MINISTERIO DE DEFENSA

Resolución 1380/2019

RESOL-2019-1380-APN-MD

Ciudad de Buenos Aires, 25/10/2019

VISTO el Expediente EX -2019-82984942-APN-SSC#MD, la Ley N° 23.554, la Ley N° 24.948, el Decreto N° 9390 del 11 de octubre de 1963, los Decretos Nº 727 del 12 de junio de 2006, 1729 del 27 de noviembre de 2007, 577 del 28 de julio del 2017, y su modificatorio 480 del 11 de julio de 2019, 703 del 30 de julio de 2018, 684 del 3 de octubre de 2019, las Resoluciones de la SECRETARIA DE GOBIERNO DE MODERNIZACION Nº 829 del 24 de mayo de 2019 y Nº 1523 del 12 de septiembre de 2019,del MINISTERIO DE DEFENSA N° 100 del 17 de enero de 2019, y

CONSIDERANDO:

Que la Ley N° 23.554 establece que la Defensa Nacional tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes.

Que, a tales fines, la norma define a las FUERZAS ARMADAS como el instrumento militar de la Defensa Nacional y prevé su integración con medios humanos y materiales orgánicamente estructurados para posibilitar su empleo en forma disuasiva y efectiva.

Que en virtud del Decreto N° 727/06, el MINISTRO DE DEFENSA tiene a su cargo el deber de dirigir, ordenar y coordinar las actividades propias de la Defensa Nacional que no sean atribuidas por la ley a otro funcionario, órgano u organismo.

Que la Ley N° 24.948 estableció las bases políticas, orgánicas y funcionales fundamentales para la reestructuración de las fuerzas armadas y determinó que para presupuestar las necesidades de cada fuerza y efectuar el control de gestión de los fondos, se utilizaría el SISTEMA DE PLANEAMIENTO, PROGRAMACIÓN Y PRESUPUESTACIÓN (S3P) con medios informáticos compatibles e interoperables con el MINISTERIO DE DEFENSA.

Que a efectos de cumplir con el Sistema mencionado, por Decreto N° 1729/07 se aprobó el Ciclo de Planeamiento de la Defensa Nacional que organiza y encuadra el proceso de definición estratégica, insumo de la primera etapa del Sistema de Planeamiento, Programación y Presupuestación.

Que tal ciclo se inicia con la DIRECTIVA DE POLÍTICA DE DEFENSA NACIONAL (DPDN) a fin de establecer los lineamientos de orientación y planeamiento estratégico de la Política de Defensa y de la Política Militar de la República Argentina.

BOLETÍN OFICIAL
de la República Argentina

PRESIDENCIA DE LA NACIÓN
Secretaría Legal y Técnica | Dra. María Ibarzabal Murphy
Dirección Nacional del Registro Oficial

Que la DPDN explicita los lineamientos centrales de la política de Defensa Nacional y de la política militar, determina los criterios y parámetros que orientan la organización, el funcionamiento, la planificación, el empleo y la administración de los recursos humanos y materiales de las FUERZAS ARMADAS de manera sistemática y coherente en el marco de la política del Estado Nacional.

Que el Decreto N° 703/18 aprobó la DPDN por la que se estableció el deber de la política de ciberdefensa de orientarse a la reducción gradual de las vulnerabilidades que emergen de la informatización de los activos estratégicos de interés para la Defensa Nacional, en cooperación con otras áreas del Estado que tengan responsabilidad en la política de ciberseguridad nacional.

Que la Resolución Nº 829/19 de la SECRETARÌA DE GOBIERNO DE MODERNIZACIÒN aprobó la Estrategia Nacional de Ciberseguridad por la que se establecieron los principios esenciales y los objetivos centrales para la protección del ciberespacio entre los que incluye la Protección de las Infraestructuras Críticas de Información del país, las que posteriormente por la Resolución N° 1523/19 definen en su ANEXO II.

Que entre esas infraestructuras críticas existe un subconjunto cuyo normal funcionamiento resulta esencial para el cumplimiento de las funciones vitales del Estado Nacional, su Defensa Nacional, el ejercicio de la soberanía, la capacidad de autodeterminación y el resguardo de la vida y la libertad de sus habitantes, tal como lo establece la Ley N° 23.554.

Que conforme lo dispuesto por la DPDN, es propósito del MINISTERIO DE DEFENSA desarrollar capacidades para enfrentar el conflicto en el ciberespacio y ejecutar acciones para proteger, monitorear, analizar, detectar y responder a potenciales adversarios o agentes hostiles que afecten a la integridad y disponibilidad de los sistemas de comunicación e informática de las Fuerzas Armadas, Estado Mayor Conjunto de las Fuerzas Armadas y del Ministerio así como la información que ellos gestionan.

Que en particular, se requiere el desarrollo de capacidades para proteger las Infraestructuras Críticas de la Defensa Nacional, lo que incluye las Infraestructuras Criticas del instrumento militar, las propias del MINISTERIO DE DEFENSA, así como las denominadas Infraestructuras Críticas de Interés para la Defensa Nacional, que agrupa a las soporte de los Servicios Esenciales de interés para la defensa y las de los procesos productivos de bienes sensibles.

Que es necesario asegurar la libertad de acción en la conducción de operaciones militares, por lo que es mandatorio extender las fronteras de defensa de las infraestructuras críticas y los sistemas de mando y control propios de las FUERZAS ARMADAS, continuando el proyecto de desarrollo tecnológicamente armonizado de las redes y sistemas de Tecnologías de la Información y Comunicación tal que mediante su gestión centralizada, permita la reducción de las vulnerabilidades ante ciberataques.

Que en cuanto a lo establecido en la DPDN respecto a la elaboración de planes para el accionar militar conjunto para el cumplimiento del objetivo de fortalecimiento de las capacidades de anticipación, disuasión, vigilancia y control de la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional, es necesario que el ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS cuente con la mayor cantidad de información respecto a la topología de redes y sistemas del Instrumento Militar y sus eventuales vulnerabilidades.

Que asimismo la hiperactividad creciente en el ciberespacio y sus características intrínsecas (que el atacante es frecuentemente anónimo y clandestino y que no es posible su neutralización siguiendo los métodos convencionales de intervención) han operado en la mayor parte de los países del mundo, como catalizador del proceso de redefinición de políticas de Defensa Nacional en la búsqueda de un rápido incremento de las capacidades cibernéticas de cada país individualmente o a través de la integración en organismos multilaterales.

Que nuestro país tiene una larga experiencia de trabajo en el marco de acuerdos bilaterales de cooperación con países hermanos en asuntos de la Defensa lo que también se ha extendido a los nuevos dominios de las operaciones militares tales como el ciberespacio, lo que nos proponemos profundizar.

Que también debe continuarse con la actividad en foros multilaterales específicos basadas en el diálogo y la cooperación entre los estados a través de la instrumentación de acuerdos de consulta y que fortalezcan la confianza que se elaboren con la intervención de la SUBSECRETARIA DE ASUNTOS INTERNACIONALES DE LA DEFENSA en el ámbito de sus competencias, conforme lo establecido por el Decreto N° 684/19.

Que a partir de tales acuerdos bilaterales y/o multilaterales se procura desarrollar capacidades de vigilancia y control para proteger la disponibilidad del ciberespacio a fin de prevenir ciberataques y la utilización de las redes y sistemas informáticos bajo control de otro Estado como soporte para operaciones que afecten a las Infraestructuras Críticas del Instrumento Militar o las de Servicios Esenciales de interés para la Defensa Nacional de nuestro país.

Que en virtud de este último Decreto la Subsecretaría de Ciberdefensa tiene entre sus objetivos asistir al Secretario de Estrategia y Asuntos Militares en el dictado de normas para el diseño, implantación y construcción de las redes soporte operacional de Infraestructuras Críticas de la Defensa Nacional, así como ejercer el control funcional sobre el COMANDO CONJUNTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS y las áreas de ciberdefensa y tecnologías de la información y comunicación de las TRES (3) Fuerzas Armadas, así como entender en la planificación, desarrollo y establecimiento de los procedimientos operativos que hacen al funcionamiento del equipo de respuesta ante emergencias informáticas en el Ministerio de Defensa (CSIRT de DEFENSA).

Que en cumplimiento de tales objetivos la Subsecretaría de Ciberdefensa debe realizar acciones preventivas de monitoreo contra potenciales adversarios o agentes hostiles que actuando en el ciberespacio, pretendan afectar la disponibilidad operativa de la infraestructura crítica de servicios esenciales de interés para la Defensa Nacional o la infraestructura soporte de procesos de fabricación de bienes sensibles, lo que exige acordar con los entes reguladores que corresponda la definición de los puntos específicos de las redes a intervenir.

Que para atender a dichos objetivos la SUBSECRETARÍA DE CIBERDEFENSA elaboró la Política de Ciberdefensa que está constituida por cuatro líneas de acción principales que conjugan armónicamente tres ejes de política, a partir de lo cual se formulan el Plan de Infraestructuras Criticas Cibernéticas de la Defensa Nacional y el Plan de Adecuación de Organizaciones Militares.

Que la primera línea de acción principal de la Política es la creación del Centro Nacional de Ciberdefensa el que funcionará en el ámbito de la SUBSECRETARÍA DE CIBERDEFENSA y tendrá el propósito de concentrar el desarrollo de capacidades para asegurar la libertad de acción de las operaciones militares en el dominio cibernético, limitando las vulnerabilidades que surgen de la informatización creciente de las infraestructuras críticas

de la Defensa Nacional y evitando asimismo que se vea afectada la confidencialidad, integridad y disponibilidad de la información.

Que la implementación del Centro contará con la colaboración del personal calificado en la materia que se desempeña en el INSTITUTO DE INVESTIGACIONES CIENTÍFICAS Y TÉCNICAS PARA LA DEFENSA (CITEDEF) y generará programas específicos de investigación, desarrollo e innovación.

Que para garantizar la convergencia de las capacidades del instrumento militar deviene necesario actualizar la normativa organizacional y funcional de cada Fuerza Armada y del ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS para que una Unidad Operacional única concentre capacidades de comunicaciones, informática y ciberdefensa.

Que en ejercicio de las competencias atribuidas por el artículo 13 inciso g) del Decreto N° 727/06, el Ministro de Defensa dictó la Resolución N° 100/19 por la que aprobó la estructura orgánico funcional del ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS en la que incluyó la dependencia orgánico funcional directa del COMANDO CONJUNTO DE CIBERDEFENSA del Jefe del Estado Mayor Conjunto de las Fuerzas Armadas.

Que en función de lo dispuesto por ANEXO II del Decreto N° 684/19, la SECRETARÍA DE ESTRATEGIA Y ASUNTOS MILITARES tiene por objetivo promover la acción conjunta de las FUERZAS ARMADAS en las áreas de competencia específica y coordinar este objetivo con otras unidades ejecutoras de la Jurisdicción.

Que en virtud de la misma norma la SUBSECRETARÍA DE PLANEAMIENTO ESTRATÉGICO Y POLÍTICA MILITAR tiene a cargo la participación en la gestión de los asuntos institucionales de las FUERZAS ARMADAS, así como en lo relacionado con la dirección y coordinación operativa y funcional del instrumento militar.

Que es necesario en consecuencia crear un Comité Consultivo en el ámbito de la SECRETARÍA DE ESTRATEGIA Y ASUNTOS MILITARES compuesto por la SUBSECRETARÍA DE PLANEAMIENTO ESTRATÉGICO Y POLÍTICA MILITAR, la SUBSECRETARÍA DE CIBERDEFENSA y ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS para que realice un estudio pormenorizado de alternativas orgánico funcionales a efectos de elaborar el Plan de Adecuación para la aprobación del Ministro de Defensa.

Que el Decreto N° 9390 del 6 de noviembre de 1963 califica como Secreto Militar a "…toda noticia, informe, material, proyecto, obra, hecho, asunto, que deba, en interés de la seguridad nacional y de los medios de defensa, ser conocido solamente por personas autorizadas y manteniendo fuera del conocimiento de cualquier otra…" (artículo 1°), y a la seguridad nacional como "…la situación en la que los intereses vitales de la Nación se hallan a cubierto de interferencias y perturbaciones sustanciales…" (artículo 2°).

Que los detalles descriptivos de las líneas de acción a implementarse, los ejes de políticas a gestionar para el desarrollo de ellas, los planes consecuentes emergentes y las infraestructuras críticas de la Defensa Nacional a proteger, implican información que debe calificarse como secreto militar para resguardarla de la publicidad.

Que ello se justifica porque en caso de ventilarse los detalles de la estrategia de Ciberdefensa Nacional ella perdería su eficacia por lo que el acceso debe restringirse en aras a la Seguridad y Defensa del Estado Nacional, el

deber de difusión y publicidad cede en virtud de las características específicas de la información comprometida.

Que la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS del MINISTERIO DE DEFENSA ha tomado la intervención que le compete.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el artículo 19 inciso 3) y 4° inciso b) punto 9 de la Ley N° 22520; el artículo 17 de la Ley N° 23.554, y el 5° del Decreto N° 9390/63.

Por ello,

EL MINISTRO DE DEFENSA

RESUELVE:

ARTÍCULO 1°.- Sustitúyese el Artículo 2° de la Resolución del Ministro de Defensa N° 59 del 23 de enero de 2017 por el siguiente:

“Entiéndase por CIBERDEFENSA a las acciones y capacidades desarrolladas por el MINISTERIO DE DEFENSA, EL ESTADO MAYOR CONJUNTO y las FUERZAS ARMADAS para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional, como así también a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o a Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia.”

ARTÍCULO 2°.- Créase el Centro Nacional de Ciberdefensa en el ámbito de la SUBSECRETARÍA DE CIBERDEFENSA, donde funcionarán el CENTRO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS DEL MINISTERIO DE DEFENSA (CSIRT de DEFENSA), el CENTRO INTELIGENTE DE OPERACIONES DE SEGURIDAD (iSOC) del COMANDO CONJUNTO DE CIBERDEFENSA del ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS que centraliza la operación de los CENTROS DE OPERACIONES DE SEGURIDAD (iSOC) remotos de cada una de las Fuerzas Armadas y el LABORATORIO DE ANÁLISIS CIBERNÉTICO (CyberLab), entre otras plataformas y sistemas, cuyas actividades y mecanismos de implementación serán definidos por el SUBSECRETARIO DE CIBERDEFENSA a través de los actos pertinentes.

ARTÍCULO 3°.- Apruébase la Política de Ciberdefensa consistente en CUATRO (4) Líneas de Acción principales que se desarrollarán conjugando TRES (3) ejes de políticas y cuya implementación se realiza a través de DOS (2) planes en orden de cumplimentar los objetivos aprobados por el artículo 2º del Decreto Nº 684 del 3 de octubre de 2019, descriptos en los Anexos I (IF-2019-96170351-APN-SSC#MD), II (IF-2019-96170945-APN-SSC#MD), III (IF-2019-96171204-APN-SSC#MD), IV (IF-2019-96172220-APN-SSC#MD) y V (IF-2019-96171563-APN-SSC#MD), los que se acompañan a la presente Resolución.

ARTÍCULO 4°.- Créase ,en el ámbito de la SECRETARÍA DE ESTRATEGIA Y ASUNTOS MILITARES, el Comité Consultivo de Ciberdefensa que estará integrado por la SUBSECRETARÍA DE PLANEAMIENTO ESTRATÉGICO Y

POLÍTICA MILITAR, la SUBSECRETARÍA DE CIBERDEFENSA y el ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS, cuyo cometido será la realización de estudios para la definición del Plan de adecuación de las Organizaciones Militares y la preparación de la propuesta de la DIRECTIVA PARA LA ELABORACIÓN DEL PLANEAMIENTO ESTRATÉGICO MILITAR (DEPEM) en materias de Tecnologías de la Información y Comunicaciones y ciberespacio en el término de treinta días desde el dictado de la presente.

ARTÍCULO 5°.- Declárase Secreto Militar en los términos del Decreto N° 6390/63, los Anexos I (IF-2019-96170351-APN-SSC#MD), II (IF-2019-96170945-APN-SSC#MD), III (IF-2019-96171204-APN-SSC#MD), y V (IF-2019-96171563-APN-SSC#MD) que se acompañan a la presente Resolución.

ARTÍCULO 6°.- Comuníquese, publíquese con excepción de los Anexos I, II, III y V, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese. Oscar Raúl Aguad

NOTA: El Anexo IV que integra esta Resolución se publica en la edición web del BORA -www.boletinoficial.gob.ar-

e. 29/10/2019 N° 82295/19 v. 29/10/2019

Fecha de publicación 19/11/2024