PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

Decreto Supremo que aprueba el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa

DECRETO SUPREMO
Nº 017-2024-PCM

LA PRESIDENTA DE LA REPÚBLICA

CONSIDERANDO:

Que, el artículo 44 de la Constitución Política del Perú, establece que son deberes primordiales del Estado, defender la soberanía nacional; garantizar la plena vigencia de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y, promover el bienestar general que se fundamenta en la justicia y el desarrollo integral y equilibrado de la Nación;

Que, el Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, de acuerdo a lo establecido en el artículo 8 del citado Decreto Legislativo, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital (actualmente, Secretaría de Gobierno y Transformación Digital), es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital;

Que, el artículo 30 del Decreto Legislativo Nº 1412, establece que la seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno;

Que, según lo dispuesto en los artículos 31 y 32 del Decreto Legislativo Nº 1412, el Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública; y, cuenta, entre otros, con el ámbito de Defensa, según el cual, el Ministerio de Defensa, en el marco de sus funciones y competencias, dirige, norma, supervisa y evalúa las normas en materia de ciberdefensa;

Que, la Ley Nº 30999, Ley de Ciberdefensa, tiene como objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia; con la finalidad de defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional;

Que, el artículo 4 de la citada Ley, define a la ciberdefensa, como la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional;

Que, la Primera Disposición Complementaria Final de la Ley Nº 30999, dispone que la Presidencia del Consejo de Ministros, en coordinación con el Ministerio de Defensa, aprueba el reglamento de la Ley;

Que, en virtud a los numerales 14 y 17 del inciso 28.1 del artículo 28 del Reglamento que desarrolla el Marco Institucional que rige el Proceso de Mejora de la Calidad Regulatoria y establece los Lineamientos Generales para la aplicación del Análisis de Impacto Regulatorio Ex Ante, aprobado por Decreto Supremo Nº 063-2021-PCM, la presente norma se considera excluida del alcance del AIR Ex Ante por la materia que comprende disposiciones consistentes en regular las operaciones militares en y mediante el ciberespacio para preservar la seguridad nacional;

Que, en ese sentido, la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros sustenta la necesidad de aprobar el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa, el cual tiene por objeto establecer las disposiciones normativas para regular las capacidades de ciberdefensa, operaciones militares, y uso de la fuerza en y mediante el ciberespacio, entre otras disposiciones para preservar la seguridad nacional, a cargo de los órganos ejecutores del Ministerio de Defensa, dentro de su ámbito de competencia;

De conformidad con lo dispuesto en el numeral 8 del artículo 118 de la Constitución Política del Perú; la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 30999, Ley de Ciberdefensa; y, el Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Resolución Ministerial Nº 224-2023-PCM;

DECRETA:

Artículo 1.- Aprobación de Reglamento

Aprobar el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa, el mismo que consta de un (01) Título Preliminar, cinco (05) Capítulos en el Título I, dos (02) Capítulos en el Título II, dieciséis (16) artículos y dos (02) Disposiciones Complementarias Finales, el cual forma parte integrante del presente Decreto Supremo.

Artículo 2.- Publicación

Disponer la publicación del presente Decreto Supremo y el Reglamento aprobado mediante el artículo precedente, en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (www.gob.pe) y en las sedes digitales de la Presidencia del Consejo de Ministros (www.gob.pe/pcm) y del Ministerio de Defensa (www.gob.pe/mindef), el mismo día de su publicación en el Diario Oficial El Peruano.

Artículo 3. Financiamiento

La implementación y la sostenibilidad de las acciones involucradas en el Presente Decreto Supremo y el Reglamento, se financia con cargo a los presupuestos institucionales de los Pliegos involucrados, sin demandar recursos adicionales al Tesoro Público.

Artículo 4.- Refrendo

El presente Decreto Supremo es refrendado por el Presidente del Consejo de Ministros y el Ministro de Defensa.

Dado en la Casa de Gobierno, en Lima, a los trece días del mes de febrero del año dos mil veinticuatro.

DINA ERCILIA BOLUARTE ZEGARRA
Presidenta de la República

LUIS ALBERTO OTÁROLA PEÑARANDA
Presidente del Consejo de Ministros

JORGE LUIS CHÁVEZ CRESTA
Ministro de Defensa

REGLAMENTO DE LA LEY Nº 30999, LEY DE CIBERDEFENSA

TÍTULO PRELIMINAR
DISPOSICIONES GENERALES

Artículo I.- Objeto

El presente reglamento tiene por objeto establecer las disposiciones normativas para regular las capacidades de ciberdefensa, operaciones militares, y uso de la fuerza en y mediante el ciberespacio, entre otras disposiciones para preservar la seguridad nacional, a cargo de los órganos ejecutores del Ministerio de Defensa, dentro de su ámbito de competencia, en el marco de la Ley Nº 30999, Ley de Ciberdefensa (en adelante la Ley).

Artículo II.- Finalidad

El presente reglamento tiene por finalidad garantizar que las capacidades nacionales mantengan la continuidad de sus operaciones a través de la protección en y mediante el ciberespacio de los activos críticos nacionales, recursos claves, la soberanía y los intereses nacionales frente amenazas o ataques, cuando estos afecten la seguridad nacional.

Artículo III.- Marco jurídico aplicable

Las operaciones militares en y mediante el ciberespacio, cuando afecten la seguridad nacional, se sujetan a lo establecido en la Constitución Política del Perú, la legislación nacional y las normas del derecho internacional que resulten aplicables.

Artículo IV. Definiciones

Para efectos de la Ley y el presente reglamento se entiende de forma específica las siguientes definiciones:

a. Activos Críticos Nacionales (ACN): Es la establecida en el numeral 3.4 del artículo 3 del Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN), aprobado por Decreto Supremo Nº 106-2017-PCM.

b. Acto hostil en el ciberespacio: Es toda acción en y mediante el ciberespacio que atenta contra la seguridad nacional, soberanía, los intereses nacionales, los ACN/RC. Da derecho al ejercicio de la legítima defensa conforme a las reglas de enfrentamiento establecidas por la autoridad competente, de acuerdo con la normatividad vigente. Con frecuencia son no cinéticos, dificultando la determinación y atribución.

c. Amenaza en el ciberespacio: Todo acto fuente, circunstancia o evento de origen externo o interno con la capacidad potencial de generar, a través del uso de sistemas, herramientas cibernéticas o cualquier otro instrumento en y mediante el ciberespacio, efectos adversos, daños o perjuicios a la seguridad nacional, soberanía, los intereses nacionales, los ACN/RC (Entiéndase también como ciberamenazas).

d. Arma cibernética: Agente de software empleado para objetivos de interés militar como parte de una acción ofensiva en y mediante el ciberespacio. Entiéndase también como ciberarma.

e. Ciberespacio: Comprende el conjunto de redes interconectadas e interdependientes de infraestructura de tecnología de la información, que incluyen a internet, las redes de telecomunicaciones, sistemas aislados (redes, sistemas y dispositivos de almacenamiento de información no conectados a internet), software, información, los protocolos de transportes, la energía eléctrica, los sistemas informáticos, procesadores y controladores integrados, junto con las personas que interactúan con ellos, entiéndase también como entorno digital. Conceptualmente es un ámbito sin un espacio físico más allá de la jurisdicción de cualquier nación.

f. Ciberseguridad: Es la establecida en el inciso h) del artículo 3 del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

g. Incidente de seguridad digital: Es la establecida en el inciso e) del artículo 3 del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

h. Infraestructura: Es la establecida en el inciso 3.3, del artículo 3, del Decreto Supremo Nº 106-2017-PCM, Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

i. Intención hostil en el ciberespacio: Es toda acción que evidencia la voluntad o preparación para ejecutar un acto hostil en o mediante el ciberespacio que atente contra la seguridad nacional, la soberanía, los intereses nacionales, los ACN/RC. Al igual que los actos hostiles son con frecuencia no cinéticos, lo que dificulta su determinación y atribución.

j. Legítima defensa: Es el derecho que tiene el Estado, mediante el empleo de los componentes de ciberdefensa de los órganos ejecutores del Ministerio de Defensa, de usar la fuerza en y mediante el ciberespacio para impedir, contener y/o neutralizar un acto o intención hostil, que atente o ponga en riesgo la Seguridad Nacional.

k. Marco de Seguridad Digital del Estado Peruano: Es la establecida en el artículo 31 del Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital.

l. Operaciones militares en el ciberespacio: Es el empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo con sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o ataques que atenten contra la seguridad nacional, la soberanía, los intereses nacionales y/o los ACN/RC. Entiéndase también como ciberoperaciones.

m. Operador de los Activos Críticos Nacionales - ACN: Es la establecida en el inciso 3.6, del artículo 3, del Decreto Supremo Nº 106-2017-PCM, Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

n. Recursos Claves: Es la establecida en el inciso 3.13 del artículo 3 del Decreto Supremo Nº 106-2017-PCM, Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

o. Reglas de enfrentamiento: Se entiende de acuerdo con lo establecido en el artículo 10 del presente reglamento.

p. Riesgo de Seguridad Digital: Es la establecida en el inciso g) del artículo 3 del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

q. Sector Responsable: Es la establecida en el inciso 3.5, del artículo 3, del Decreto Supremo Nº 106-2017-PCM, Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

r. Seguridad Digital: Es la establecida en el artículo 30 del Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital.

s. Seguridad nacional: Es la situación en la cual el Estado tiene garantizada su independencia, soberanía e integridad y, la población los derechos fundamentales establecidos en la Constitución. Esta situación contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, basada en los valores democráticos y en el respeto a los derechos humanos.

t. Uso de la fuerza: Entiéndase por uso de la fuerza, a la actuación que realizan las Fuerzas Armadas, en y mediante el ciberespacio, con los medios y métodos que correspondan, los cuales se encuentran delimitados a lo que dispone el artículo 51 de la Carta de las Naciones Unidas, la ley de Ciberdefensa y las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario y demás normativa del derecho internacional aplicable.

u. Vulnerabilidades cibernéticas: Debilidad o ausencia de capacidad para la defensa cibernética que puede ser utilizada por una amenaza. Esto comprende, pero no se limita a, un diseño deficiente, errores de configuración o técnicas de codificación, debilidades tecnológicas o políticas de seguridad inadecuadas e inseguras.

Artículo V. Acrónimos

Para efectos del presente reglamento se aplican los siguientes acrónimos:

a. ACN: Activos críticos nacionales
b. RC: Recursos clave
c. REN: Reglas de enfrentamiento
d. JCCFFAA: Jefe del Comando Conjunto de las Fuerzas Armadas
e. COCID: Comando Operacional de Ciberdefensa

TÍTULO I
DE LA CIBERDEFENSA

CAPÍTULO I
DEL MINISTERIO DE DEFENSA

Artículo 1.- Rol del Ministerio de Defensa en la Ciberdefensa

Para la gestión del marco de Seguridad Digital del Estado Peruano, en el ámbito de la defensa, el Ministerio de Defensa, dentro del alcance de sus funciones y competencias dirige, norma, supervisa y evalúa las disposiciones en materia de ciberdefensa.

El Ministerio de Defensa, es la entidad encargada de gestionar la ciberdefensa. Asimismo, dicta políticas y lineamientos para el planeamiento y conducción de operaciones militares en y mediante el ciberespacio conforme a la Política de Seguridad y Defensa Nacional aprobada por el Consejo de Seguridad y Defensa Nacional y de manera articulada con los objetivos de seguridad nacional y con la Política Nacional de Transformación Digital, aprobada mediante el Decreto Supremo Nº 085-2023-PCM u otra norma que lo sustituya.

CAPÍTULO II
DE LOS ÓRGANOS EJECUTORES DEL MINISTERIO DE DEFENSA EN MATERIA DE CIBERDEFENSA

Artículo 2.- Órganos Ejecutores del Ministerio de Defensa y componentes de ciberdefensa

Los órganos ejecutores del Ministerio de Defensa están constituidos por el Ejército, la Marina de Guerra, la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas.

La ciberdefensa comprende al COCID, y a sus componentes de ciberdefensa que son: el componente de Ciberdefensa del Ejército del Perú, componente de Ciberdefensa de la Marina de Guerra del Perú y componente de Ciberdefensa de la Fuerza Aérea del Perú, los cuales ejecutan operaciones de ciberdefensa en y mediante el ciberespacio.

Artículo 3.- Responsabilidades del Comando Operacional de Ciberdefensa

Son responsabilidades del COCID los siguientes:

a. Planear, organizar y conducir las operaciones militares en y mediante el ciberespacio, ejerciendo el comando y control de las operaciones de ciberdefensa conjuntas.
b. Proteger sus sistemas de información y el segmento del ciberespacio asignado.
c. Gestionar el registro de incidentes, el intercambio de información sobre ataques informáticos y patrones de amenazas entre los componentes de ciberdefensa de las Instituciones Armadas. Dicho registro es interno y de uso

exclusivo del COCID, y tiene relevancia únicamente para las operaciones que realicen las Fuerzas Armadas.

d. Otras que se asignen en la normativa legal sobre la materia.

Artículo 4.- Responsabilidades de los componentes de ciberdefensa de las Instituciones Armadas

Son responsabilidades de los componentes de ciberdefensa de las Instituciones Armadas las siguientes:

a. Planear, organizar y conducir a su nivel las operaciones militares en y mediante el ciberespacio, ejerciendo el comando y control de las operaciones de ciberdefensa propias.

b. Proteger sus sistemas de información y el segmento del ciberespacio propio o asignado.

c. Alistar integralmente a las unidades a su cargo, para el eficiente desempeño de sus funciones.

d. Desarrollar y mantener un óptimo nivel de sus capacidades de ciberdefensa.

e. Otras que se asignen en la normativa legal sobre la materia.

CAPÍTULO III
CAPACIDADES DE CIBERDEFENSA

Artículo 5.- De las medidas pasivas y activas de ciberdefensa

5.1 Medidas pasivas en ciberdefensa: conjunto de actividades de prevención, protección y resiliencia del ciberespacio propio y/o asignado. Son de aplicación constante y generalizada, abarcando al personal, medios y sistemas propios o asignados. Involucra, pero no se limita al monitoreo de redes propias o asignadas, mantenimiento de sistemas informáticos, actualizaciones de seguridad y operativas, establecimiento de políticas, disposiciones, procedimientos y reglas de seguridad institucional, robustecimiento en la infraestructura cibernética propia y la concientización en materia de ciberdefensa, entre otras.

5.2 Medidas activas en ciberdefensa: conjunto de actividades de naturaleza proactiva, reactiva o de recuperación, en o mediante el ciberespacio propio, asignado y/o de interés. Estas medidas se aplican ante la necesidad militar para la defensa y la seguridad nacional. Involucra, pero no se limita al análisis de vulnerabilidades, una intensa labor de detección, evaluación, identificación y reconocimiento de actos hostiles o amenazas en el ciberespacio; o la aplicación de acciones cibernéticas sobre medios o sistemas que constituyen una amenaza, para degradar o neutralizar sus capacidades y formas de acción, a fin de impedir que estas puedan afectar la libertad de acción en el ciberespacio propio, asignado y/o de interés, entre otras.

Artículo 6.- Capacidades de ciberdefensa de los Órganos Ejecutores del Ministerio de Defensa

En el ámbito de sus competencias, el COCID y los Componentes de Ciberdefensa de las Instituciones Armadas cuentan con las capacidades siguientes:

a. Capacidad de Defensa: consiste en la prevención, protección y resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas.

b. Capacidad de explotación: consiste en la búsqueda, identificación, reconocimiento, vigilancia y seguimiento de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas.

c. Capacidad de respuesta: consiste en limitar o negar, temporal o permanentemente, el uso del ciberespacio del objetivo militar mediante la degradación o neutralización de sus sistemas, impactando en sus capacidades; recurriendo a medidas activas.

d. Capacidad de investigación digital o Investigación Forense Digital: consiste en el análisis de evidencia digital con la finalidad de determinar su funcionalidad, comportamiento, origen e impacto; así como su explotación futura a través de un proceso de ingeniería inversa. Engloba técnicas de investigación y análisis forense digital para recolectar, analizar y preservar evidencias sobre actos maliciosos en el ciberespacio, recurriendo a medidas pasivas y activas. Esta capacidad de ciberdefensa se ejerce de acuerdo a las competencias asignadas, la cual no se vincula ni contrapone con la Investigación Digital que pueda realizar cualquier otra entidad pública o privada.

CAPÍTULO IV
OPERACIONES MILITARES EN Y MEDIANTE EL CIBERESPACIO

Artículo 7.- De las Operaciones Militares en y mediante el ciberespacio

Comprende el conjunto de acciones orientadas, planificadas, organizadas y coordinadas para ser ejecutadas en y mediante el ciberespacio, con la finalidad de generar los efectos militares deseados para la seguridad nacional.

Con el empleo de las capacidades de ciberdefensa en las operaciones militares, articuladas sistémicamente por los componentes de ciberdefensa, de acuerdo a sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o ataques cuando estos afecten la Seguridad Nacional. Entiéndase también como ciberoperaciones.

CAPÍTULO V
DEL USO DE LA FUERZA EN Y MEDIANTE EL CIBERESPACIO

Artículo 8.- Del uso de la fuerza en las operaciones de Ciberdefensa

8.1 Los componentes de ciberdefensa de las Instituciones Armadas recurren al uso de la fuerza en y mediante el ciberespacio para degradar o neutralizar las capacidades y formas de acción del adversario, que afecten la libertad de acción propia en el ciberespacio, ante la necesidad militar para la Defensa y la seguridad nacional.

8.2 El uso de la fuerza en y mediante el ciberespacio sólo se atribuye a los componentes mencionados en el párrafo precedente en operaciones militares bajo la conducción del JCCFFAA, de conformidad con lo dispuesto en las normas de Derecho Internacional de Derechos Humanos, del Derecho Internacional Humanitario y demás normativa del derecho internacional aplicable.

Artículo 9.- Autorización para el uso de la fuerza

La autorización para el uso de la fuerza en las operaciones militares en y mediante el ciberespacio que atente contra la seguridad nacional está sujeta a disposición expresa, por parte del Presidente de la República, Jefe Supremo de las Fuerzas Armadas, que se efectúa por medio de Resolución Suprema refrendada por el Ministro de Defensa, y se ejecuta a través de los procedimientos establecidos para las otras operaciones militares, conforme a la normativa establecida para tal fin.

Artículo 10.- Reglas de enfrentamiento

Son instrucciones emitidas por el JCCFFAA, mediante los cuales se mantiene el control sobre el uso de la fuerza por parte de las Fuerzas Armadas durante la ejecución de las operaciones militares en y mediante el ciberespacio ante un acto hostil e intención hostil que afecten la seguridad nacional. Se aprueban por Resolución Suprema refrendada por el Ministro de Defensa.

Artículo 11.- Finalidades de las reglas de enfrentamiento

Las REN comprenden las siguientes finalidades:

a. Legal.- Las REN constituyen un medio para asegurar que la actuación militar se sujete al marco jurídico vigente, tanto nacional como internacional durante la ejecución de las operaciones militares en y mediante el ciberespacio.

b. Militar.- Las REN sirven de guía a los comandantes en lo referido al uso de la fuerza, durante la ejecución de las operaciones militares en y mediante el ciberespacio, estableciendo límites a su accionar.

c. Política.- Las REN son una forma de asegurar que las Fuerzas Armadas actúen según los lineamientos

políticos del nivel estratégico, vinculados al estado final deseado.

Artículo 12.- Requerimiento, autorización o negación e implementación de las reglas de enfrentamiento

12.1 Cuando resulte necesario, el comandante militar que conduce las operaciones en y mediante el ciberespacio, puede requerir ante su superior inmediato la implementación, modificación o cancelación de alguna REN, a través del mecanismo de solicitud formal establecido por el JCCFFAA.

12.2 El comando superior que recibe la solicitud de implementación, modificación o cancelación de alguna REN se encuentra facultado para autorizar o denegar dicha solicitud, empleando los mecanismos formales establecidos por el JCCFFAA. Asimismo, el comando superior que recibe la solicitud, se encuentra facultado a incorporar restricciones adicionales a las REN liberadas.

Artículo 13.- De la responsabilidad y su exención

Los supuestos de exención de responsabilidad penal derivados del uso de la fuerza durante las operaciones militares en y mediante el ciberespacio en aplicación de la Ley Nº 30999, Ley de Ciberdefensa y el presente reglamento son regulados conforme con lo establecido en los incisos 8 y 11 del artículo 20 del Código Penal.

TÍTULO II
DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES

CAPÍTULO I
DE LA PROTECCIÓN DE CONTROL DE LOS ACN/RC

Artículo 14.- Protección y control de los activos críticos nacionales y recursos claves en y mediante el ciberespacio

14.1 Se considera que la seguridad digital de los ACN/RC es afectada cuando se genera un ataque directo o inminente a sus recursos, infraestructura y sistema en sus componentes digitales, por la materialización de riesgos derivados de amenazas y vulnerabilidades en y mediante el ciberespacio, y que generen como consecuencia daños a la persona, prosperidad económica, social y la seguridad nacional.

14.2 En el ámbito de la seguridad nacional, cuando la capacidad de protección en el ciberespacio de los operadores de los ACN/RC, del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia (DINI) sean sobrepasados, la protección y control de los mismos está a cargo del COCID, siguiendo el protocolo señalado en el artículo 16 del presente reglamento, con la finalidad de mantener las capacidades nacionales.

CAPÍTULO II
DE LOS PROTOCOLOS DE ESCALAMIENTO, COORDINACIÓN, INTERCAMBIO Y ACTIVACIÓN PARA LA PROTECCIÓN DE LOS ACN/RC

Artículo 15.- De los responsables y etapas para la protección de los ACN/RC

La protección de los ACN/RC en y mediante el ciberespacio se realiza a través de los siguientes responsables y etapas:

15.1 En un primer momento, la ciberseguridad del ACN/RC está a cargo de su propio operador para preservar la Seguridad Digital, en cumplimiento de la normatividad vigente en seguridad y confianza digital; asimismo, coordina con el sector responsable y la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces.

15.2 En un segundo momento, a su solicitud, cuando se presente un incidente que no pueda ser gestionado por el operador o supere sus capacidades, la Dirección Nacional de Inteligencia (DINI) complementa la capacidad de ciberseguridad del operador del ACN/RC, en coordinación con la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces.

15.3 En un tercer momento, a su solicitud, cuando la capacidad de ciberseguridad de los Operadores de los ACN/RC, el sector responsable y la DINI sea sobrepasada, el Ministerio de Defensa, a través del Comando Conjunto de las Fuerzas Armadas y el COCID complementa las capacidades de ciberseguridad con sus capacidades de ciberdefensa.

15.4 En un cuarto momento, la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, a través del Centro Nacional de Seguridad Digital, en el marco de sus competencias establecidas en el Decreto de Urgencia Nº 007-2020, ejerce sus propias facultades y/o acude a la asistencia nacional e internacional en materia de Seguridad Digital cuando las capacidades de ciberseguridad y ciberdefensa nacionales hayan sido sobrepasadas. La asistencia internacional complementa las capacidades de Ciberseguridad de los operadores de los ACN/RC, el sector responsable, la DINI y las capacidades de ciberdefensa de los órganos ejecutores del Ministerio de Defensa.

Artículo 16.- Sobre el Protocolo de escalamiento, coordinación, intercambio y activación de incidentes de seguridad digital

16.1 El Protocolo de escalamiento, coordinación, intercambio y activación, debe incluir los procedimientos detallados, criterios y condiciones para la identificación y cambio de momento a los cuales se refiere el artículo precedente, así como la asignación de responsabilidades y la cadena de autoridad apropiada, de acuerdo a la normativa legal vigente.

16.2 El Protocolo de escalamiento, coordinación, intercambio y activación debe ser legible para humanos y adecuados para su uso mediante plataformas digitales o aplicaciones informáticas que automaticen el intercambio de información.

16.3 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, elabora y emite el Protocolo de escalamiento, coordinación, intercambio y activación de incidentes de seguridad digital de los ACN/RC, de conformidad con lo establecido en el artículo 13 de la Ley.

16.4 Cuando algún incidente de seguridad digital comprometa los ACN/RC, se ejecuta el Protocolo de escalamiento, coordinación, intercambio y activación a través de las Directivas y/o lineamientos emitidos por la Secretaría de Gobierno y Transformación Digital o la que haga sus veces.

16.5 El referido protocolo se ejecuta con la comunicación directa e inmediata desde la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, al titular o representante del sector correspondiente.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Entrenamiento de capacidades en ciberdefensa

Los Órganos Ejecutores del Ministerio de Defensa establecen de manera permanente ejercicios en ciberdefensa con la finalidad de entrenar las capacidades en ciberdefensa.

Segunda. Protocolo de escalamiento, coordinación, intercambio y activación de incidentes de seguridad digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, emite los protocolos de escalamiento, coordinación, intercambio y activación de incidentes de seguridad digital de los ACN/RC, en un plazo no mayor a ciento ochenta (180) días hábiles contados a partir del día siguiente de la publicación del presente Reglamento.

2261522-1