AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

MANUAL DE ADMINISTRACIÓN DE RIESGOS Y OPORTUNIDADES

ELABORÓ	REVISÓ	APROBÓ
FECHA: 25 06 2019	FECHA: 08 07 2019	FECHA: 09 07 2019
NOMBRE: Fabian Ernesto Ponguta Castro	NOMBRE: Miguel Angel Arevalo Luque	NOMBRE: Coronel (RA) Oscar Alberto Jaramillo Carrillo
CARGO: Profesional Defensa	CARGO: Jefe Oficina Asesora de Planeación	CARGO: Director General de la Agencia Logística de las Fuerzas Militares
FIRMA	FIRMA	FIRMA

TABLA DE CONTENIDO

INTRODUCCIÓN

La Administración del Riesgo se introduce en las entidades públicas, teniendo en cuenta que todas las organizaciones independientemente de su naturaleza, tamaño y razón de ser están permanentemente expuestos a diferentes riesgos o eventos que pueden poner en peligro su existencia.

La **Norma Técnica NTC-ISO 31000**, se interpreta que la eficiencia del control está en el manejo de los riesgos, es decir: el propósito principal del control es la prevención o reducción de los mismos propendiendo porque el proceso y sus controles garanticen, de manera razonable que los riesgos están minimizados o se están reduciendo y por lo tanto, que los objetivos de la entidad sean alcanzados.

La administración del riesgo es un proceso liderado por la Alta Dirección de la Agencia Logística de las Fuerzas Militares con la participación y compromiso de todo el personal. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planificación.

Por lo que es concebido como una herramienta de gestión establecida para minimizarlos, monitorearlos o mitigarlos y así evitar la extensión de sus efectos, bajo parámetros de calidad, eficiencia, economía y eficacia. El Mapa de Riesgos que se encuentra consolidado en el presente documento bajo la estructura de un enfoque por procesos, es el producto de un trabajo colectivo de los responsables de Procesos y demás servidores públicos vinculados a la Entidad.

El documento incluye la política Institucional de la administración del riesgo, sus objetivos y el compromiso para su ejecución, así como el marco legal y conceptual sobre el cual se soporta la metodología para su control y cómo debe realizarse el monitoreo al mapa de riesgos; concluye, con la definición de un conjunto de términos, que tiene como finalidad estandarizar el lenguaje de la administración del riesgo en la entidad.

Este documento introduce una metodología similar a la gestión de los riesgos, cuyo objetivo se centrará en la gestión de las oportunidades, con ello se pretende hacer gestión adecuada, generando actividades oportunas, con el fin de poner a disposición de la Entidad los planes necesarios para evidenciar la completa asimilación de la matriz DOFA frente a las actividades de cada proceso.

1. OBJETIVOS

1.1. Objetivo General

Orientar las acciones frente a la política de Administración del Riesgo y Oportunidades de la Agencia Logística de las Fuerzas Militares que conduzcan a disminuir la vulnerabilidad, frente a situaciones que puedan interferir en 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, políticas de administración de riesgos y oportunidades, su trazabilidad, registro y monitoreo.

1.2. 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.
- ✓ Diseñar el formato para estandarizar la información y visualizar globalmente los riesgos y las oportunidades.
- ✓ Construir los Mapas de Riesgo y oportunidades por Proceso de manera coherente y ordenada para proceder a identificar y construir los correspondientes mapas.
- ✓ Involucrar y comprometer a todos los servidores 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.

2. 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.

3. 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.

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.
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).
Directiva Presidencial 09 de 1999	Lineamientos para la implementación de la Política de Lucha contra la Corrupción.
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 4485 de 2009	Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g) "establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder". Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.

Ley 1474 de 2011. Estatuto Anticorrupción	Art. 73. Plan Anticorrupción 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 corrupción y de atención al

	ciudadano; siendo uno de sus componentes el Mapa de Riesgos de Corrupción y las medidas para mitigar estos riesgos. Al Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción, -hoy Secretaría de Transparencia-, le corresponde diseñar la metodología para elaborar el Mapa de Riesgos de Corrupción.
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 Corrupción.
	Art. 2°. Crea la Secretaría de Transparencia en el Departamento Administrativo de la Presidencia de la República.
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 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 corrupción la contenida en el documento "Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano."
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 Anticorrupción y de Atención al Ciudadano.
Decreto 1083 de 2015 Único Función Pública	Art. 2.2.22.1 y siguientes. Establece que el Plan Anticorrupción 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 943 de 2014 MECI	Art. 1 ° y siguiente. Adopta la Actualización del 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.

4. DEFINICIONES

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.
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.
Causa	Son los medios, circunstancias y agentes que generan los riesgos

Cliente	Organización, entidad o persona que recibe un producto y/o servicio.
Confidencialidad	Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
Consecuencia	Es el resultado de un evento (causa) expresado cualitativa o cuantitativamente, que genera pérdida, perjuicio, daño, desventaja o ganancia
Control	Es toda acción que tiende a minimizar los riesgos, significa analizar el desempeño de las operaciones, evidenciando posibles desviaciones frente al resultado esperado para la adopción de medidas preventivas. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.
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	Manifestaciones o características medibles u observables de un proceso que indican la presencia de Riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la Entidad.
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	Consecuencias que puede ocasionar a la Entidad 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.
Mapas de riesgos	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.
Pérdida	Consecuencia negativa que trae consigo un evento.
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	Grado en el cual es probable que ocurra un evento, que se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir.
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	Posibilidad de ocurrencia de toda aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.
Riesgo de Corrupción	El Riesgo de corrupción es la posibilidad de que por acción y omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
Riesgo de Seguridad Digital	Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
Riesgo residual	Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo
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
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).
Zona de riesgo	Es el nivel de exposición al riesgo, hallado mediante el cruce entre la probabilidad y el impacto.

5. 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-, los requisitos de la NTC ISO 9001:2015 y la norma técnica Colombiana ISO 31000.

Para este proceso se tienen los siguientes documentos:

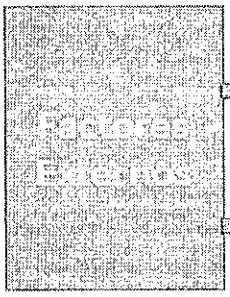
- ✓ Mapa de riesgos de proceso: La entidad debe establecer un mapa de Riesgos y oportunidades que contendrá toda la información del proceso de administración de las mismas: Causas, identificación, análisis, valoración, acciones.
- ✓ Identificación de activos de información por proceso: Cada proceso deberá identificar y clasificar los activos de información que administra según su criticidad y de acuerdo con las directrices emitidas por la Oficina TIC.
- ✓ Mapa de riesgos institucional: 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 Corrupción de los que trata la Ley 1474 de 2011.
- ✓ La información consolidada de este proceso se podrá consultar en la herramienta Suit Vision Empresarial, en la cual se hará la gestión de las acciones propuestas para los riesgos y las oportunidades.

6. CONTEXTO ESTRATÉGICO

Son las condiciones internas y del entorno, que pueden generar originando oportunidades o afectando negativamente el cumplimiento de la misión y los objetivos de una institución[1]. Para determinar los diferentes factores internos y externos se aplica una herramienta de gestión denominada matriz DOFA.

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

1 Modelo Estándar de Control Interno 2014.



Oportunidades
Son aquellos factores que resultan positivos y que favorecen el logro de los resultados

Amenazas
Son aquellas situaciones que impiden el lograr de los resultados

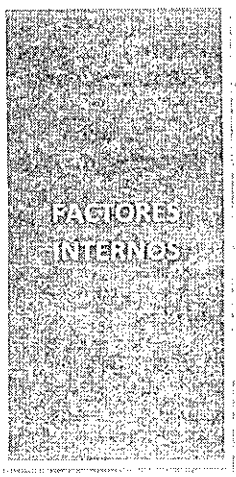
- Cultural
- Económico
- Geográficos
- Legal
- Medioambientales
- Políticos y sociales
- Tecnológicos

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 dl 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.



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 dl 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.

- Atención al cliente.
- Capacidad del Talento Humano.
- Capacidad Directiva.
- Capacidad financiera y Operativa.
- Capacidad Tecnológica.
- Estructura Organizacional.
- Cultura Organizacional.

La tabla a continuación presenta algunos e[illegible]s de riesgo u oportunidades:

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 de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento.
TECNOLÓGICOS: Interrupciones comercio electrónico, datos externos, tecnología emergente.	

Esta etapa se documenta con el formato Matriz DOFA.

7. CLASIFICACIÓN DE LOS RIESGOS Y OPORTUNIDADES

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

Riesgos Estratégicos	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
Riesgos gerenciales	Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
Riesgos Operativos	Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
Riesgos Financieros	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
Riesgos de Cumplimiento	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
Riesgos de Tecnología	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
Riesgos de Imagen	Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.
Riesgos de Corrupción	Posibilidad de que por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado.
Riesgos de seguridad digital	Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía

	nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

- 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 similar a la de los riesgos en cuanto a su contexto, 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

8. RESPONSABLES

Responsabilidad y Compromisos frente al riesgo y oportunidades:

8.1. RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS

8.1.1. 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 a través de una adecuada gestión de riesgos con relación a lo siguiente:

- Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Revisión del 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.
- Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.
- Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas.
- Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos 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.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

- Corresponde a los Comités Institucionales de Coordinación de Control Interno, establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

8.1.2. Primera línea de defensa

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 gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.

Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos instituciones y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.
- Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos 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.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
- Corresponde a los jefes de área y/o grupo (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades

8.1.3. Segunda línea de defensa

Asiste y guía la línea estrategia 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 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 (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)

Los jefes de planeación, supervisores e interventores de contratos o proyectos o responsables de sistemas de gestión 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 corrupción, con relación a lo siguiente:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno 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.

- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

- 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.

- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.

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

- Corresponde al área encargada de la gestión del riesgo (segunda línea de defensa) 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.

8.1.4. Tercera línea de defensa

Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de 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 de corrupción. Está conformada por la Oficina de Control Interno o Auditoría Interna.

La oficina de control interno o auditoría interna monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno 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 que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.

- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer 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 o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.
- Le corresponde a las Unidades de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría, y por tanto debe dar a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos, y los resultados de la evaluación de la gestión del riesgo.

NOTA: Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es del caso ajustarlo, (primera línea de defensa). Le corresponde, igualmente a la oficina de planeación adelantar el monitoreo, (segunda línea de defensa) para este propósito se cuenta con la herramienta SVE. Este monitoreo será mensual según lo programado por la Oficina Asesora de Planeación e Innovación Institucional.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es - por sus propias características una actividad difícil de detectar.

Para el efecto deben atender las actividades descritas en la primera y segunda línea de defensa de este documento.

8.2. RESPONSABILIDADES PARA LAS OPORTUNIDADES

RESPONSABLE	FUNCIÓN
Alta Dirección	Establecer política para riesgos y oportunidades Realizar seguimiento y análisis de las oportunidades
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 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 metodologia para el análisis, calificación y valoración de las oportunidades Consolidar el Mapa de riesgos/oportunidades institucionales y de corrupción de la entidad
Demás 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

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 y 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.

		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

Los riesgos siempre se ocasionan afectando un objetivo Institucional, o un objetivo de proceso, por tal motivo los riesgos son institucionales cuando afectan un objetivo institucional o de proceso, cuando afecta un objetivo de proceso los cuales pueden afectar otros procesos, pero por este motivo no se pueden catalogar como transversales. En ambas ocasiones pueden ser de gestión o de corrupción.

En esta etapa es donde se identifican los riesgos y las oportunidades, lo cual es importante tener en cuenta las siguientes variables, las cuales están incluidas dentro del formato GI-FO-06 MATRIZ DE RIESGOS INSTITUCIONALES, DE CORRUPCIÓN Y OPORTUNIDADES:

- **No Identificación:** Consecutivo que cada proceso debe asignar a cada uno de los riesgos y/u oportunidades que se identifiquen, deberá comenzar con una letra que diferencie entre los dos, en el caso de los riesgos será la letra "R" y para las oportunidades la letra "O", ejemplo: "R-01" – "O-01"

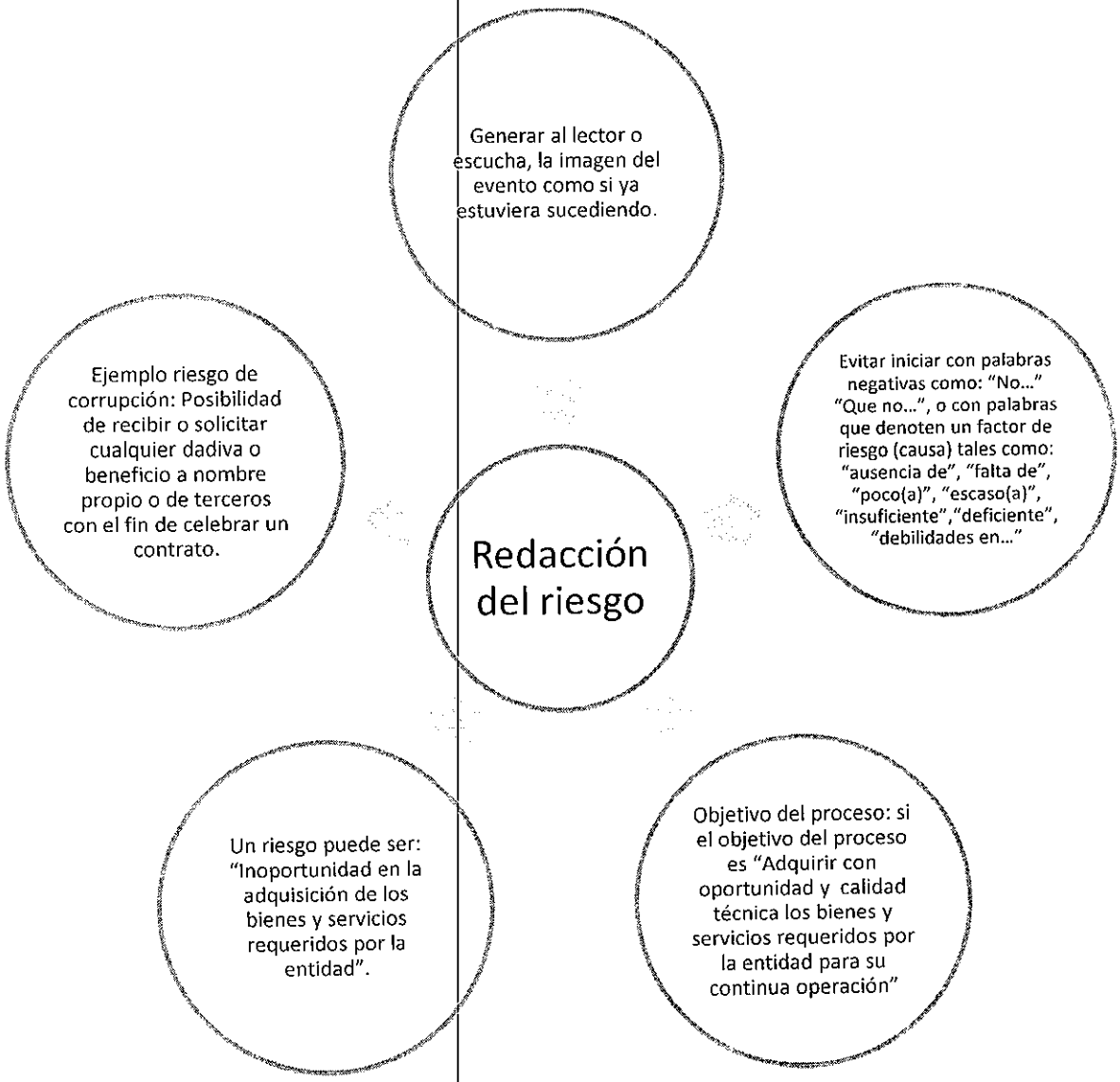
- **Proceso**: Nombre del Proceso.

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

- **Riesgo:** Representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.

  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.

  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 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:



- **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.
- ***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.
- **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 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.

- ***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, de bienes, de imagen, 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.

9.1. Riesgos inherentes de seguridad digital

Para efectos del presente manual y según lo establecido se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- 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 a usar.

10. IDENTIFICACIÓN DE RIESGOS INHERENTES A LA SEGURIDAD DIGITAL

Dentro del contexto de la gestión de riesgos, la guía expedida por el DAFP da una importancia y metodología propia a este tipo de riesgos, en el presente capítulo se dará el paso a paso que se debe seguir para su adecuada gestión.

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.

10.1 Paso 1: Listar los activos por cada proceso

En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Ejemplo:

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

Fuente: Tabla tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

10.2. Paso 2: Identificar el dueño de los activos

Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

Ejemplo:

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO
Base de datos de nómina	Base de datos con información de nómina de la entidad	Director Administrativo y de Talento Humano
Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos	Oficina de TIC's
Cuentas de Cobro	Formatos de cobro diligenciados	Director Financiero

Fuente: Tabla tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

10.3. 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.

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros

Personas	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 especifica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: Tabla tomada textualmente Ministerio de Tecnologías de la Información y las Comunicaciones

Ejemplo:

ACTIVO	TIPO DE ACTIVO
Base de datos de nómina	Información
Aplicativo de Nómina	Software
Cuentas de Cobro	Información

10.4. 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, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

ACTIVO	TIPO DE ACTIVO	Ley 1712 de 2014	Ley 1581 de 2012
Base de datos de nómina	Información	Información Reservada	No Contiene datos personales
Aplicativo de Nómina	Software	N/A	N/A
Cuentas de Cobro	Información	Información Pública	No contiene datos personales

10.5. 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.

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	Información	ALTA	ALTA	ALTA	ALTA

Aplicativo de Nómina	Software	BAJA	MEDIA	BAJA	BAJA
Cuentas de Cobro	Información	BAJA	MEDIA	BAJA	BAJA

10.5.1. CLASIFICACIÓN DE ACUERDO CON LA CONFIDENCIALIDAD

INFORMACION PUBLICA RESERVADA (A)	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 (M)	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 (B)	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.

10.5.2. CLASIFICACIÓN DE ACUERDO CON LA INTEGRIDAD

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

10.5.3. CLASIFICACIÓN DE ACUERDO CON LA DISPONIBILIDAD

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

Una vez se encuentren clasificados los activos de acuerdo con su criticidad, se procederá a realizar el análisis de riesgos a aquellos activos que se encuentren en un nivel alto o medio de criticidad. Este análisis es igual al que se aplica a los riesgos de gestión y de corrupción que se explicará en el capítulo 11 del presente manual. Sin embargo, su monitoreo no se realizará a través de la Suite Visión Empresarial debido a que esta herramienta no incluye la clasificación de los activos. El monitoreo se realizará en la misma hoja de Excel donde se realice la clasificación de los activos que debe diligenciar cada uno de los procesos.

11. ANALISIS 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 parecida, conserva diferencias marcadas.

11.1. 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 servidores de la Agencia Logística de las Fuerzas Militares.

La probabilidad, que hace referencia a la ocurrencia del riesgo. Para valorar la probabilidad de ocurrencia se utilizan los siguientes criterios, los mismos se encuentran en la herramienta SVE:

NIVEL	CONCEPTO	DESCRIPCIÓN	FRECUENCIA
1	Raro	Excepcional El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años

2	Improbable	Improbable El evento puede ocurrir en algún Momento.	Al menos de 1 vez en los últimos 5 años
3	Moderada	Posible El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años
4	Probable	Es probable El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año
5	Casi certeza	Es muy seguro Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año

El impacto, que tiene que ver con las consecuencias que se pueden producir por la materialización del riesgo en la organización.

- Criterios de impacto para riesgos de gestión:

Nivel	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO	• Impacto que afecte la ejecución presupuestal en un valor ≥ 50% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	• Interrupción de las operaciones de la Entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Pérdida de Información critica para la entidad que no se puede recuperar. • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	• Impacto que afecte la ejecución presupuestal en un valor ≥ 20% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor	• Interrupción de las operaciones de la Entidad por más de dos (2) días. • Pérdida de información critica que puede ser recuperada de forma parcial o incompleta. • Sanción por parte del ente de control u otro ente regulador. • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. • Imagen institucional afectada en el orden

	≥20% del presupuesto general de la entidad.	nacional o regional por incumplimientos en la prestación del servicio a los usuarios ciudadanos.
MODERADO	• Impacto que afecte la ejecución presupuestal en un valor ≥ 5% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	• Interrupción de las operaciones de la Entidad por un (1) día. • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. • Reproceso de actividades y aumento de carga operativa. • Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. • Investigaciones penales, fiscales o disciplinarias.
MENOR	• Impacto que afecte la ejecución presupuestal en un valor ≥ 1% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	• Interrupción de las operaciones de la Entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	• Impacto que afecte la ejecución presupuestal en un valor ≥ 0,5% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el	• No hay interrupción de las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa.

	presupuesto total de la entidad en un valor ≥0,5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	

- 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**
INSIGNIFICANTE	1	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	2	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	3	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	4	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	5	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

Tratándose de riesgos de 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.

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

- ✓ Formato para determinar el Impacto en los Riesgos de Corrupción:

N°	Pregunta	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 Fiscalia, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos Penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
Total preguntas afirmativas_____			
Total preguntas negativas_____			
Clasificación del Riesgo:			

Respuestas:

- ✓ Responder afirmativamente de UNO a CINCO pregunta(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**.

Se realiza a través de la Suite Visión Empresarial.

11.2. Calificación del riesgo

Esta se da a través de la estimación de la probabilidad de la ocurrencia, que expresa el número de veces que el riesgo se ha presentado o puede presentarse; y el impacto, que se califica según la magnitud de los efectos, todo lo anterior, por la materialización del riesgo.

- ✓ Calificación de Riesgos de Corrupción Impacto

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

11.3. 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.

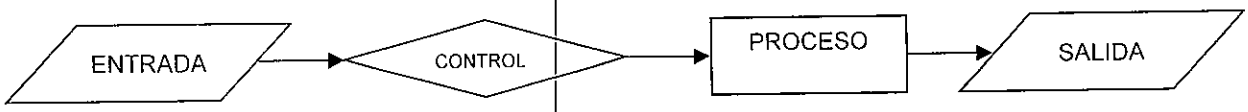
Tabla de valoración riesgos de gestión y corrupción.

Probabilidad	Puntaje	Zonas de Riesgo				
Casi seguro	5			Extrema 15	Extrema 20	Extrema 25
Frecuente	4	Media 4			Extrema 16	Extrema 20
Posible	3	Baja 3	Media 6		Extrema 12	Extrema 15
Ocasional	2	Baja 2	Baja 4	Media 6		Extrema 10
Rara vez	1	Baja 1	Baja 2	Media 3		
Impacto		Insignificante	Menor	Moderado	Mayor	Catastrófico
Puntaje		1	2	3	4	5

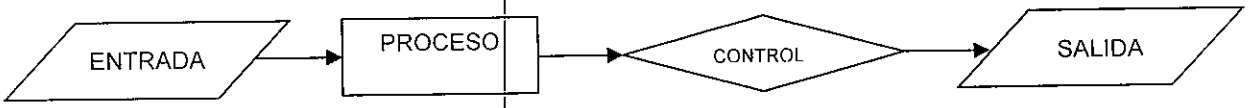
a) Identificación de Controles

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 corrupción.
Es necesario identificar los *puntos de control* existentes para el desarrollo de esta etapa, estos son deductivos, preventivos y correctivos.

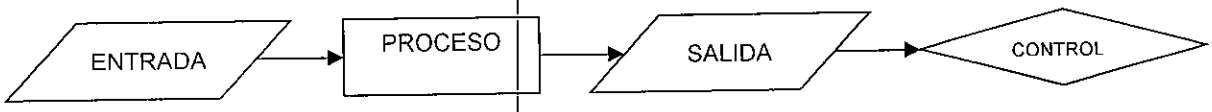
- ***Preventivos:*** Actúan sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos.



- ***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.



- ***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.



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.

Criterio de evaluación.	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control

1.1 Asignación del responsable	Asignado	15
	No Asignado	0
1.2 Segregación y autoridad del responsable.	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control.	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control.	Completa	10
	Incompleta	5
	No existe	0

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:

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

** Esta columna es ajustada a lo expuesto en la guía de administración de riesgos publicada por el DAFP, sin embargo para el caso de la ALFM se implementará la evaluación de controles bajo el supuesto que no es posible cambiar la calificación del impacto de los riesgos, de considerar que el control afecta el impacto, deberá justificarse el por qué.*

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 abajo. Si afecta el impacto se avanza a la izquierda*.

Evaluación del Riesgo de Corrupción = Primera calificación y evaluación del riesgo de corrupción VS controles identificados.

Probabilidad	Puntaje	Zonas de Riesgo				
Casi seguro	5			Extrema 15	Extrema 20	Extrema 25
Frecuente	4	Media 4			Extrema 16	Extrema 20
Posible	3	Baja 3	Media 6		Extrema 12	Extrema 15
Ocasional	2	Baja 2	Baja 4	Media 6		Extrema 10
Rara vez	1	Baja 1	Baja 2	Media 3		
Impacto		Insignificante	Menor	Moderado	Mayor	Catastrófico
Puntaje		1	2	3	4	5

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 de Contingencia

Es una forma de organizarse para actuar frente a un evento posible. El Plan de contingencia establece las medidas a tomar, las tareas a realizar, los recursos que se necesitan y las indicaciones 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, la Suite Visión automáticamente solicitará un plan de contingencia una vez se haya materializado un riesgo.

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.

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.

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.

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.

12. ANALISIS DE LAS OPORTUNIDADES

12.1. 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:

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

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

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.

12.2. VALORACIÓN DE LAS OPORTUNIDADES

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.

Tabla de valoración de 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

a) Identificación de Controles

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, 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.

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	

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:

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

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.

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

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 los riesgos, 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.

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

13. MAPA DE RIESGOS Y OPORTUNIDADES

El mapa de riesgos y oportunidades es la consolidación de la información documentada en cada uno de los formatos de caracterización de los riesgos y las oportunidades, diligenciados.

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

El Mapa de riesgos en la herramienta Suite Visión Empresarial - Modulo de gestión del riesgo tiene vinculado el plan de acciones preventivas y de indicadores que le está dando tratamiento a cada uno de los riesgos, allí se puede consultar el avance de las acciones preventivas propuestas y esta información puede ser consultada por cualquier funcionario de la Agencia Logística de las Fuerzas Militares, de la misma forma, los planes asociados a la gestión de las oportunidades se pueden consultar a través de la herramienta.

En la herramienta Suite Visión Empresarial-Modulo de gestión del riesgo se encuentran:

- ✓ Mapa de riesgos Institucional
- ✓ Mapa de riesgos de corrupción
- ✓ Mapa de riesgos por Procesos

En plan de mitigación de riesgos y 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.

a) Mapa de Riesgos Institucional, de 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.

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 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.

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

14. SEGUIMIENTO

Se debe monitorear el Mapa de Riesgos y oportunidades, con el fin de actualizarlo permanentemente, con base en los objetivos, controles existentes.

Teniendo en cuenta la dinámica de la Agencia Logística de las Fuerzas Militares, es necesario que permanentemente 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 li9nea de defensa según lo establezca la normatividad en materia de riesgos, se realizará el monitoreo cuatrimestral frente a riesgos de corrupción y anual para los de gestión y de seguridad digital.

En cuanto al Autocontrol, los responsables de proceso, de conformidad con la estructura orgánica vigente; son los responsables de mantener actualizados los mapas de riesgos tanto de gestión como de 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 informes, esto con el fin de generar evidencia de cumplimiento a la gestión de oportunidades según lo establecido en la norma ISO 9001:2015.

Para esta actividad cada uno de los procesos a nivel central cargará la información al plan de mitigación de riesgos y gestión de las oportunidades de manera cuatrimestral, con el fin de generar los informes correspondientes para la gestión de riesgo y oportunidades en la Entidad.

15. MONITOREO A RIESGOS Y OPORTUNIDADES

Una vez diseñado y validado el plan para administrar los riesgos, en el mapa de riesgos y oportunidades, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para la organización.
El monitoreo es esencial para asegurar que las acciones de control se están desarrollando y para evaluar su eficiencia, a través de revisiones periódicas que permitan evidenciar situaciones o factores que pueden influir o afectar la ejecución de acciones preventivas.

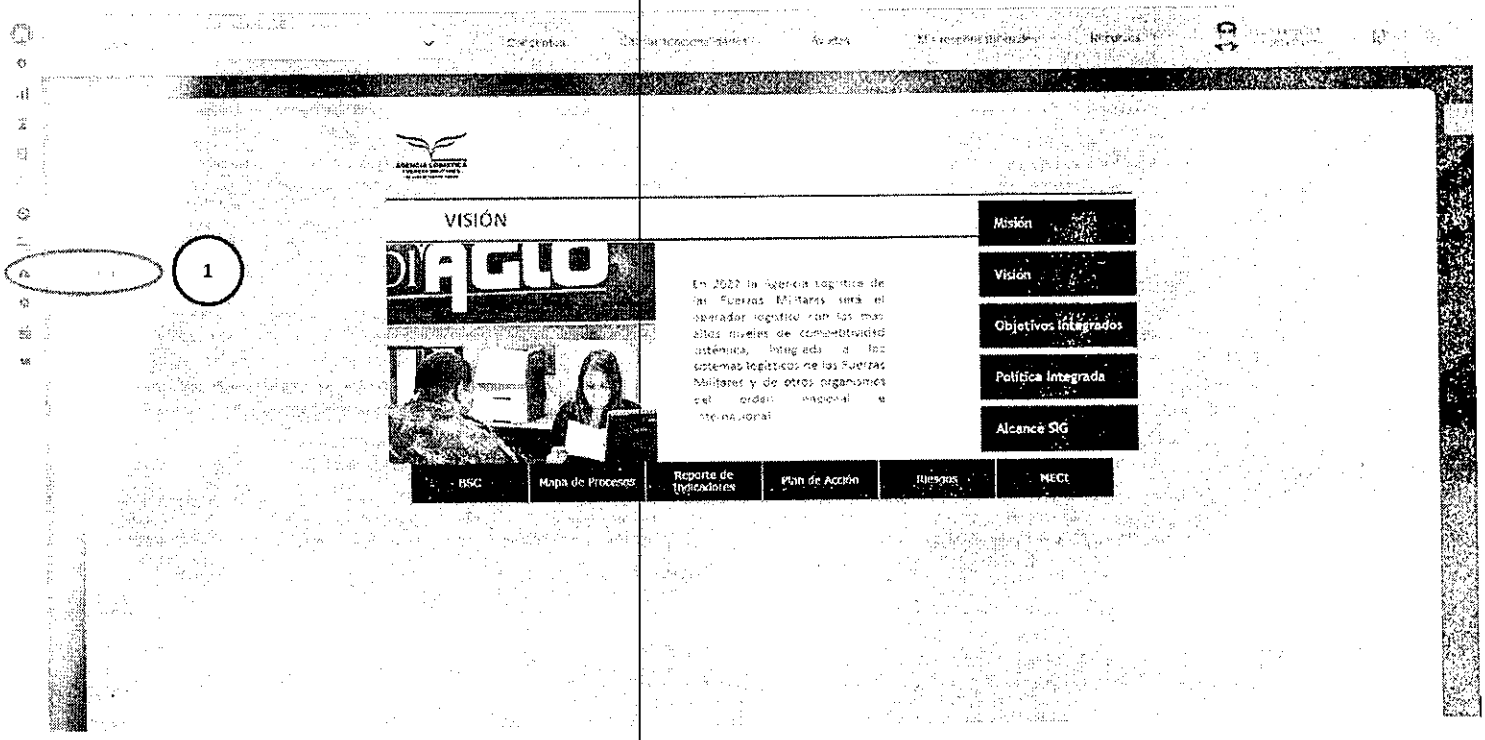
El monitoreo está a cargo de:

- ✓ Los Responsables de los procesos
- ✓ La Oficina de Planeación e Innovación Institucional

Su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo.

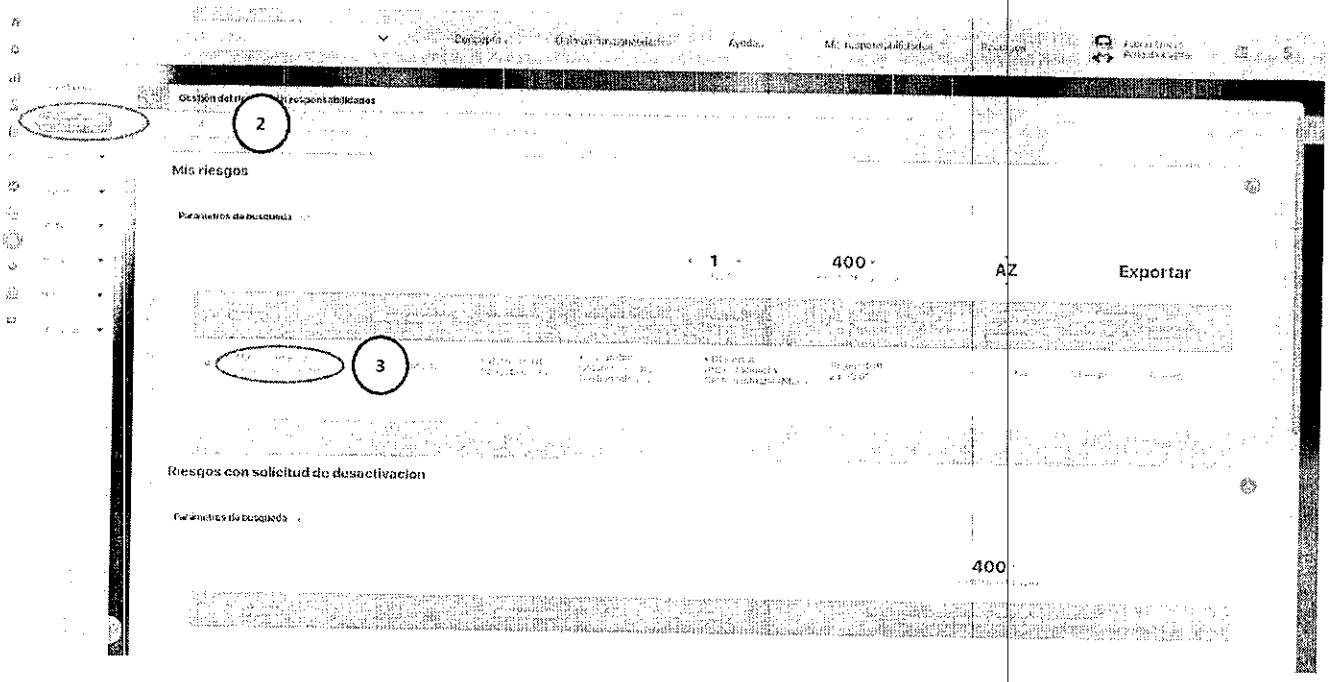
El monitoreo a riesgos se hará de manera mensual por cada uno de los Responsables de Proceso asignados en la matriz de riesgos y oportunidades, este monitoreo se evidencia en la herramienta SVE, a continuación, se encuentra una pequeña guia de la manera como se deberá realizar esta actividad.

1. Ingrese a la herramienta SVE Modulo de Gestión de riesgo.



2. Seleccione "Mis responsabilidades"

3. Dé click izquierdo sobre el riesgo del cual es responsable, en caso de no tener responsabilidad en ningún riesgo de la entidad esta sección aparecerá en blanco, en caso de presentarse problemas comunicarse con la Oficina de Planeación.

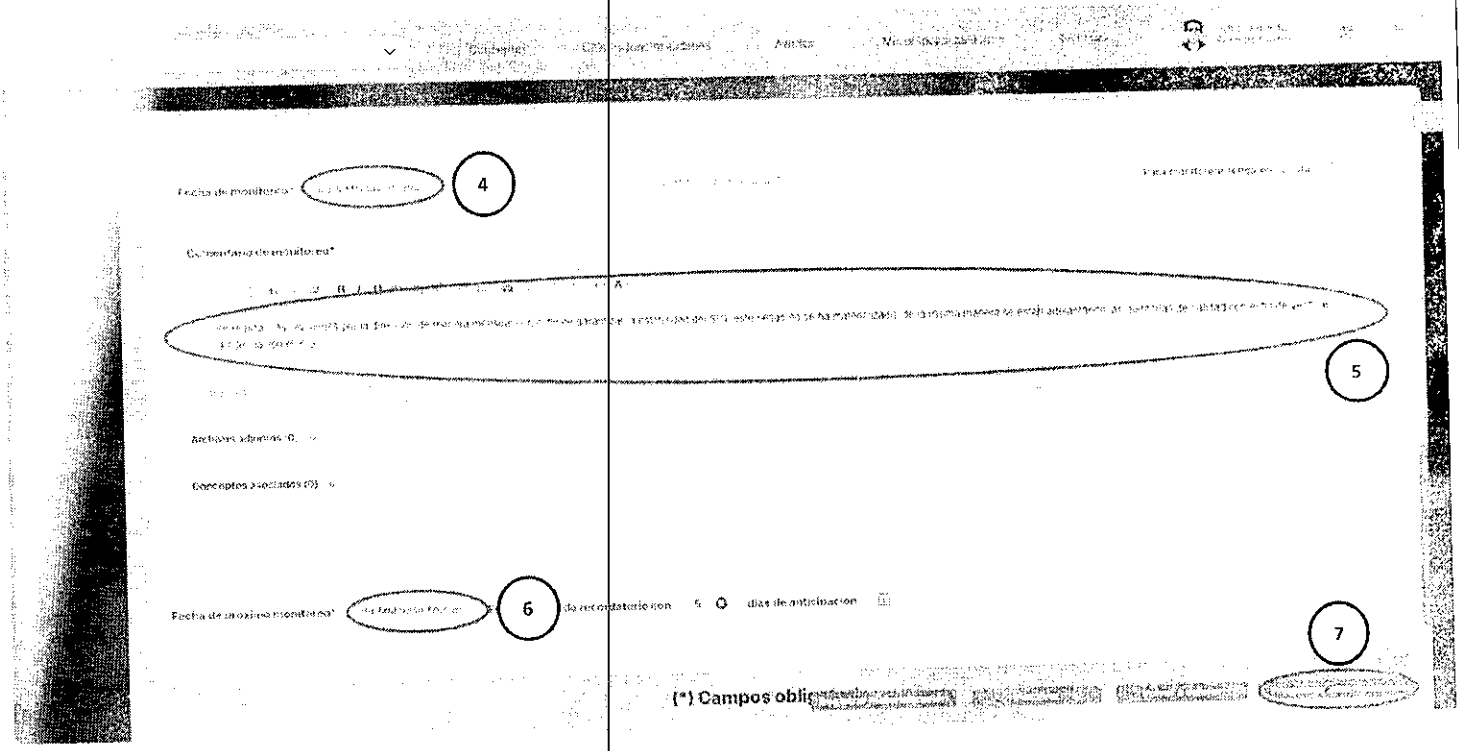


4. Selecciona la fecha de monitoreo, por defecto aparecerá la fecha actual, se recomienda no modificarla.

5. Da una descripción detallada del monitoreo al riesgo seleccionado, que incluya una explicación de las actividades que se han desarrollado durante el mes y como se evidencia que no se ha materializado, en caso de que se haya dado la materialización del riesgo dirígete a la Oficina Asesora de Planeación para recibir orientación acerca de los pasos adicionales.

6. Selecciona una fecha posterior para el siguiente monitoreo, esta fecha será modificada por la Oficina Asesora de Planeación, sin embargo, es requisito del sistema para continuar.

7. Da click en "programar otro monitoreo", luego de esto el monitoreo quedará guardado, lo cual se podrá validar desde la opción "consultar".



13. DIVULGACIÓN Y AJUSTES DE UN RIESGO

a) Divulgación

El Manual de Administración del Riesgo y la Política de Administración de Riesgos y los Mapas de Riesgos y oportunidades se divulgarán a todos los servidores públicos de la Agencia Logística de las Fuerzas Militares a través de los medios de comunicación y/o charlas informativas.

b) Ajustes del Riesgo

Como resultado del autocontrol y la evaluación realizada por la Oficina de Control Interno o revisión de los Responsables de proceso, se pueden generar circunstancias que con llevan ajustar el riesgo. Para esto se debe diligenciar el correspondiente formato de matriz de identificación de riesgos y oportunidades con el fin de ser cargados a la herramienta SVE.

c) Materialización de los riesgos

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

1. Si se presenta por primera vez se realizará el correspondiente registro del evento en la herramienta SVE para posteriormente reevaluar el riesgo en términos de probabilidad.

2. Cuando la materialización se reporte en dos de los cuatrimestres de seguimiento se llamará al proceso responsable para el rediseño de los controles establecidos para el riesgo, de la misma manera se creará un flujo de mejoramiento en la herramienta SVE con plazo no mayor a 1 mes para llevar a cabo estas actividades de análisis, esto con el fin de garantizar la correcta modificación al riesgo materializado, los líderes de los procesos diseñaran la actividades con acompañamiento de la Ofician Asesora de Planeación e Innovación Institucional.

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

14. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
08	Se cambió al nuevo formato Se rediseñó el objetivo general y específico del Manual de Administración del Riesgo. Se ajustaron las responsabilidades y roles. Se actualizó la normatividad. Se incorporaron directrices de Administración de Riesgos de Corrupción. Se dieron instrucciones particulares frente a la gestión de administración del riesgo por parte de las Direcciones Regionales. Se cambió al nuevo formato, cambios en los anexos de los formatos anexos, se incluyen los cambios correspondientes al nuevo modelo de operación. 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. 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.