AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

MINISTERIO DE DEFENSA NACIONAL
AGENCIA LOGÍSTICA DE LAS FUERZAS MILITARES

COPIA No.____ DE____COPIAS
Bogotá D.C.
FECHA 11 AGO 2020

No 06 ALDG – ALOAJD – ALOTIC – ALOAPII – GI – DOGI – 10011

DIRECTIVA PERMANENTE

ASUNTO: Establecer lineamientos y responsabilidades en la administración del Riesgo (Institucionales, de Corrupción y Seguridad Digital) en la Agencia Logística de las Fuerzas Militares.

AL: Señores: Secretario General, Subdirectores Generales, Jefes de Oficina, Directores Nacionales, Directores Regionales, responsables de procesos, Jefes de Oficina, Comité y Subcomités de Coordinación del Sistema de Control Interno (CCSCI) y todos los funcionarios.

1. OBJETIVO Y ALCANCE

a. Finalidad

1) La administración del Riesgo (Institucionales, de Corrupción y Seguridad Digital) de la Agencia Logística de las Fuerzas Militares, tiene como propósito orientar las acciones necesarias que conduzcan a disminuir la vulnerabilidad e impacto frente a situaciones que puedan interferir en el cumplimiento de las funciones y en el logro de los objetivos institucionales.

2) La gestión y administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo, monitoreo y seguimiento a los riesgos que se deben identificar para cada uno de los procesos.

3) Establecer herramienta la Suite Visión Empresarial como mecanismo y sistema de información para la planificación, tratamiento y monitoreo de los riesgos institucionales y de corrupción, así como herramienta para seguimiento de las actividades establecidas en los planes institucionales relacionados con la administración del riesgo.

b. Referencias

1) Ley 87 de 1993, 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.

2) Ley 1474 de 2011, Estatuto Anticorrupción. Artículo 73. "Plan anticorrupción y de Atención al ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias antitrámites y los mecanismos para mejorar la atención al ciudadano.
3) LEY 1712 de 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
4) Decreto 1537 de 2001, Reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno. Artículo 4° la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…).
5) Decreto 943 de 2014, por el cual se actualiza el Modelo Estándar de Control Interno MECI.
6) Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
7) 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."
8) 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.
9) Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
10) Resolución 2497 de 2017 por la cual se crea y reglamenta el Comité y Subcomités de Coordinación del Sistema de Control Interno en la ALFM.
11) Resolución 5563 de 2018, por la cual se formula el Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2018-2022.
12) NTC ISO 9001:2015 Numeral 6 Planificación 6.1. Acciones para abordar riesgos y oportunidades
13) Documento CONPES 3701 de 2011, Lineamientos de Política para Ciberseguridad y Ciberdefensa.
14) Documento CONPES 3854 de 2016, Política Nacional de Seguridad Digital.
15) Directiva permanente Ministerio de Defensa No. 018 de 2014, Políticas de Seguridad de la Información para el sector Defensa.
16) Manual Operativo del MIPG V3 diciembre de 2019: 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
17) Guía para la administración del riesgo y el diseño de controles en entidades públicas de octubre de 2018.

18) Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

c. Vigencia.

A partir de la fecha de expedición. Deroga la Directiva Permanente No. 11 ALDG-ALOAPII-110 del 05 de julio 2019.

2. INFORMACIÓN

La Administración o gestión del riesgo es un proceso efectuado por la Alta Dirección de la Agencia Logística de las Fuerzas Militares y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. 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 planeación. 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.

El riesgo, es la 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. Se expresa en términos de probabilidad y consecuencias.

El riesgo de corrupción es la posibilidad 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.

El riesgo asociado a la seguridad digital es la 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.

3. EJECUCIÓN.

a. Misión General

La administración de riesgos en la Agencia Logística de las Fuerzas Militares, tendrá un carácter prioritario y estratégico, fundamentado en el modelo de operación por procesos, fomentando la cultura del autocontrol al interior de los procesos, la cual debe ser aplicada por todos los responsables de procesos y funcionarios de la ALFM, de acuerdo con los lineamientos y responsabilidades definidas en la presente directiva.

b. Misiones Particulares

Para el tratamiento de los riesgos, se contará con el Manual de Administración del Riesgo y esta directiva en la cual se establecen los siguientes lineamientos:

1) Director General, Secretario General, Subdirectores Generales, Jefes de Oficina, Comité y Subcomités de Coordinación del Sistema de Control Interno (CCSCI):

Pertenecientes a la línea estratégica de la entidad, serán los encargados de:

- Establecer y aprobar la política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico.
- Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo).
- Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad, desempeño de los procesos y que puedan generar cambios en la estructura de riesgos y sus controles.
- Realizar seguimiento y análisis periódico a los riesgos institucionales, de corrupción y de seguridad digital.
- Realimentar al Comité Institucional de Gestión y Desempeño y/o responsables de la administración del riesgo en la entidad sobre los ajustes que se deban hacer frente a la gestión del riesgo.
- Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.

2) Responsables de procesos:

Pertenecientes a la primera línea de defensa de la entidad, serán los encargados de:

- Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera, de manera oportuna, con énfasis en la prevención del daño antijurídico.
- Identificar y clasificar los activos de información que administra en el desempeño de su proceso según su criticidad y de acuerdo con las directrices emitidas por la Oficina TIC.

- Definir, aplicar y hacer seguimiento a los controles definidos para mitigar los riesgos identificados alineados con las metas, objetivos de la entidad y proponer mejoras a la gestión del riesgo en los procesos.

- Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora, a que haya lugar.

- Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.

- Informar a la Oficina Asesora de Planeación e Innovación Institucional (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo, con el fin de determinar las acciones correctivas del caso, de manera oportuna.

- Reportar en el SIG los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.

3) Oficina Asesora de Planeación e Innovación Institucional:

Perteneciente a la segunda línea de defensa, será la encargada de:

- Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.

- Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité Institucional de Gestión y Desempeño y/o alta dirección.

- Presentar al CCSCI el seguimiento a los controles en las áreas identificadas en los diferentes niveles de operación de la entidad.

- Acompañar, asesorar y capacitar a los responsables de procesos en la identificación, gestión, análisis y valoración del riesgo.

- Monitorear a través de la herramienta SVE los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de procesos.

- Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones efectivas y oportunas.

- Evaluar que los riesgos sean consistentes con la presente directiva, dando aplicabilidad a los lineamientos de administración del riesgo y que sean monitoreados por la primera línea de defensa.

- Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del comité institucional de coordinación de control interno.

- Establecer la Suite Visión Empresarial como herramienta para la formulación, seguimiento y tratamiento a través de la parametrización del Módulo de Gestión del Riesgo, para lo cual capacitará y acompañará en el uso de la misma, a los usuarios de acuerdo a los roles establecidos previamente por cada Líder de proceso, Director Regional y /o alta Dirección.

- Realizará las diferentes publicaciones y mantendrá actualizada la información relacionada con la administración y gestión del riesgo, en la página web institucional en cumplimiento de la normatividad aplicable vigente.

- Una vez efectuados los seguimientos a riesgos por proceso, realizará la publicación en la página web institucional del Reporte del Monitoreo de riesgos Institucionales de manera cuatrimestral.

4) Oficina Tecnologías de la Información y las Comunicaciones (TIC)

Pertenecientes a la segunda línea de defensa, será la encargada 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.

- 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.

5) Secretario General, Subdirectores Nacionales, Jefes de Oficina, Directores Nacionales, Coordinadores Nacionales, Directores Regionales, Coordinadores Regionales, Responsables de Procesos:

Pertenecientes a la segunda línea de defensa, serán encargados de:

- Monitorear y hacer seguimiento a los riesgos identificados y controles establecidos para los procesos por la primera línea de defensa acorde con la estructura de los temas a su cargo.

- Reportar a la Oficina Asesora de Planeación e Innovación Institucional a través de la herramienta Suite Visión Empresarial – módulo de riesgos, el seguimiento efectuado al mapa de riesgos y los respectivos controles a su cargo, proponiendo las acciones de mejora a que haya lugar.

- Reportar a la Oficina Asesora de Planeación e Innovación Institucional sobre los cambios y/o ajustes en las responsabilidades del seguimiento y monitoreo de los riegos con el fin de realizar los cambios y/o asignación de roles a los usuarios en la Herramienta Suite visión empresarial de manera oportuna, asegurando el cumplimiento de los lineamientos y plazos establecidos en la presente directiva.

- Acompañar, orientar y entrenar a los funcionarios pertenecientes a sus áreas en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención del daño antijurídico.

- Supervisar que la primera línea de defensa identifique, evalué y gestione los riesgos en los temas de su competencia.

- Los responsables de procesos con el acompañamiento de la Oficina Asesora de Planeación e Innovación Institucional y/o la Oficina de TIC revisarán los controles establecidos para la mitigación de los riesgos y/o vulnerabilidades de los activos de información al menos una vez al año y se ajustarán si es necesario para adaptarlos a los cambios, situaciones o circunstancias por las que pueda atravesar la Agencia Logística de las Fuerzas Militares. Deben dejar evidencias de dichas revisiones y/o actuaciones.

c. Instrucciones Generales de Coordinación

- Se establece alineación del seguimiento a los riesgos institucionales y de corrupción en el plan de mitigación diseñado para cada proceso de la ALFM y por cada vigencia, por lo cual los responsables de procesos reportaran en la herramienta Suite Vision Empresarial el monitoreo de las actividades de mitigación realizadas en forma integral, así como también los Coordinadores Regionales incorporan en la Suite Vision Empresarial los resultados obtenidos en las Direcciones Regionales (si aplica).

- Para los riesgos asociados a posibles actos de corrupción, se debe dar cumplimiento a las fechas establecidas por la Guía de la Secretaría de Transparencia, denominada "*Estrategias para la construcción del plan anticorrupción y de atención al ciudadano*"; en este caso, se aplicará para riesgos institucionales y de corrupción la misma periodicidad de monitoreo en la Suite Vision Empresarial, la cual será cuatrimestral, así:

  - ✓ Primera evaluación: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los cinco (5) primeros días hábiles del mes de mayo.
  - ✓ Segunda evaluación: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los cinco (5) primeros días hábiles del mes de septiembre.
  - ✓ Tercera evaluación: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los cinco (5) primeros días hábiles del mes de enero.

- Todos los procesos de acuerdo a la identificación de riesgos inherentes deben diseñar controles para evitar la materialización del riesgo o establecer acciones preventivas para eliminar la causa del posible riesgo. Las acciones preventivas, deben fundamentarse en la comprensión y origen de las causas que generan el riesgo, así como en el análisis de las interacciones de los procesos, porque de ello depende el grado de control que pueda ejercerse sobre ellas y por consiguiente la efectividad del tratamiento.

- Cuando se establezca la necesidad de ajuste en los mapas de riesgos y/o planes de mitigación, los responsables de proceso deben comunicarlo oportunamente a la Oficina Asesora de Planeación e Innovación Institucional, para efectos de actualización de los mismos en las herramientas destinadas para tal fin; para lo cual deben generar actas de coordinación y/o evidencias que garanticen la comunicación y socialización de los cambios realizados a todos los involucrados.

- Los responsables de los procesos que incurran en incumplimiento de los lineamientos de esta directiva, deberán adelantar acciones correctivas, que permitan eliminar la causa del incumplimiento. De ser reiterativa esta situación, se presentará a consideración del CCSCI, para que tome las decisiones pertinentes.

4. DISPOSICIONES ADMINISTRATIVAS

- Los responsables de proceso deben difundir la presente directiva al personal bajo su mando
- Es responsabilidad de todos los funcionarios de la entidad cumplir los lineamientos establecidos en la presente directiva.

Coronel (RA) OSCAR ALBERTO JARAMILLO CARRILLO
Director General Agencia Logística de las Fuerzas Militares

Elaboró: Fabian E. Ponguta Castro
Cargo: Profesional de Defensa

Revisó: Ing. Ind. Yamile Betancourt Vega
Cargo: Coordinadora Grupo DOGI

Aprobó: Ing. Mec. Rommel Daniel Gutiérrez Gómez
Cargo: Jefe Oficina asesora de Planeación e Innovación Institucional

Aprobó: Martha Eugenia Cortez Baquero
Cargo: Jefe Oficina asesora Jurídica

Aprobó: CT (RA) Sonia Dolly Gutiérrez Carrillo
Cargo: Jefe Oficina TIC

DISTRIBUCIÓN:

ORIGINAL: Dirección General
COPIA No. 1 Secretaría General
COPIA No. 2 Grupo Atención y Orientación Ciudadana
COPIA No. 3 Oficina Asesora de Planeación e Innovación Institucional
COPIA No. 4 Oficina Control Interno
COPIA No. 5 Oficina Control Interno Disciplinario
COPIA No. 6 Oficina Tecnologías de la Información y las Comunicaciones – TIC
COPIA No. 7 Subdirección General de Abastecimientos y Servicios
COPIA No. 8 Dirección Abastecimientos Clase I
COPIA No. 9 Dirección Otros Abastecimientos y Servicios
COPIA No. 10 Dirección Infraestructura
COPIA No. 11 Subdirección General de Contratación
COPIA No. 12 Subdirección General Operación Logística
COPIA No. 13 Dirección Producción
COPIA No. 14 Dirección Administrativa y del Talento Humano
COPIA No. 15 Dirección Financiera
COPIA No. 16 Regional Amazonía
COPIA No. 17 Regional Antioquia – Chocó
COPIA No. 18 Regional Caribe
COPIA No. 19 Regional Centro
COPIA No. 20 Regional Llanos Orientales
COPIA No. 21 Regional Nororiente
COPIA No. 22 Regional Norte
COPIA No. 23 Regional Pacífico
COPIA No. 24 Regional Suroccidente
COPIA No. 25 Regional Sur
COPIA No. 26 Regional Tolima Grande