o a través de ejercicios de revisión documentados en los planes, según la complejidad del monitoreo, mínimo una vez al año.
	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.
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 -2024

El monitoreo se debe realizar con el fin de detectar cualquier novedad referente a la dinámica del riesgo. Lo anterior, en el entendido que estas acciones de monitoreo constituyen un mecanismo de reporte por parte los responsables o líderes de proceso y en caso de materialización es indispensable para la activación de los planes o acciones de contingencia a las que haya lugar:

Ingresar a la herramienta SVE Modulo de Gestión de riesgo.
Selecciona la opción “Mis responsabilidades”.
Da clic izquierdo sobre el riesgo del cual eres responsable, En caso de no tener responsabilidad en el monitoreo de algún riesgo de la entidad esta sección aparecerá en blanco, si consideras que debes tenerla contáctate con la Oficina Asesora de Planeación.
Seleccionar la fecha de monitoreo, por defecto aparecerá la fecha actual en la cual se realiza la consulta, se recomienda no modificarla.

Describir de manera exacta y detallada el evento de materialización o necesidad, de ajuste al riesgo. También, es posible asociar un concepto, donde se trae una tarea que se encuentre en otro módulo de la herramienta, esto es útil en los casos donde se presente un acta que sea general para todos los monitoreos evitando la duplicidad de la información.

Seleccione una fecha posterior para el siguiente monitoreo – en caso de materialización, a fecha que seleccione deberá estar dentro de los primeros diez días del mes siguiente a la materialización ya que debe realizarse un seguimiento a las acciones correctivas. También puede seleccionar los días de anticipación con los cuales desea que la herramienta SVE envié un correo recordando esta actividad, asegúrese tener dentro de los destinatarios seguros el correo suitevision@agencialogistica.gov.co.

Dar clic en "programar otro monitoreo", luego de esto el monitoreo quedará guardado, lo cual se podrá validar desde la opción "monitoreos anteriores" que se encuentra en la parte superior de la misma ventana.

4.18. DIVULGACIÓN Y AJUSTES DE UN RIESGO

4.18.1. Divulgación

El Manual de administración del riesgo y el mapa de riesgos y oportunidades se divulgarán a todos los servidores públicos de la Agencia Logística de las Fuerzas Militares a través de los canales de comunicación, herramienta SVE y/o charlas informativas.

4.18.2 Ajustes del Riesgo

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 diligenciar el correspondiente monitoreo explicando las necesidades de ajuste con el fin de actualizar la herramienta SVE.
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.

La guía de mejoras y planes de mejora establece los parámetros esenciales para llevar a cabo este análisis y la documentación de la necesidad de revisión por parte del equipo auditor. En este contexto, se destaca que el objetivo principal es asegurar la eficacia continua del sistema, identificando posibles áreas de mejora y fortalecimiento en los controles existentes, incluso antes de que los riesgos se materialicen.

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.

En resumen, este enfoque proactivo y preventivo, respaldado por las normativas ISO mencionadas, busca asegurar que la organización esté preparada para abordar cualquier desafío potencial, mitigando riesgos y promoviendo la excelencia en la gestión.

4.18.3 Materialización de los riesgos

En caso de reportarse una posible materialización de un riesgo la Oficina Asesora de Planeación e Innovación Institucional procederá a:

A. Si se presenta por primera vez se realizará el correspondiente registro del evento en la herramienta SVE y según análisis de criticidad de la posible materialización se elaborará o diligenciará el correspondiente plan de contingencia o una acción de corrección inmediata, posteriormente se reevaluará el riesgo de acuerdo al evento presentado para determinar si requiere ajuste.

B. Cuando la materialización se detecte en dos reportes de seguimiento de forma consecutiva se informará al líder de proceso con el fin de rediseñar los controles establecidos para el riesgo, los líderes de los procesos serán los responsables de diseñar las actividades para lo cual podrán solicitar el acompañamiento de la Oficina Asesora de Planeación e Innovación Institucional.

C. En caso de encontrarse un plan de mejoramiento vigente por parte del proceso de Seguimiento y Evaluación, o por otro origen, se hará el seguimiento a las actividades planeadas por el proceso responsable del riesgo.

5 CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
0	Versión Inicial
1	Se cambió al nuevo formato
2	Se rediseñó el objetivo general y específico del Manual de Administración del Riesgo
3	Se ajustaron las responsabilidades y roles
4	Se actualizó la normatividad
5	Se incorporaron directrices de Administración de Riesgos de Fraude o corrupción.
6	Se dieron instrucciones particulares frente a la gestión de administración del riesgo por parte de las Direcciones Regionales.
7	Se cambió al nuevo formato, cambios en los formatos anexos, se incluyen los cambios correspondientes al nuevo modelo de operación.
8	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
9	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	