RESOLUCIÓN D.G. N° 1410/2025

POR LA CUAL SE APRUEBA LA GUÍA PARA LA GESTIÓN DE RIESGOS EN SU VERSIÓN N° 01, EN EL MARCO DE LA IMPLEMENTACIÓN DE LA NORMA DE REQUISITOS MÍNIMOS MECIP: 2015 - PARA UN SISTEMA DE CONTROL INTERNO DEL MINISTERIO DE LA DEFENSA PÚBLICA. ----------

Asunción, 04 de septiembre de 2025

VISTO: El **Memorándum DP N° 99/2025** de la **DIRECCIÓN DE PLANIFICACIÓN** recibido en fecha ***02 de septiembre de 2025*** con ***mesa de entrada N° 2918/25,*** por el cual se solicita la aprobación de la ***"Guía para la Gestión de Riesgos"*** en su **Versión N° 01** en el Ministerio de la Defensa Pública. ----------

Asimismo, la vigencia de la **Resolución D.G. N° 591/2025** de fecha ***15 de abril de 2025*** "Por la cual se asume el compromiso para la implementación del Sistema de Control Interno basado en la Norma de Requisitos Mínimos, en el Ministerio de la Defensa Pública" y la **Resolución D.G. N° 441/2025** de fecha ***31 de marzo de 2025*** "Por el cual se aprueba el Plan y Cronograma del Sistema de Control Interno - NRM, del Ministerio de la Defensa Pública, correspondiente al ejercicio fiscal 2025", y; ----------

C O N S I D E R A N D O:

Que, el Ministerio de la Defensa Pública es una Institución autónoma y autárquica, que brinda asistencia y representación jurídica gratuita a personas en situación de vulnerabilidad, vigilando la efectiva aplicación del debido proceso en el ámbito jurisdiccional. Asimismo, promueve investigaciones vinculadas con el acceso a la justicia y la salvaguarda de los derechos humanos, en el ámbito de su competencia. ----------

El **Memorándum DP N° 99/2025** de la **DIRECCIÓN DE PLANIFICACIÓN** recibido en fecha ***02 de septiembre de 2025*** con ***mesa de entrada N° 2918/25,*** por el cual se solicita la aprobación de la ***"Guía para la Gestión de Riesgos"*** en su **Versión N° 01**, en el marco de la Gestión de la Planificación Institucional y la implementación de la Norma de Requisitos Mínimos (NRM) para un Sistema de Control Interno del Modelo Estándar de Control Interno para Instituciones Públicas del Paraguay – MECIP: 2015 del Ministerio de la Defensa Pública. El mismo, será utilizado como referencia principal para la elaboración e implementación de los distintos mecanismos necesarios para la Administración de Riesgos en todos los procesos de las dependencias de la institución. ----------

En tal sentido, se tiene la necesidad de cumplir con los requerimientos establecidos en la Norma de Requisitos Mínimos, dispuestos por **Resolución CGR N° 377/2016** de fecha ***13 de mayo de 2016,*** se adopta la Norma de Requisitos Mínimos para un Sistema de Control Interno del Modelo Estándar de Control Interno para Instituciones Públicas del Paraguay – MECIP: 2015", así como por **Resolución CGR N° 147/2019** de fecha ***25 de marzo de 2019,*** se aprueba la Matriz de Evaluación por Niveles de Madurez, a ser utilizada en el marco del Sistema de Control Interno del Modelo de Control Interno para Instituciones Públicas del Paraguay – MECIP: 2015. ----------

Abg. ANALIA MIYAZAKI
Secretaria General
Ministerio de la Defensa Pública

Dr. Javier Dejesús Esquivel González
Defensor General
Ministerio de la Defensa Pública

RESOLUCIÓN D.G. Nº 1410 /2025

Asimismo, se encuentran vigentes la **Resolución D.G. Nº 591/2025** de fecha ***15 de abril de 2025*** "Por la cual se asume el compromiso para la implementación del Sistema de Control Interno basado en la Norma de Requisitos Mínimos, en el Ministerio de la Defensa Pública" y la **Resolución D.G. Nº 441/2025** de fecha ***31 de marzo de 2025*** "Por el cual se aprueba el Plan y Cronograma del Sistema de Control Interno - NRM del Ministerio de la Defensa Pública, correspondiente al ejercicio fiscal 2025". ----------

La ***Ley Nº 4423/11 "Orgánica del Ministerio de la Defensa Pública",*** en su ***Título III – Organización, Capítulo II – Del Defensor General, Artículo 14º Atribuciones.*** *Son atribuciones del Defensor General,* en su ***numeral 2)*** establece que puede: *"...Ejercer la Superintendencia de la Defensa Pública, con las potestades administrativas, reglamentarias y de contralor que les son atribuidas por la presente Ley y las demás leyes dictadas sobre la materia y el Reglamento Interno...",* así como el ***numeral 4)*** regula: *"...Dictar instrucciones generales y particulares para la organización de la Defensa Pública que permitan un mejor desenvolvimiento del servicio, a fin de optimizar los resultados de la gestión y la observancia de los principios que rigen el funcionamiento del mismo. Dichas instrucciones serán públicas y no deberán referirse al trámite de causas en particular..."* y el ***numeral 5)*** el cual instituye que el Defensor General puede: ***5)*** *"...Adoptar y poner en ejecución las directrices necesarias para la organización de las diversas dependencias de la Defensa Pública, las condiciones para acceder al servicio, los criterios para la asignación y distribución de los casos y, en general, cuanto sea menester para la prestación del servicio público...".* ----------

Tomando en consideración los documentos agregados, así como la Legislación y Reglamentación, vigentes en la materia, para disponer del presente acto, conforme a las facultades otorgadas por la Ley Orgánica de la Institución y en cumplimiento de los objetivos institucionales, corresponde la aprobación de la ***"Guía para la Gestión de Riesgos"*** en su **Versión Nº 01,** en el marco de la Gestión de la Planificación Institucional y la implementación de la Norma de Requisitos Mínimos (NRM) para un Sistema de Control Interno del Modelo Estándar de Control Interno para Instituciones Públicas del Paraguay – MECIP: 2015 del Ministerio de la Defensa Pública, cuyo Anexo forman parte de la presente resolución. --------

POR TANTO, el Defensor General, en uso de sus atribuciones establecidas en la ***Ley Nº 4.423/11 "Orgánica del Ministerio de la Defensa Pública"*** así como en el ***Reglamento Interno*** de la Institución y en razón de los antecedentes documentales que conforman el legajo. ----------

R E S U E L V E:

Artículo 1º. - APROBAR la ***"Guía para la Gestión de Riesgos"*** en su **Versión Nº 01,** en el marco de la implementación de la Norma de Requisitos Mínimos MECIP: 2015 - para un Sistema de Control Interno del Ministerio de la Defensa Pública, cuyo **ANEXO** forman parte de la presente resolución, en virtud a lo dispuesto en el considerando de la disposición. -----

Abg. ANALIA MIYAZAKI
Secretaria General
Ministerio de la Defensa Pública

Dr. Javier Dejesús Esquivel González
Defensor General
Ministerio de la Defensa Pública

RESOLUCIÓN D.G. Nº 1410/2025

Artículo 2°. - DISPONER que la **DIRECCIÓN DE GESTIÓN DE CALIDAD** y la **DIRECCIÓN DE PLANIFICACIÓN,** sean los encargados de la socialización, instrucción e internalización de la Guía aprobada en la presente resolución, al grupo de los Referentes Técnicos, en el marco de la implementación de la Norma de Requisitos Mínimos, para un Sistema de Control Interno. ----------

Artículo 3°. - ENCOMENDAR a la **DIRECCIÓN DE PLANIFICACIÓN,** la realización de las gestiones internas correspondientes para los casos de modificación y/o actualización de la misma. ----------

Artículo 4°. - DISPONER que la **SECRETARÍA GENERAL** y la **DIRECCIÓN DE COMUNICACIÓN,** coordinen los mecanismos disponibles para la socialización y difusión de lo aprobado en la presente resolución. ----------

Artículo 5°. - COMUNICAR a quienes corresponda y una vez cumplido archivar. ----

ANTE MÍ.-

Abg. ANALIA MIYAZAKI
Secretaria General
Ministerio de la Defensa Pública

Dr. Javier Dejesús Escrivel González
Defensor General
Ministerio de la Defensa Pública

PODER JUDICIAL
DEFENSORIA GENERAL
MINISTERIO DE LA DEFENSA PÚBLICA

MINISTERIO DE LA DEFENSA PÚBLICA

GUIA PARA LA GESTION DE RIESGOS

VERSION 1

DIRECCION DE PLANIFICACION – DIRECCION DE GESTION DE LA CALIDAD

Mag. Raúl A. Bogarín Alfonso
Director
Dirección de Gestión de Calidad

Asunción – Paraguay
2025

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

I. PRESENTACIÓN

En cumplimiento de lo establecido por la Contraloría General de la República, a través de las Normas de Requisitos Mínimos del Sistema de Control Interno, y en concordancia con el Modelo Estándar de Control Interno del Paraguay (MECIP), el Ministerio de la Defensa Pública pone a disposición esta Guía de Administración de Riesgos de Procesos de Gestión.

La presente guía constituye un documento de referencia institucional, diseñado para fortalecer la gestión administrativa y operativa de la Defensa Pública, dotando a las distintas dependencias de un instrumento que facilite la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de riesgos asociados a los procesos estratégicos, misionales, de apoyo y de control.

El propósito principal de este material es promover la cultura de gestión de riesgos, garantizando que cada servidor público incorpore en sus actividades los principios de transparencia, eficiencia, eficacia, legalidad y responsabilidad, en consonancia con la misión constitucional de asegurar la defensa efectiva de los derechos de la ciudadanía.

La guía se presenta como un **marco metodológico y práctico** para:

- Identificar los riesgos que afectan a los procesos institucionales.
- Evaluar la probabilidad e impacto de los riesgos en el cumplimiento de los objetivos.
- Definir medidas de control preventivo y correctivo.
- Fortalecer la rendición de cuentas y el uso eficiente de los recursos públicos.
- Consolidar un sistema de control interno que brinde seguridad razonable en la gestión institucional.

Con esta herramienta, la Defensa Pública reafirma su compromiso de consolidar una **gestión pública moderna, transparente y orientada a resultados**, contribuyendo al fortalecimiento del Estado de Derecho y al acceso equitativo a la justicia.

II. MARCO CONCEPTUAL

A partir de los objetivos de este documento de referencia, es importante resaltar algunos conceptos asociados a la gestión de riesgo:

- **Riesgo**: Son eventos potenciales, inciertos o inesperados que pueden afectar el cumplimiento de un objetivo determinado. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo Estratégico**: Son aquellos riesgos que pueden afectar a la capacidad del MDP para alcanzar sus objetivos y metas generales.
- **Riesgo Operacional**: Es la posibilidad de sufrir pérdidas debido a la falta de adecuación o fallas de los procesos internos, personas, sistemas o eventos externos.
- **Política de Administración de Riesgos**: Determina la posición de la Máxima Autoridad frente al manejo de los Riesgos, en las que se fijan los lineamientos con relación a la Calificación de éstos, la forma de Administrarlos y la Protección de los Recursos, estableciéndose guías de acción para que todos los funcionarios, usuarios internos y externos las apliquen en los distintos procesos definidos para la gestión institucional.
- **Administración del Riesgo**: Es un proceso de gestión y toma de decisiones sobre eventos que podrían suceder, la determinación de sus posibles consecuencias y la definición de acciones para prevenir o reducir el impacto de los mismos, con el objeto de asegurar el logro de los objetivos institucionales. Se determina a través de aplicación sistemática de políticas, procedimientos y

prácticas de gestión a las etapas de identificación, análisis, valoración, tratamiento, monitoreo y comunicación de los riesgos.

- **Mapa o Matriz de Riesgo**: Es la representación de los distintos parámetros vinculados a los riesgos de la institución en los distintos niveles de la gestión, conforme a un criterio de probabilidad, impacto, controles, causas entre otros. Es una herramienta metodológica fundamental para la administración de los riesgos.
- **Amenaza**: Situación externa que no está bajo el control de la institución y que puede afectar negativamente el logro de sus objetivos.
- **Calificación del Riesgo**: Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Causa**: Razones o motivos por los cuales se genera un riesgo.
- **Efecto**: situaciones resultantes de la materialización del riesgo que impactan en el desempeño y en el logro de objetivos institucionales.
- **Contexto de la Organización:** Es la determinación de las cuestiones externas e internas que son pertinentes para la gestión institucional y que pueden afectar el logro de los resultados previstos.
- **Debilidad:** Situación interna que puede afectar el desempeño institucional, su operación y el logro de los resultados esperados.
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos. Es lo mismo que Agentes Generadores de Riesgo.
- **Identificación del Riesgo:** Etapa de la administración del riesgo donde se definen los riesgos con sus causas, agentes generadores asociados a las causas, consecuencias, definición de productos y/o servicios que pueden afectarse con la materialización del riesgo.
- **Impacto:** Son las consecuencias que puede ocasionar a la institución la materialización del riesgo.
- **Materialización del Riesgo:** Ocurrencia del riesgo identificado.
- **Nivel del Riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar sus objetivos.
- **Probabilidad:** Es la posibilidad de ocurrencia del riesgo. Medida para estimar cuantitativa y/o cualitativamente la posibilidad de ocurrencia del riesgo.
- **Tratamiento de Riesgos**: Es el proceso de seleccionar e implementar medidas para gestionar el riesgo. Las medidas de **tratamiento** pueden incluir evitar, modificar, transferir o retener el riesgo.
- **Evitar el Riesgo**: Es una opción de tratamiento, que consiste en tomar la decisión de no verse involucrado, o una acción de retiro de una situación de riesgo.
- **Reducir el Riesgo**: Es una opción de tratamiento que consiste en el fortalecimiento de los controles para prevenir la materialización del riesgo.
- **Transferir el Riesgo**: Es una opción de tratamiento que consiste en cambiar la responsabilidad o compartir con otra parte la carga de la pérdida o el beneficio de la ganancia relacionada a un riesgo.
- **Control de Riesgos**: Parte de la administración de riesgos que involucra la definición de políticas, normas y procedimientos para mitigar los riesgos adversos.
- **Control Preventivo**: Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control Detectivo**: Acción o conjunto de acciones que permiten descubrir un evento, irregularidad o un resultado no previsto; alertando la presencia de los riesgos y permiten tomar medidas inmediatas.

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

Mag. Raúl A. Bogarín Alfonso
Director
Dirección de Gestión de Calidad

- **Control de Protección**: Acción o conjunto de acciones que permiten neutralizar los efectos de los eventos no deseables y el alcance de los daños que pueden producir al materializarse, permitiendo minimizarlos o eliminarlos.
- **Control Correctivo**: Acción o conjunto de acciones que permiten restablecer una actividad después de ser detectado un evento no deseable y contribuyen a modificar las acciones que propiciaron su ocurrencia.
- **Valoración del Riesgo**: Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.
- **Vulnerabilidad**: Representa la debilidad de un control en la gestión institucional que puede facilitar la incorporación de riesgos.

III. OBJETIVO

Disponer de un documento de referencia para la Gestión o Administración de Riesgos en el Ministerio de la Defensa Pública, que permita aplicar adecuadamente en las diferentes etapas de la gestión institucional, mediante distintos mecanismos para identificar, analizar, evaluar y comunicar los riesgos y los mecanismos de control necesarios en los niveles estratégicos y operativos, de manera a contribuir al cumplimiento de los objetivos institucionales.

IV. ALCANCE

Esta Guía Metodológica es aplicable a todas las dependencias del Ministerio de la Defensa Pública, para la Gestión de los riesgos identificados en los distintos procesos de gestión.

V. ETAPAS DE LA GESTIÓN DE RIESGOS

Para el diseño e implementación de la Gestión de Riesgos, todos los mecanismos a ser elaborados e implementados estarán referenciadas a los requisitos establecidos en la Norma de Requisitos Mínimos (NRM) e implementadas a través de una Política de administración de Riesgos y sus distintos mecanismos operacionales, según el siguiente detalle:

1. Los criterios para la identificación y evaluación de los riesgos que deberán tenerse en cuenta según la Norma de Requisitos Mínimos en la gestión del Ministerio de la Defensa Pública, incluidos en la Política de Administración de Riesgos, en los niveles estratégicos y operativos son:

   - El contexto estratégico interno y externo del MDP.
   - La etapa de configuración del plan estratégico y operativo.
   - Los diferentes niveles del modelo de gestión por procesos.
   - Las actividades rutinarias y no rutinarias.
   - Las actividades de todo el personal que tengan relación con los objetivos y la misión institucional (incluyendo aquellas realizadas por contratistas).
   - El comportamiento humano, sus capacidades y otros factores humanos, incluyendo consideraciones sobre la perspectiva de género y la no discriminación.
   - La probabilidad de ocurrencia y el impacto potencial que podría ocasionar su materialización.
   - La infraestructura, tecnología y materiales utilizados, tanto provistos por la institución o por otros.
   - Las modificaciones en la estructura organizacional o en el sistema de gestión, incluyendo cambios temporarios, y sus impactos en los objetivos institucionales, procesos o actividades.

Mag. Raúl A. Bogarín Alfonso
Director
Dirección de Gestión de Calidad

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

- Toda obligación legal relacionada con la evaluación de riesgos y la implementación de los controles necesarios.
- El diseño de procesos, instalaciones, tecnología, procedimientos operativos y la organización del trabajo, incluyendo su adaptación a las capacidades humanas.

2. La comunicación sobre distintos aspectos en el proceso de administración de riesgos se debe dar de manera transversal a toda la organización, para lo cual se deberán implementar canales adecuados de comunicación interna y externa, a fin de que los responsables de la implementación de las políticas de administración de riesgos lo puedan desarrollar a través de Políticas operacionales sobre los Riesgos Críticos identificados en el Mapa de Riesgos de los distintos procesos de gestión.

3. La gestión documental de los distintos instrumentos o formatos relevantes, registros resultantes de los procesos de la identificación, análisis y evaluación de riesgos, deberán ser utilizados como insumos fundamentales para el análisis crítico del Sistema de Control Interno.

4. Se deberán implementar mecanismos de seguimiento de los distintos controles sobre la gestión de riesgos, así como el tratamiento de instrumentos que deben ser ejecutados para accionar sobre los incumplimientos de la aplicación de la presente Guía Metodológica y los instrumentos aprobados, que permitan tomar las medidas correctivas en tiempo y forma.

5. Niveles de la organización para la administración de los riesgos:

Para una buena gestión en la administración del riesgo en el nivel estratégico y operativo se establecen niveles jerárquicos de la organización institucional que intervienen, según responsabilidades definidas, mediante el enfoque de las líneas de acción en materia de riesgos y controles, de tal forma a poder dar respuesta a las vulnerabilidades y materialización de los riesgos en cada etapa de la gestión institucional.

Así se dispone los siguientes niveles jerárquicos y responsabilidades en la Resol. DG. 1567/2024 donde se aprueba la conformación del Grupo de Trabajo para la implementación del Sistema de Control Interno en el MDP.

A. Nivel Estratégico para la Gestión De Riesgos
Responsables: Máxima Autoridad - Implementador - Directivos.

B. Nivel de análisis, seguimiento y ajustes de la Gestión De Riesgos
Responsables: Dirección de Planificación, Dirección de Gestión de Calidad.

C. Nivel operativo, elaboración e implementación de la Gestión de Riesgos
Responsables: Grupo de Referentes Técnicos

D. Nivel de control y evaluación interna de la gestión de riesgos
Responsables: Auditoría General del Rectorado.

Mag. Raúl L. Bogarín Alfonso
Director
Dirección de Gestión de Calidad

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

VI. CONTEXTO ESTRATÉGICO DEL RIESGO

Este elemento de control permite establecer lineamientos estratégicos institucionales, frente a los riesgos que pueden afectar el cumplimiento de los objetivos, resultado de identificar y analizar las circunstancias internas y externas que puedan generar eventos de riesgo. La definición del contexto contribuye a la formulación de controles para evitar o reducir los eventos adversos que puedan impedir o degradar el cumplimento de los objetivos y planes institucionales, o para maximizar los resultados, al identificar y reconocer las situaciones generadoras de riesgos y de oportunidades.

Una vez establecidos los eventos, éstos deben asociarse a los procesos, a través del análisis, valoración y calificación en términos de impacto, de manera a permitir una razonable gestión de los riesgos según los roles y responsabilidades claramente establecidas.

En el análisis del contexto externo es necesario conocer los factores principales que se vinculan a la gestión del MDP, factores tales como: políticos, económicos, sociales, culturales, legales, reglamentarios, ambientales, tecnológicos, financieros y competitivo, a nivel local, nacional, regional e internacional.

En cuanto al análisis del contexto interno, es necesario considerar aspectos vinculados a:

- El liderazgo y compromiso de la Alta Dirección
- El talento humano que compone la institución
- Los objetivos y las estrategias trazados para lograrlos
- Los recursos financieros y tecnológicos con que cuenta
- Los flujos de información y comunicación
- El comportamiento ético, los valores y la cultura organizacional
- Las políticas y la gestión por procesos
- La estructura organizacional
- Los sistemas de gestión

VII. IDENTIFICACIÓN DEL RIESGO

El desarrollo de esta etapa, permite conocer todos los elementos que potencialmente representen algún grado de amenaza. Responde a las siguientes interrogantes: ¿Qué? – ¿Por qué? – ¿Dónde? – ¿Cuándo? y ¿Cómo? podrían ocurrir el suceso que podría impedir, degradar o demorar el logro de los objetivos. Constituye la base para el análisis de los riesgos, tanto en el nivel estratégico como en el nivel operativo de la gestión institucional, de forma a permitir avanzar en las demás etapas de la administración de riesgos.

Incluye cuatro elementos fundamentales:

- **Identificar el Riesgo:** se define en los distintos niveles de la gestión, desde los Objetivos Institucionales, Planes y Programas a través de los Macroprocesos, Procesos, Subprocesos y Actividades.
- **Identificar los Agentes Generadores:** se refiere a las personas u objetos que tienen la capacidad de generar algún tipo de riesgo.
- **Determinar las Causas:** se refiere a las razones o motivos por los que se produce un riesgo.
- **Definir los Efectos:** de la ocurrencia del riesgo.

Mag. Raúl A. Bogarín Alfonso
Director
Dirección de Gestión de Calidad

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

Para la identificación adecuada de los Riesgos en los distintos niveles de los procesos institucionales, se tendrá en cuenta los siguientes criterios, establecidos en la Norma de Requisitos Mínimos:

- El Contexto estratégico interno y externo
- La etapa de configuración de los Planes Estratégicos y Operativos
- Los diferentes niveles del modelo de Gestión por procesos
- La infraestructura, tecnología y materiales utilizados
- Actividades rutinarias y no rutinarias
- Comportamiento humano, sus capacidades y otros factores humanos
- Probabilidad de ocurrencia y el impacto potencial ocasionado.
- Modificaciones de la organización o del sistema de gestión y sus impactos en los objetivos, procesos y actividades.
- Las actividades de todo el personal que tengan relación con los objetivos y la misión institucional.
- Conocimiento de otras Entidades u Organizaciones y dependencias involucradas.
- El propósito y alcance del Proceso.
- Procesos asociados.
- Responsabilidades de los funcionarios involucrados.
- Factores internos y externos.
- Mantenimiento y actualización permanente.
- Toda obligación legal relacionada con la evaluación de riesgos y la implementación de controles.
- Diseño de procesos, instalaciones, tecnología, procedimientos operativos y la organización del trabajo, incluyendo su adaptación a las capacidades humanas.

Además, se podrá considerar como referencia para la identificación del riesgo, el listado de riesgos más comunes, que se anexa en la presente guía.

VIII. ANÁLISIS Y EVALUACIÓN DEL RIESGO

Esta etapa, a partir de la identificación de los distintos riesgos, permite evaluar la probabilidad de ocurrencia y la gravedad del evento, de manera a determinar el impacto o la magnitud de los efectos que puede generar en alguna etapa del proceso.

Comprende un conjunto de acciones vinculadas al análisis necesario, fundamentalmente lo relacionado a la probabilidad de ocurrencia y la gravedad del efecto, que permitirán comparar los niveles estimados de impacto de los riesgos.

En la Evaluación se puede hablar de Valorar el riesgo desde la calificación hasta la priorización según nivel de importancia, de forma a disminuir el nivel de exposición a los impactos del riesgo.

Mag. Raúl A. Bogarín Alfonso
Director
Dirección de Gestión de Calidad

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

La matriz a ser considerada para la evaluación de los riesgos es la siguiente:

Probabilidad de ocurrencia	Valor	5	15	25
Alta	5	**Zona de Riesgo Moderado** ▪ *Prevenir* ▪ *Proteger* ▪ *Compartir*	**Zona de Riesgo Importante** ▪ *Prevenir* ▪ *Proteger* ▪ *Compartir*	**Zona de Riesgo Inaceptable** ▪ *Evitar* ▪ *Prevenir* ▪ *Proteger* ▪ *Compartir*
Media	3	3 **Zona de Riesgo Tolerable** ▪ *Prevenir* ▪ *Proteger*	9 **Zona de Riesgo Moderado** ▪ *Prevenir* ▪ *Proteger* ▪ *Compartir*	15 **Zona de Riesgo Importante** ▪ *Prevenir* ▪ *Proteger* ▪ *Compartir*
Baja	1	1 **Zona de Riesgo aceptable** ▪ *Aceptar*	3 **Zona de Riesgo Tolerable** ▪ *Prevenir* ▪ *Proteger*	5 **Zona de Riesgo Moderado** ▪ *Prevenir* ▪ *Proteger* ▪ *Compartir*
Gravedad		**Baja**	**Media**	**Alta**
Valor		**1**	**3**	**5**

En la **columna Probabilidad** se debe establecer la posibilidad de ocurrencia de los riesgos identificados.

Bajo el **criterio de Probabilidad**, el riesgo se debe medir a partir de los siguientes parámetros:

PROBABILIDAD	DESCRIPCIÓN	VALOR
Alta	Es muy factible	5
Media	Es factible	3
Baja	Es poco factible	1

Bajo el **criterio de Gravedad**, el riesgo se debe medir a partir de los siguientes parámetros:

GRAVEDAD	DESCRIPCIÓN	VALOR
Alta	Alto efecto	5
Media	Medio efecto	3
Baja	Bajo efecto	1

De esta manera, combinando la probabilidad de ocurrencia y la gravedad del evento se podrá definir el nivel de importancia del **impacto probable**.

Estará definido por la siguiente expresión: I = OxG, donde "I" es el impacto probable, "O" es la probabilidad de ocurrencia y "G" la gravedad del evento.

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

Mag. Raúl A. Bogarín Alfonso
Director
Dirección de Gestión de Calidad

TABLA DE PRIORIZACIÓN DEL RIESGO. IMPACTO: VALOR 15 Y 25 SON RIESGOS CRÍTICOS

PRIORIZACIÓN	VALOR
Baja prioridad	Menor a 15
Mediana prioridad	15
Alta prioridad	25

Riesgos Críticos: Todos los riesgos, identificados, analizados y evaluados, cuyos valores definidos determinen la calificación de riesgos importantes o riesgos intolerables, donde los valores del Impacto oscile entre I= 15 e I=25 serán denominados Riesgos Críticos y considerados como prioritarios para su ubicación en el Mapa de Riesgos y su tratamiento correspondiente, tanto en el nivel estratégico como en el operativo.

IX. TRATAMIENTO DEL RIESGO

Se refiere a la manera de actuar, es decir, la definición de las líneas de acción ante los resultados provenientes de los controles y de las evaluaciones de Riesgos Críticos. Es importante resaltar, que en esta etapa arrojarán resultados que son la base para los ajustes de los distintos controles a partir del correspondiente análisis de efectividad de su aplicación.

Fundamentalmente, implica definir y elaborar las Políticas o Directrices de la Administración de Riesgos e implementarlos a través de políticas operacionales vinculadas a los Riesgos Críticos de los distintos procesos.

Si la medición de los niveles de riesgos establecidos es baja y son tolerables, no se requiere modificaciones en el tratamiento.

Para mayores niveles de riesgo, es decir Riesgos Críticos, se deben desarrollar e implementar estrategias y planes de acción específicos para aumentar los beneficios y reducir costos potenciales.

Cuando se determinen las acciones de control, los encargados de la ejecución de los procesos, deben tener en cuenta la reducción de los riesgos con las siguientes jerarquías:

- **Control Preventivo**: se actúa sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia y constituye la primera línea de defensa contra los riesgos.
- **Control Detectivo**: a fin de descubrir tempranamente un evento, irregularidad o un resultado no previsto, generando alertas que permitan tomar medidas inmediatas. Ofrece la segunda barrera de seguridad frente a los riesgos.
- **Control de Protección**: de manera a neutralizar los efectos de los eventos no deseables y minimizar la propagación de los daños que pudieran ocurrir, se toman medidas adicionales que buscan proteger la acción del riesgo.
- **Control Correctivo**: para permitir 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 controles no operan.

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

Para dar mayor claridad de esta jerarquía o clasificación, podríamos visualizar un esquema en una línea de tiempo que muestra las distintas fases del desarrollo del Riesgo y su transformación en un Suceso y así establecer los distintos tipos de controles:

Por tanto, como etapas principales, dentro del marco de la Política de Administración de Riesgos a través de políticas operacionales, se puede resumir en lo siguiente:

Evitar Riesgo: tomar medidas para prevenir su materialización (prevención).

Reducir Riesgo: tomar medidas para disminuir la probabilidad (prevención) y reducir el impacto (protección).

Compartir Riesgo: reduce el efecto a través del traspaso a otras organizaciones (compartir).

Asumir Riesgo: aceptar el efecto y elaborar planes de contingencia para su manejo.

X. CONTROL OPERACIONAL DE LA GESTIÓN DE RIESGO

Monitoreo y control de efectividad: los responsables de la supervisión y control revisarán periódicamente el desempeño del Sistema de Administración de Riesgos, procurando la detección de cambios que pudieran afectar la adecuación o beneficio de los controles.

Los mecanismos de seguimiento a través de los distintos tableros de controles establecidos, deberán determinar mediante los indicadores correspondientes, el nivel de efectividad de los controles sobre los riesgos críticos identificados.

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

El cuadro de análisis de la efectividad de las acciones de mitigación y los controles respectivos, será el siguiente:

CUADRO DE ANÁLISIS DE EFECTIVIDAD

EFECTIVIDAD	CONDICIONES
1. No Efectivo	No se cumplieron ninguno de los indicadores
2. Poco Efectivo	Se cumplieron parcialmente los indicadores previstos
3. Efectivo	Se cumplieron todos los indicadores previstos

XI. CONTROL DE LA MEJORA EN LA GESTIÓN DE RIESGOS

Planes de mejora de la gestión de riesgos: a partir de los tableros de seguimiento y control de riesgos, a través de mecanismos de medición y análisis de indicadores, se determinan los niveles de efectividad de las acciones de mitigación planteadas sobre los probables Riesgos Críticos, donde todos aquellos que no cumplan con los límites de efectividad establecidos para la obtención de los productos institucionales, deberán ser considerados y vinculados a los planes de mejora sectoriales resultantes de la evaluación de los planes operativos anuales.

XII. MAPA DE RIESGOS CRITICOS

La estrategia frente al riesgo podría derivar en acciones que permitan evitarlo, protegerlo, reducirlo, transferirlo o asumir sus consecuencias.

El monitoreo de los Riesgos Críticos es fundamental para asegurar que las acciones ejecutadas y evaluadas puedan determinar la eficacia y eficiencia de su implementación para mantenerlo controlado, es decir podría facilitar acciones que permitan evitar, reducir, transferir o controlar las consecuencias de los riesgos críticos en la gestión institucional.

El diseño del Mapa de Riesgos Críticos, facilita la visualización y entendimiento de los Riesgos que se presentan, tanto a nivel de Objetivos Estratégicos Institucionales como en el nivel operativo (Macroprocesos, Procesos/ Subprocesos, Actividades, procedimientos) facilitando la definición de las medidas de respuesta o tratamiento, de acuerdo con su nivel de importancia para la institución.

En el Mapa de Riesgos, la NRM exige básicamente la inclusión de parámetros tales como:

- Riesgo
- Descripción
- Valoración del riesgo
- Controles existentes
- Causa del riesgo
- Acción de mitigación
- Responsable de la mitigación
- Cronograma de controles
- Indicador del cumplimiento

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

XIII. ANEXO

Tabla referencial de riesgos más comunes

- ACCESO ILEGAL: posibilidad de llegar a algo o a alguien valiéndose de medios que van contra la ley.
- ACCIDENTES: suceso imprevisto, generalmente negativo, que altera la marcha normal de las cosas.
- ACTOS MALINTENCIONADOS: hecho o acción realizada con la intención de llegar a algo o a alguien con mala fe o mala intención.
- ATENTADOS: llevar a cabo una acción que cause daño grave a una persona o cosa.
- AUSENTISMO: no asistir al trabajo u otro lugar de asistencia obligatoria, sin justificación.
- CAMBIOS CLIMÁTICOS: alteración en las condiciones climáticas.
- CELEBRACIÓN INDEBIDA DE CONTRATOS: intervenir en la celebración de un contrato sin cumplir con los requisitos legales.
- COHECHO: aceptar dinero, otra utilidad y/o promesas remuneratorias por parte de un funcionario público a cambio de retardar u omitir un acto que corresponda a su cargo, ejecutar uno contrario a sus deberes oficiales, ejecutar actos en el desempeño de sus funciones, o dar información sobre asuntos sometidos a su conocimiento.
- Las personas que realizan los ofrecimientos anteriormente descritos también incurren en cohecho.
- COLAPSO DE OBRA: derrumbe de un conjunto de elementos debido a la pérdida estructural de los mismos.
- COLAPSO DE TELECOMUNICACIONES: decrecimiento o disminución intensa de la interconexión de sistemas informáticos situados a distancia.
- COLUSIÓN: cuando un funcionario público abusando de su cargo o de sus funciones, induce a que alguien dé o promete para su propio beneficio o el de un tercero, ya sea dinero o cualquier otra utilidad indebida, o los solicite.
- CONFLICTO: situación de desacuerdo u oposición constante entre personas.
- CORRUPCIÓN DE ALIMENTOS, PRODUCTOS MÉDICOS O MATERIALES PROFILÁCTICOS: envenenar, contaminar y/o alterar productos o sustancias alimenticias, médicas o materiales profilácticos, medicamentos o productos farmacéuticos, bebidas alcohólicas o productos de aseo de aplicación personal; así como comercializarlos, distribuirlos o suministrarlos. También hace parte de éste riesgo el suministro, comercialización o distribución de los productos mencionados anteriormente que se encuentren deterioradas, caducados o incumplan las exigencias técnicas relativas a su composición, estabilidad y eficiencia, siempre que se ponga en peligro la vida o salud de las personas.
- CORTOCIRCUITO: circuito eléctrico que se produce accidentalmente por contacto entre los conductores y suele determinar una descarga de alta energía.
- DEMANDA: escrito que se presenta ante un juez para que resuelva sobre un derecho que se reclama contra el deudor u obligado.
- DEMORA: tardanza en el cumplimiento de algo.
- DESACIERTO: equivocación o error en la toma de decisiones.
- DESPILFARRO: gastar mucho dinero u otra cosa innecesaria o imprudentemente.
- DETERIORO: daño. Poner en mal estado o en inferioridad de condiciones algo.
- DISTURBIOS: Perturbaciones del orden público y de la tranquilidad.
- DOLO: toda aserción falsa o disimulación de lo verdadero. Fraude, simulación o engaño.
- ENCUBRIMIENTO: tener conocimiento de la misión encargada a alguien para realizar un acto que merece castigo por la ley, y sin haberlo acordado previamente se ayude a eludir la acción de la autoridad o a entorpecer la investigación correspondiente; además adquirir, poseer, convertir o transferir bienes muebles o inmuebles, que tengan su origen en un delito, o realizar cualquier otro acto para ocultar o encubrir su origen ilícito.

- ENFERMEDADES: alteración más o menos grave en la salud del cuerpo o de la mente.
- EPIDEMIA: enfermedad infecciosa que, durante un cierto tiempo, ataca simultáneamente en un sitio más o menos extendido a un gran número de personas.
- ERROR: idea, opinión o creencia falsa. Acción equivocada, o desobedecer una normas establecida.
- ESTAFA: inducir o mantener a otra persona en un error por medio de engaños.
- ERROR: opinión, concepto o juicio falso que proviene de percepción inadecuada o ignorancia; también se llama error al obrar sin reflexión, sin inteligencia o acierto.
- EVASIÓN: incumplir total o parcialmente con la entrega de las rentas que corresponda legalmente pagar.
- EXCLUSIÓN: negar la posibilidad de cierta cosa. Quitar a una persona o cosa del lugar en el que le correspondería estar o figurar.
- EXTORSIÓN: causar que una persona haga, tolere u omita alguna cosa contra su voluntad, con el propósito de obtener provecho ilícito para sí mismo o para un tercero.
- FALSEDAD: cuando un funcionario público en el desarrollo de sus funciones, al escribir o redactar un documento público que pueda servir de prueba, consigne una falsedad o calle total o parcialmente la verdad. Cuando bajo la gravedad de juramento, ante la autoridad competente, se falte a la verdad o se calle total o parcialmente. Falsificar documento privado, sellos y/o estampillas oficiales, o usarlos fraudulentamente.
- FALSIFICACIÓN DE DOCUMENTOS: imitar, copiar o reproducir un escrito o cualquier cosa que sirva para comprobar algo, haciéndolo pasar por auténtico o verdadero.
- FALLAS DE HARDWARE: defecto que puede presentarse en los Comités de un sistema informático, que impide su correcto funcionamiento.
- FALLAS DE SOFTWARE: defecto que puede presentarse en el conjunto de programas que ha sido diseñado para que la computadora pueda desarrollar su trabajo.
- FLUCTUACIÓN TASA DE CAMBIO: variaciones en el precio relativo de las monedas o del precio de la moneda de un país, expresado en términos de la moneda de otro país.
- FRAUDE: inducir a cometer un error, a un funcionario público para obtener sentencia, resolución o acto administrativo contrario a la ley; así como evitar el cumplimiento de obligaciones impuestas en resoluciones judiciales. También se considera fraude obtener mediante maniobras engañosas que un ciudadano o un extranjero vote por determinado candidato, partido o corriente política. Engaño malicioso con el que se trata de obtener una ventaja en detrimento de alguien – sustracción maliciosa que alguien hace a las normas de la ley o a las de un contrato en perjuicio de otro.
- HUELGAS: interrupción indebida del trabajo que realizan los funcionarios públicos para obtener del gobierno cierta pretensión, o para manifestar una protesta.
- HURTO: apoderarse ilegítimamente de una cosa ajena, sin emplear violencia, con el propósito de obtener provecho para sí mismo o para otro.
- INCENDIO: fuego grande que destruye lo que no está destinado a arder, como un edificio o un bosque.
- INCUMPLIMIENTO: no realizar aquello a que se está obligado.
- INEXACTITUD: presentar datos o estimaciones equivocadas, incompletas o desfiguradas.
- INFLUENCIAS: actuar sobre la manera de ser o de obrar de otra persona o cosa.
- INFRACCIONES: quebrantamiento de una norma o un pacto. Acción con la que se infringe una ley o regla.
- INSTIGACIÓN: incitar pública o directamente a otras personas a cometer un determinado delito.

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública

Mag. Raúl A. Bogarín Alfonso
Director
Dirección de Gestión de Calidad

- INUNDACIÓN: anegación o acción directa de las aguas procedentes de lluvias, deshielo o de cursos naturales de agua en superficie, cuando éstos se desbordan de sus cauces normales y se acumulan en zonas que normalmente no están sumergidas.
- IRREGULARIDADES: actos intencionales por parte de uno o más individuos de la administración, funcionarios.
- LESIÓN DE CONFIANZA: daño o perjuicio causado en los contratos onerosos, especialmente en las compras y ventas por no hacerlas en su valor justo.
- OMISIÓN: falta o delito que consiste en dejar de hacer, decir o consignar algo que debía ser hecho, dicho o consignado. Según el código penal, omisión significa omitir auxiliar a una persona cuya vida o salud se encuentre en grave peligro, o prestar asistencia humanitaria en medio de un conflicto armado a favor de las personas protegidas.
- PARO: suspensión total o parcial de la jornada laboral.
- PECULADO: cuando un funcionario público se apropia, usa o permite el uso indebido, de bienes del Estado o de empresas institucionales administradas, o en que tenga parte el Estado, ya sea para su propio provecho o de un tercero.
- PRESIONES INDEBIDAS: fuerza o coacción que se hace sobre una persona o colectividad para que actúe de cierta manera ilícita o injusta.
- PRESTACION ILEGAL DE SERVICIOS: desempeñar labores destinadas a satisfacer necesidades del público, o hacer favores en beneficio de alguien, de forma contraria a lo que la ley exige.
- PREVARICATO: emitir resoluciones, dictámenes o conceptos contrarios a la ley; u omitir, retardar, negar o rehusarse a realizar actos que le corresponden a las funciones del funcionario público.
- RAYO: chispa eléctrica de gran intensidad producida por descarga entre dos nubes o entre una nube y la tierra.
- RUIDO: sonido confuso y no armonioso más o menos fuerte, producido por vibraciones sonoras desordenadas.
- RUMOR: noticia imprecisa y no confirmada que corre entre la gente.
- SABOTAJE: destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo.
- SOBORNO: entregar o prometer dinero o cualquier otra utilidad a un testigo para que falte a la verdad o guarde silencio total o parcialmente en un testimonio.
- SUPLANTACIÓN: ocupar fraudulentamente el lugar de otro.
- SUSPENSIÓN: interrupción de una acción.
- TERRORISMO: provocar o mantener en zozobra o terror a la población o a un sector de ella, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas, edificaciones o medios de comunicación, transporte, procesamiento o conducción de fluidos o fuerzas motrices, valiéndose de medios capaces de causar estragos.
- TRÁFICO DE INFLUENCIAS: utilizar indebidamente influencias de un funcionario público derivadas de su cargo o su función, para obtener cualquier beneficio para el mismo funcionario.
- VIRUS INFORMÁTICO: el virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de diskettes o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas computarizados.

----------////----------

Ing. Miguel Gómez
Director
Dirección de Planificación
Ministerio de la Defensa Pública