RESERVADO

"SESQUICENTENARIO DE LA EPOPEYA NACIONAL 1864-1870"

FUERZAS ARMADAS DE LA NACIÓN
COMANDO DE LAS FUERZAS MILITARES
Comandancia

114 (catorce).

CORRESPONDE AL EXP. Nº: RESOLUCION N° 573 **HORA:** : **FECHA**

ORIGEN: MDN.

Al / A la:

- ☐ Jefatura CMC FFMM
- ☐ DGP
- ☐ DGI
- ☐ DGO
- ☐ DGL
- ☐ DIGEASCI
- ☐ DOMP
- ☐ DICOMEL
- ☐ DIR SANIDAD
- ☐ DIR PATRIMONIO
- ☐ DPPOI
- ☐ DDHH y DIH
- ☑ **DIGETIC**
- ☐ **Com. Evaluac. Apt. Fís.**
- ☐ **JJ RR MM FFAA**

- ☐ **Auditoria Interna**
- ☐ **Ayudantía General COMANJEFE**
- ☐ **Ayudantía General FFMM**
- ☐ **Ayudantía Personal FFMM**
- ☐ **C.F. N° 1**
- ☐ **TCG FFMM**
- ☐ **CODI**
- ☐ **DAJ**
- ☐ **DGAF**
- ☐ **DICOSO**
- ☐ **Giraduría COMANJEFE/FFMM**
- ☐ **Oficina de Información Pública**
- ☐ **FEDEMIPAR**
- ☐ **RECURRENTE**
- ☐

Para:

- ☐ *Autorizado*
- ☐ *No autorizado*
- ☐ *Dictamen*
- ☐ *Nominar Candidatos*
- ☐ *Notificación mediante Nota*
- ☐ *Redacción de Orden/Nota/Memorándum*
- ☐ *Redacción de PROYECTO de Orden/ Nota*
- ☐ *Su Archivo*
- ☑ *Su Conocimiento*
- ☐ *Fines pertinentes*
- ☐ *Su Cumplimiento*
- ☐ *Su efecto - Coordinar*
- ☐ *Su Estudio e Informe*
- ☐ *Su Informe*
- ☐ *Su trámite*
- ☐ *Preparar Estadística*
- ☐

GRAL DEL AIRE ELADIO CASIMIRO GONZALEZ AGUILAR
Comandante de las Fuerzas Militares

RESERVADO

"SESQUICENTENARIO DE LA EPOPEYA NACIONAL 1864-1870"

FUERZAS ARMADAS DE LA NACIÓN
COMANDO DE LAS FUERZAS MILITARES
Ayudantía General

CORRESPONDE AL EXP. Nº : RESOLUCION Nº 573 | HORA: | FECHA: 3 OCT 2023

ORIGEN: M.D.N.

Al / A la | Para:

- [x] Jefatura EMC FFMM
- [x] COMANDO DE LA ARMADA
- [x] COMANDO DE LA FUERZA AÉREA
- [x] COMANDO DEL EJÉRCITO
- [x] COMANDO LOGÍSTICO
- [x] DIMABEL
- [x] DIGERRMOV
- [x] BCFE
- [ ] Junta de Reconocimiento Médico FFAA
- [ ] Junta de Calificación de Servicios FFAA
- [ ] Comisión de Evaluación de Aptitud Física FFAA
- [ ] Comisión Verificadora de Armamentos y Municiones
- [ ] Ayudantía General COMANJEFE
- [ ] Ayudantía General FFMM
- [ ] Ayudantía Personal FFMM

- [ ] CODI
- [ ] DAJ
- [ ] DGAF
- [ ] DICOSO
- [ ] Giraduría COMANJEFE/FFMM
- [ ] Oficina de Información Pública
- [ ] RECURRENTE

- [ ] *Autorizado*
- [ ] *No autorizado*
- [ ] *Dictamen*
- [ ] *Nominar Candidatos*
- [ ] *Notificación mediante Nota*
- [ ] *Redacción de Orden/Nota/Memorándum*
- [ ] *Redacción de PROYECTO de Orden/ Nota*
- [ ] *Su Archivo*
- [ ] *Su Conocimiento*
- [x] *Su Conocimiento y fines pertinentes*
- [ ] *Su Cumplimiento*
- [ ] *Su efecto - Coordinar*
- [ ] *Su Estudio e Informe*
- [ ] *Su Informe*
- [ ] *Su trámite*
- [ ] *Preparar estadística*

POR ORDEN DEL SEÑOR COMANDANTE DE LAS FUERZAS MILITARES

FUERZAS ARMADAS DE LA NACIÓN · COMANDO DE LAS FUERZAS MILITARES · AYUDANTIA GENERAL

BENICIO RAUL GALVAN GARCIA
Cnel DCEM -Ayudante General Cmdte FFMM

RESERVADO

Ministerio de Defensa Nacional

Resolución N° 573

POR LA CUAL SE APRUEBA LA POLÍTICA DE CIBERDEFENSA, QUE FORMA PARTE COMO ANEXO "A" DE LA PRESENTE RESOLUCIÓN MINISTERIAL.

Asunción, 04 de octubre de 2021.

VISTO: El Estudio e Informe N° 12, del 4 de mayo de 2020, del Comando de las Fuerzas Militares - Dirección General de Tecnologías de la Información y Comunicación, (Expediente N° 1877/2020), y;

CONSIDERANDO: Que en el mismo recomienda la Aprobación de la Política de Ciberdefensa.

Que la Constitución Nacional en su Artículo 30 - De las Señales de Comunicación Electromagnética, establece: "La emisión y la programación de las señales de comunicación electromagnética son del dominio público del Estado, el cual, en ejercicio de la Soberanía Nacional, promoverá el pleno empleo de las mismas según los derechos propios de la República y conforme con los Convenios Internacionales ratificados sobre la materia".

Que la Política de Defensa Nacional 2019 - 2030, hace referencia a los ataques cibernéticos, mencionando que: "Ante la necesidad de prevenir y combatir eficientemente las nuevas amenazas; tales como terrorismo, los secuestros, el crimen organizado transnacional, el narcotráfico, los grupos armados ilegales, los ataques cibernéticos, entre otras, sin descuidar las amenazas tradicionales para la República". Del mismo modo, establece en su apartado VI - Delineamientos Estratégicos para la Defensa en el punto 6"De previsión y protección", referente a considerar y trabajar sobre oportunidades y riesgos inexplorados o escasamente desarrollados, mencionando a la Defensa y explotación del Ciberespacio y espacial.

Que, en el Apartado VII - "Líneas de Acción para la Defensa", el punto 1 menciona como Instituciones con Responsabilidad primaria, al Consejo de Defensa Nacional (CODENA), Ministerio de Defensa Nacional (MDN), Ministerio de Relaciones Exteriores (MRE), y las Fuerzas Militares (FF MM), Ministerio del Interior (MI), Secretaría Nacional de Inteligencia (SNI), igualmente menciona en el referido apartado y punto, inciso b) "El Ministro de Defensa Nacional es el representante de las Fuerzas Armadas en el Nivel Político, es decir, le compete la parte de Defensa de los Intereses Vitales de la Nación y sus Recursos Estratégicos, que involucra a las Fuerzas Militares, sea en forma disuasiva o efectiva.

En tal sentido: Promulga la Política Militar y en coordinación con las Fuerzas Militares, promueve y fortalece la Ciberdefensa".

Ministerio de Defensa Nacional

Resolución N° 573

POR LA CUAL SE APRUEBA LA POLÍTICA DE CIBERDEFENSA, QUE FORMA PARTE COMO ANEXO "A" DE LA PRESENTE RESOLUCIÓN MINISTERIAL.

Que, el inciso d), de la normativa mencionada anteriormente, dispone: "Las Fuerzas Militares planifica, propone y ejecuta la política militar en coordinación con el Ministerio de Defensa Nacional, organiza, prepara y actualiza la doctrina, el personal y equipo, teniendo en cuenta las amenazas tradicionales y las amenazas emergentes".

Que la Dirección General de Asuntos Jurídicos del Ministerio de Defensa Nacional, con los términos del Dictamen N° 468, del 6 de setiembre de 2021, recomienda la Aprobación de la Política de Ciberdefensa, conforme al Anexo "A".

POR TANTO, en ejercicio de sus atribuciones Legales,

EL MINISTRO DE DEFENSA NACIONAL

RESUELVE:

1°.- Aprobar la Política de Ciberdefensa, que forma parte como Anexo "A" de la presente Resolución Ministerial.

2°.- Establecese la Difusión y Ejecución de la Política de Ciberdefensa.

3°. - Registrar, comunicar y archivar.

ES COPIA:

(FDO): BERNARDINO SOTO ESTIGARRIBIA

GRAL DIV (R) ROGELIO CANO MENDOZA

SECRETARIO GENERAL

Ministerio de Defensa Nacional

Anexo "A" de la Resolución N° 573

ÍNDICE

Capítulo I - Introducción

1.1. Finalidad
1.2. Aplicación
1.3. Planteamientos Básicos

Capítulo II - Objetivos
2.1. Son Objetivos de la Política de Ciberdefensa.

Capítulo III - Directrices

3.1. Directrices aplicables a los Objetivos presentados

3.1.1. Garantizar el uso efectivo del ciberespacio por la Ciberdefensa, para predecir, prevenir u obstaculizar las amenazas y/o riesgos emergentes que puedan surgir desde a través del mismo y que afecten los intereses nacionales, la soberanía nacional y su proyección a la soberanía digital:

3.1.2. Proyectar y capacitar los recursos humanos necesarios con las capacidades Cibernéticas, de manera a contar con las competencias necesarias para llevar a cabo las actividades a ser desarrollados en el Ciberespacio, a través de las FFMM y el Ministerio de Defensa Nacional:

3.1.3 Cooperar en la producción de inteligencia de fuente Cibernética que sea de interés para la Ciberdefensa, con énfasis en las instituciones y/o unidades responsables de la Defensa Nacional:

3.1.4 Desarrollar y mantener actualizada la doctrina de empleo de la Ciberdefensa:

3.1.5 Adaptar las estructuras de la Ciencia, Tecnología e Innovación de las Fuerzas Singulares y Direcciones Generales, para implementar las actividades de investigación y desarrollo, a fin de satisfacer las necesidades de la Ciberdefensa:

3.1.6 Definir los principios básicos que guían la creación de legislación y normas específicas para el empleo de la Ciberdefensa:

3.1.7 Contribuir con la seguridad de las infraestructuras críticas y de los activos críticos de las instituciones (públicas y privadas), que estén fuera del alcance del Ministerio de Defensa Nacional:

3.1.8 Establecer las estrategias y las estructuras adecuadas que permitan dirigir, coordinar y supervisar las infraestructuras críticas a cargo de las FFAA de la Nación:

MINISTERIO DE DEFENSA NACIONAL SECRETARÍA GENERAL

3.1.9 Cooperar con el esfuerzo de la Movilización Nacional:

3.1.10 Cooperar con otros órganos o estamentos de Ciberdefensa:

Capítulo IV - Responsabilidades, Actualización y Proyección

4.1. Responsabilidades

4.2. Actualización

4.3. Proyección

a) A corto Plazo - Año 2020 / 22

b) A mediano Plazo - Año 2023/25

c) A largo Plazo – Año 2026/30

Capítulo I

Finalidad, Aplicación, Planteamientos Básicos.

1.1. Finalidad

La Política de Ciberdefensa tiene como finalidad orientar las acciones del Ministerio de Defensa Nacional (MDN), en el ámbito de la Defensa Nacional, en el nivel estratégico, operacional y táctico, para lograr los objetivos trazados en el ciberespacio.

1.2. Aplicación

La Politica de Ciberdefensa se aplica en el ámbito de Expresión Militar proyectado al Poder y Potencial Nacional; así como a las instituciones y/o entidades que cooperan para las actividades de Defensa y el Desarrollo Nacional y/o Ciberdefensa.

1.3. Planteamientos Básicos

La definición y determinación de los lineamientos de una Politica de Ciberdefensa están orientadas a los siguientes planteamientos básicos:

a. La Ciberdefensa está a cargo del Ministerio de Defensa Nacional y están encaminadas a satisfacer las necesidades de Defensa Nacional y su proyección al mantenimiento de la soberanía digital.

b. Las acciones cibernéticas defensivas, exploratorias y defensa activa se ejecutarán de acuerdo con las hipótesis de empleo (HE) en el ciberespacio.

c. El fortalecimiento de la Ciberdefensa depende primordialmente de la acción colaborativa de los actores responsables de la preservación y mantenimiento de las infraestructuras críticas, enmarcadas no solo en el ámbito del Ministerio de Defensa Nacional, sino también su proyección a las expresiones del Poder Nacional.

3) Cooperar en la producción de inteligencia de fuente Cibernética que sean de interés para la Ciberdefensa, con énfasis en las instituciones y/o unidades responsables de la Defensa Nacional.

4) Desarrollar y mantener actualizada la Doctrina de empleo de la Ciberdefensa.

5) Adaptar las estructuras de Ciencias, Tecnologías e Innovaciones de las Fuerzas Singulares y Direcciones Generales, para implementar las actividades de investigación y desarrollo, a fin de satisfacer las necesidades de la Ciberdefensa.

6) Definir los principios básicos que guían la creación de leyes y normas específicas para el empleo de la Ciberdefensa.

7) Contribuir a la seguridad de las infraestructuras críticas y de los activos críticos de las instituciones (públicas y privadas), que estén fuera del alcance del Ministerio de Defensa Nacional.

8) Establecer las estrategias y las estructuras adecuadas que permitan dirigir, coordinar y supervisar las infraestructuras críticas, a cargo de las FFAA de la Nación.

9) Cooperar con la Movilización Nacional para acciones de Ciberdefensa.

10) Cooperar con otros órganos o entes de Ciberdefensa.

Capítulo III
Directrices

Las directrices sugieren las actividades a ser definidas e implementadas por el Ministerio de Defensa Nacional, a fin de alcanzar los objetivos trazados en la Política de Ciberdefensa.

3.1. Directrices aplicables a los Objetivos presentados

3.1.1 Garantizar el uso efectivo del ciberespacio por la Ciberdefensa, para predecir, prevenir u obstaculizar las amenazas y/o riesgos emergentes que puedan surgir desde a través del mismo y que afecten los intereses nacionales, la soberanía nacional y su proyección a la soberanía digital:

a. Diseñar e implementar un Consejo de Ciberdefensa, con la participación de representantes de las expresiones del Poder Nacional.

b. Crear un Comando Conjunto de Ciberdefensa (CCCD) para llevar a cabo la coordinación e integración de la Ciberdefensa entre el Ministerio de Defensa Nacional y las Fuerzas Militares.

c. Establecer los criterios de riesgo de los activos críticos de información, mitigando los riesgos para las infraestructuras críticas, de interés para la Defensa Nacional y su proyección a la soberanía digital.

d. Crear y estandarizar procesos de seguridad de la información de las infraestructuras críticas y de interés para la Defensa Nacional y la soberanía digital.

e. Establecer programas y/o proyectos para garantizar la capacidad de conectividad de las redes. de manera a fortalecer la operatividad de la actividad de Comando y Control (C2), Guerra Electrónica, Comunicaciones, Inteligencia, Equipos de Respuestas a Incidentes Cibernéticos (preventivos, detectivos y correctivos) como parte de un Comando Conjunto de Ciberdefensa, a través de las FFMM y el Ministerio de Defensa Nacional;

f. Coordinar con las infraestructuras críticas de información asociadas a la Ciberseguridad, para contribuir con la Ciberdefensa en apoyo a la Defensa y el Desarrollo Nacional.

3.1.2 **Proyectar y capacitar los recursos humanos necesarios con las capacidades Cibernéticas, de manera a contar con las competencias necesarias para llevar a cabo las actividades a ser desarrolladas en el Ciberespacio, a través de las FFMM y el Ministerio de Defensa Nacional:**

a. Definir los perfiles de personal, necesarios para llevar a cabo las actividades de la Ciberdefensa.

b. Crear los cargos y funciones específicas, enrolarlos y movilizarlos como personal especializado y que formen parte de la Ciberdefensa.

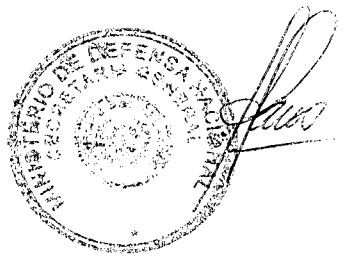
c. Establecer criterios y controlar la movilización y desmovilización de la reserva activa de Ciberdefensa.

d. Identificar, registrar y seleccionar personal con habilidades o destrezas, existentes en los entornos internos y externos de las FFAA, para integrar un Comando Conjunto de Ciberdefensa.

e. Capacitar continuamente al personal para trabajar en Ciberdefensa, a cargo de un Comando Conjunto de Ciberdefensa, aprovechando las estructuras existentes.

f. Proyectar la participación del personal involucrado en la Ciberdefensa realizando cursos, pasantías, congresos, seminarios, simposios, ejercicios de simulación conjunto y otras actividades relacionadas en nuestro país y en el extranjero.

g. Realizar eventos periódicos que permitan la presentación y discusión de temas relevantes en áreas de interés para el sector Cibernético, a ser organizado y dirigido por el Comando Conjunto de Ciberdefensa, para unificar criterios, nivelar y actualizar el conocimiento.



h. Crear instrumentos para permitir y motivar la permanencia del personal especializado en las actividades de la Ciberdefensa, permitiendo la continuidad de la actividad.

i. Establecer vínculos e intercambios entre las FF AA e instituciones estratégicas.

j. Incluir el contenido de Ciberdefensa al Plan de estudios de los cursos en todos los niveles de las instituciones educativas de las FFAA.

k. Desarrollar y mantener actualizado un banco de activos de información de interés para la movilización de la Ciberdefensa.

l. Preparar planes y programas de movilización de activos de información, con sus costos, de conformidad con la Ley Nacional de Movilización.

m. Ajustar las necesidades de movilización de la Ciberdefensa al Sistema Nacional de Movilización de Ciberdefensa.

n. Proponer al gobierno nacional la realización de una campaña nacional de educación en Ciberdefensa, dirigida a la Movilización Nacional, para aumentar el nivel de sensibilización y concientización.

3.1.3 **Cooperar en la producción de inteligencia de fuente Cibernética que sea de interés para la Ciberdefensa, con énfasis en las instituciones y/o unidades responsables de la Defensa Nacional:**

a. Adaptar la doctrina e insertar la fuente Cibernética para la integración a otras fuentes de datos, destinadas a la producción de conocimiento.

b. Crear estructuras de Ciberinteligencia, según lo necesiten las instituciones y/o unidades de inteligencia de las FFAA, para aplicar métodos científicos y sistemáticos, buscando extraer y analizar datos de la fuente Cibernética, produciendo conocimiento de interés para la Ciberdefensa.

c. Establecer un canal sistémico y técnico entre los órganos de Ciberdefensa y de inteligencia de las FFAA.

d. Contribuir a la formación de la conciencia situacional necesaria para las actividades de inteligencia en apoyo a la Defensa y el Desarrollo Nacional.

3.1.4 **Desarrollar y mantener actualizada la doctrina de empleo de la Ciberdefensa:**

a. Crear la doctrina de Ciberdefensa.

b. Fomentar el desarrollo e intercambio de tesis, disertaciones y otros trabajos similares, con enfoque doctrinario, en instituciones de educación superior civil y militar de interés para las actividades de la Ciberdefensa.

c. Promover intercambios doctrinarios, normativos y técnicos con instituciones civiles y militares, nacionales y de países amigos.

d. Insertar la Ciberdefensa en ejercicios de simulación de combate y Operaciones Conjuntas.

e. Crear un sistema de gestión del conocimiento de las lecciones aprendidas para la composición y actualización de la doctrina de Ciberdefensa.

f. Designar conforme a creación al Comando Conjunto de Ciberdefensa, como responsable de proponer innovaciones y actualizaciones de doctrina de la Ciberdefensa en el campo de la Defensa Nacional.

3.1.5 **Adaptar las estructuras de la Ciencia, Tecnología e Innovación de las Fuerzas Singulares y Direcciones Generales, para implementar las actividades de investigación y desarrollo, a fin de satisfacer las necesidades de la Ciberdefensa:**

a. Planificar y ejecutar la adecuación de las estructuras de Ciencia, Tecnología e Innovación (C, T & I), integrando esfuerzos entre las instituciones para satisfacer las necesidades de la Ciberdefensa.

b. Crear un Comité permanente compuesto por representantes del Ministerio de Defensa Nacional e invitados, otros ministerios y agencias de financiamiento para intensificar y explorar nuevas oportunidades de cooperación en C, T & I en las áreas de interés del Sistema de Ciberdefensa.

c. Proyectar las necesidades de Ciberdefensa en el área de C, T & I, para identificar las capacidades científicas - tecnológicas necesarias para el desarrollo del Sector de la Ciberdefensa.

d. Identificar habilidades específicas (individuales y organizativas) en C, T & I, de interés para la Ciberdefensa, en el marco del MDN y los centros de innovación y desarrollo (I+D) civiles (públicos y privados), estableciendo asociaciones entre centros a nivel nacional; para agregar instituciones y evitar la dispersión de recursos.

e. Crear asociaciones y cooperación entre los centros de investigación y desarrollo militar y los centros de investigación y desarrollo civil (públicos y privados) para alentar la integración de iniciativas de interés para el Sistema de Ciberdefensa;

f. Crear programas a cargo del MDN, en asociación con el MITIC que aborden la doble característica (empleo civil y militar) de las tecnologías de información y comunicación (TIC) empleadas en el área cibernética, para fortalecer la participación del sector industrial en las fases de Proyectos de interés de la Ciberdefensa.

Capítulo IV
Responsabilidades, Actualización y Proyección

4.1. Responsabilidades

El Comandante de las Fuerzas Militares (FFMM) a través de un Comando Conjunto de Ciberdefensa (CCCD) a ser creado a futuro, será el responsable de asesorar al Ministro de Defensa Nacional sobre la implementación y gestión de la Ciberdefensa, a fin de garantizar en el marco de la Defensa Nacional las capacidades de redes, la interoperabilidad de los sistemas, de manera a lograr los niveles de seguridad y resiliencia adecuada en el ciberespacio.

4.2. Actualización

Esta Política será revisada y actualizada periódicamente por el Ministerio de Defensa Nacional, por iniciativa propia o a propuesta de las Fuerzas Armadas de la Nación.

4.3. Proyección

a) **A corto Plazo - Año 2020 / 22**

- ✓ Política de Ciberdefensa – 2020
- ✓ Doctrina de Ciberdefensa – 2021
- ✓ Establecer comisión para proyectar la creación de CCCD (Comando Conjunto de Ciberdefensa) – 2021
- ✓ Presentación de Proyecto de Creación del CCCD – 2021/22

b) **A mediano Plazo - Año 2023/25**

- ✓ Creación del CCCD - 2023
- ✓ Puesta en Operación del CCCD – 2024/25

c) **A largo Plazo – Año 2026/30**

- ✓ Optimizar estructura - 2026
- ✓ Optimizar tecnología – 2026/27
- ✓ Formación Cibersoldados – 2028/30