SEGUNDO SUPLEMENTO

REGISTRO OFICIAL®
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

MINISTERIO DE DEFENSA NACIONAL

MINISTERIO
DE DEFENSA NACIONAL

RESOLUCIÓN No. 026

SE APRUEBA LA "ESTRATEGIA DE CIBERDEFENSA 2026"

Año II - Nº 284 - 94 páginas
Quito, jueves 14 de mayo de 2026

PUBLICADO EN LA ORDEN GENERAL MINISTERIAL No. 030 DE 26-FEB-2026

MINISTERIO DE DEFENSA NACIONAL

RESOLUCIÓN MINISTERIAL No. 026

Gian Carlo Loffredo Rendón
MINISTRO DE DEFENSA NACIONAL

CONSIDERANDO:

Que el artículo 3 de la Constitución de la República del Ecuador, determina: *"Son deberes primordiales del Estado: (…) 2. Garantizar y defender la soberanía nacional, (…) 8. Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción";*

Que el artículo 66 ibidem, señala: *"Se reconoce y garantizará a las personas: (…) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (…) 21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación (…)";*

Que el artículo 141, inciso segundo ibidem, señala que, al establecer la integración de la Función Ejecutiva, dispone que los ministros de Estado deben cumplir, en el ámbito de su competencia, las atribuciones de rectoría, planificación, ejecución y evaluación de las políticas públicas nacionales y planes que se creen para ejecutarlas;

Que el artículo 154, numeral 1 ibidem preceptúa que las ministras y ministros de Estado, además de las atribuciones establecidas en la ley, les corresponde: *"Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión";*

Que el artículo 158 ibidem, expresa que las Fuerzas Armadas es una institución de protección de los derechos, libertades y garantías de los ciudadanos; y su misión fundamental es la defensa de la soberanía e integridad territorial;

Que el artículo 226 ibidem, dispone: "*Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.";*

Que el artículo 279 ibidem, determina que el sistema nacional descentralizado de planificación organizará la planificación para el desarrollo, que estará conformado por un Consejo Nacional de Planificación que integra a los distintos niveles de Gobierno, con participación ciudadana; y, tendrá una Secretaría Técnica, que lo coordinará;

Que el artículo 280 ibidem, prevé que el Plan Nacional de Desarrollo es el instrumento al que se sujetarán las políticas, programas y proyectos públicos, la programación y ejecución del Presupuesto del Estado, y la inversión y la asignación de los recursos públicos; coordinará las competencias exclusivas entre el Estado Central y los gobiernos autónomos descentralizados, siendo su observancia de carácter obligatorio para el sector público e indicativo para los demás sectores;

Que el artículo 313 ibidem, determina que, el Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia. Los sectores estratégicos, de decisión y control exclusivo del Estado, son aquellos que por su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, y deberán orientarse al pleno desarrollo de los derechos y al interés social;

Que el artículo 8 de la Ley Orgánica de la Defensa Nacional, establece: *"El Ministerio de Defensa Nacional, es el órgano político, estratégico y administrativo de la defensa nacional.";*

Que el artículo 10 ibidem, establece las atribuciones y obligaciones del señor ministro de Defensa Nacional, entre las cuales consta: *"(…) b) Ejercer la representación legal del Ministerio de Defensa Nacional y de las Ramas de las Fuerzas Armadas; (…) d) Emitir las políticas para la planificación estratégica institucional; e) Coordinar y apoyar la política de seguridad del Estado;"*;

Que en el artículo 11, letra a) ibidem concluye que: la defensa de la soberanía del Estado y la integridad tendrá como ente rector al Ministerio de Defensa Nacional;

Que el artículo 6 de la Ley Orgánica para la Transformación Digital y Audiovisual**,** indica: *"El uso estratégico de tecnologías digitales y datos en la Administración Pública, como parte integral de las estrategias de modernización de los gobiernos para crear valor público (…) El Gobierno Digital se fundamenta en los pilares de la gobernanza de datos, interoperabilidad y seguridad digital. La Administración Pública del Estado ecuatoriano estará determinada por una real y eficiente gobernanza digital entendiéndose por aquélla al conjunto de procesos, estructuras, herramientas y normas que permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la institucionalidad.";*

Que el artículo 17 ibidem, preceptúa: *"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. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.";*

Que el artículo 19 ibidem, determina: *"El Marco de Seguridad Digital del Estado se tienen que observar y cumplir con lo siguiente:*

a. *Defensa: El Ministerio de Defensa en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa;*
b. *Inteligencia: El Centro de Inteligencia Estratégica o la entidad que haga sus veces, como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia;*
c. *Justicia: El Ministerio de la Mujer y Derechos Humanos, el Ministerio del Interior, la Policía Nacional, la Fiscalía General del Estado y la Corte Nacional de Justicia, en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en*

materia de ciberdelincuencia, d. Institucional: Las entidades de la Administración Pública deberán establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información.";

Que el artículo 10 ibidem, enfatiza: "*La entidad encargada de la coordinación de la seguridad pública y del Estado cumplirá las siguientes funciones: "a) Formular el Plan Nacional de Seguridad Integral y propuestas de políticas de seguridad pública y del Estado con el aporte de los órganos del Sistema, otras entidades del Estado y de la ciudadanía para ponerlas en consideración del presidente de la República y del Consejo de Seguridad Pública y del Estado (…)";*

Que el artículo 11 ibidem, instituye: *"Los órganos ejecutores del Sistema de Seguridad Pública y del Estado estarán a cargo de las acciones de defensa; seguridad ciudadana, protección interna y orden público; prevención; gestión integral de riesgos; y, gestión penitenciaria, conforme lo siguiente: a) (…) La defensa de la soberanía del Estado y la integridad territorial tendrá como entes rectores al ministerio rector de la defensa nacional y al ministerio rector de la política exterior en los ámbitos de su responsabilidad y competencia. Corresponde a las Fuerzas Armadas su ejecución para cumplir con su misión fundamental de defensa de la soberanía e integridad territorial.";*

Que el artículo 43 ibidem, menciona: *"El ministro de Defensa Nacional ante circunstancias de inseguridad críticas que pongan en peligro o grave riesgo la gestión de las empresas públicas y privadas, responsables de la gestión de los sectores estratégicos dispondrá a las Fuerzas Armadas, como medida de prevención, la protección de las instalaciones e infraestructura necesaria para garantizar el normal funcionamiento (…)";*

Que el artículo 66 de la Ley de Seguridad Pública y del Estado, establece: *"La entidad encargada de la coordinación de la seguridad pública y del Estado, o quien haga sus veces, establecerá el procedimiento para atender las solicitudes de excepciones respecto a la adquisición de tierras y concesiones en zonas de seguridad de frontera y en áreas reservadas de seguridad (…)";*

Que el artículo 190 del Código Orgánico Integral Penal**,** dicta: *"La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.";*

Que el artículo 229 del mismo cuerpo legal, establece: *"La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.";*

Que acerca de la competencia normativa de carácter administrativo, el artículo 130 ibidem, manifiesta: *"Las máximas autoridades administrativas tienen competencia normativa de carácter administrativo únicamente para regular los asuntos internos del órgano a su cargo, salvo los casos en los que la ley prevea esta competencia para la máxima autoridad legislativa de una administración pública. La competencia regulatoria de las actuaciones de las personas debe estar expresamente atribuida en la ley";*

Que el artículo 231 ibidem, dispone: *"La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años";*

Que el artículo 234 ibidem, señala: *"Acceso no consentido a un sistema informático, telemático o de telecomunicaciones; 1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años; 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años."*;

Que el artículo 234 ibidem, establece: *"Falsificación informática: 1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años; 2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena.";*

Que a través del Decreto Ejecutivo N° 633 de 8 de enero de 2019, se expide la Política de la Defensa Nacional, como una política pública participativa y producto de una reflexión integral que permitirá mejorar la planificación sectorial, la interacción con la sociedad civil y redefinir la política de defensa ante el escenario geopolítico actual;

Que con el Acuerdo Ministerial N° MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, expide el Esquema Gubernamental de Seguridad de la Información – EGSI que se encuentra como Anexo al presente Acuerdo Ministerial, el cual es el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público;

Que través del oficio N° MDN-SUF-2026-0337-OF de 27 de enero de 2026, el señor subsecretario de Defensa Nacional, manifiesta: *"En alcance al oficio N° MDN-SUF-2025-4674-OF de fecha 14 de diciembre de 2025, en el cual se solicita: "(...) la revisión y aprobación de la Estrategia de Ciberdefensa, en cumplimiento al Estatuto Orgánico de Gestión Organizacional del Ministerio de Defensa vigente, en donde se determinan los productos de la Gestión de Análisis y Prospectiva de la Defensa, específicamente: literal i) Directrices y Estrategias de Ciberdefensa (...)"; mediante el presente me permito muy respetuosamente remitir a usted señor Ministro de Defensa Nacional, la Estrategia de Ciberdefensa 2026, con los cambios realizados de acuerdo a reuniones mantenidas (…)", mismo que ha sido aprobado por el titular de esta cartera de Estado;*

Que el señor subsecretario de Defensa Nacional, mediante oficio N° MDN-SUF-2026-0382-OF de 30 de enero de 2026, en el cual solicita: "se *elabore el Acuerdo Ministerial para la publicación de la Estrategia de Ciberdefensa 2026, una vez que se ha completado el proceso de revisión y aprobación por parte del señor ministro de Defensa Nacional (…)";*

Que mediante oficio N° MDN-SUF-2026-0382-OF de 30 de enero de 2026, mediante el cual el señor subsecretario de Defensa Nacional, solicita la elaboración del Acuerdo Ministerial para la publicación de la Estrategia de Ciberdefensa 2026, en cumplimiento al Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Defensa Nacional vigente, en donde se determinan los productos de la gestión de Análisis y Prospectiva de la Defensa, específicamente el literal i) Directrices y Estrategias de Ciberdefensa;

Que el propósito de la Estrategia de Ciberdefensa es definir directrices orientadas a fortalecer las capacidades de ciberdefensa, a fin de permitir a las Fuerzas Armadas cumplir su misión constitucional y ejecutar operaciones eficaces de defensa, exploración y respuesta frente a ciberataques; así como garantizar la protección de la infraestructura crítica digital institucional y contribuir a la defensa de la infraestructura crítica digital del Estado; para lo cual dicha Estrategia se construye tomando como referencia los principales instrumentos de planificación nacional vigentes en materia de seguridad y defensa; y,

En ejercicio de las atribuciones previstas en el artículo 154 de la Constitución de la República del Ecuador, artículo 130 del Código Orgánico Administrativo y el artículo 10, letra g) de la Ley Orgánica de la Defensa Nacional,

RESUELVE:

Art. 1.- Aprobar la "Estrategia de Ciberdefensa 2026", que se adjunta y forma parte integra del presente instrumento jurídico.

Art. 2.- Disponer que la Subsecretaría de Defensa Nacional, difunda la "*Estrategia de Ciberdefensa 2026"* a las dependencias que conforman la Planta Central del Ministerio de Defensa Nacional, el Comando Conjunto de las Fuerzas Armadas, Fuerzas: Terrestre, Naval y Aérea y las entidades adscritas y dependientes.

Art. 3.- Deróguese todos los documentos que se opongan o no guarden conformidad con los contenidos de la *" Estrategia de Ciberdefensa 2026".*

Art. 4.- La presente Resolución Ministerial entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en la Orden General Ministerial y, en el Registro Oficial.

Publíquese y Comuníquese. -

Dado en Quito, DM, a **26-FEB-2026**

Firmado electrónicamente por:
GIAN CARLO LOFFREDO RENDON
Validar únicamente con FirmaEC

Gian Carlo Loffredo Rendón
MINISTRO DE DEFENSA NACIONAL


REPUBLICA DEL ECUADOR
MINISTERIO DE DEFENSA NACIONAL

CERTIFICO. - Que el documento que en 05 (cinco) páginas antecede, es fiel copia del documento firmado y que consta en los Archivos Digitales de Ordenes Generales Ministeriales de la Dirección de Secretaría General de esta Cartera de Estado: ***"Resolución Ministerial No. 026 del 26 de febrero de 2026, publicado en la Orden General Ministerial No. 030 de la misma fecha"***

Quito, D.M. 09 de abril de 2026

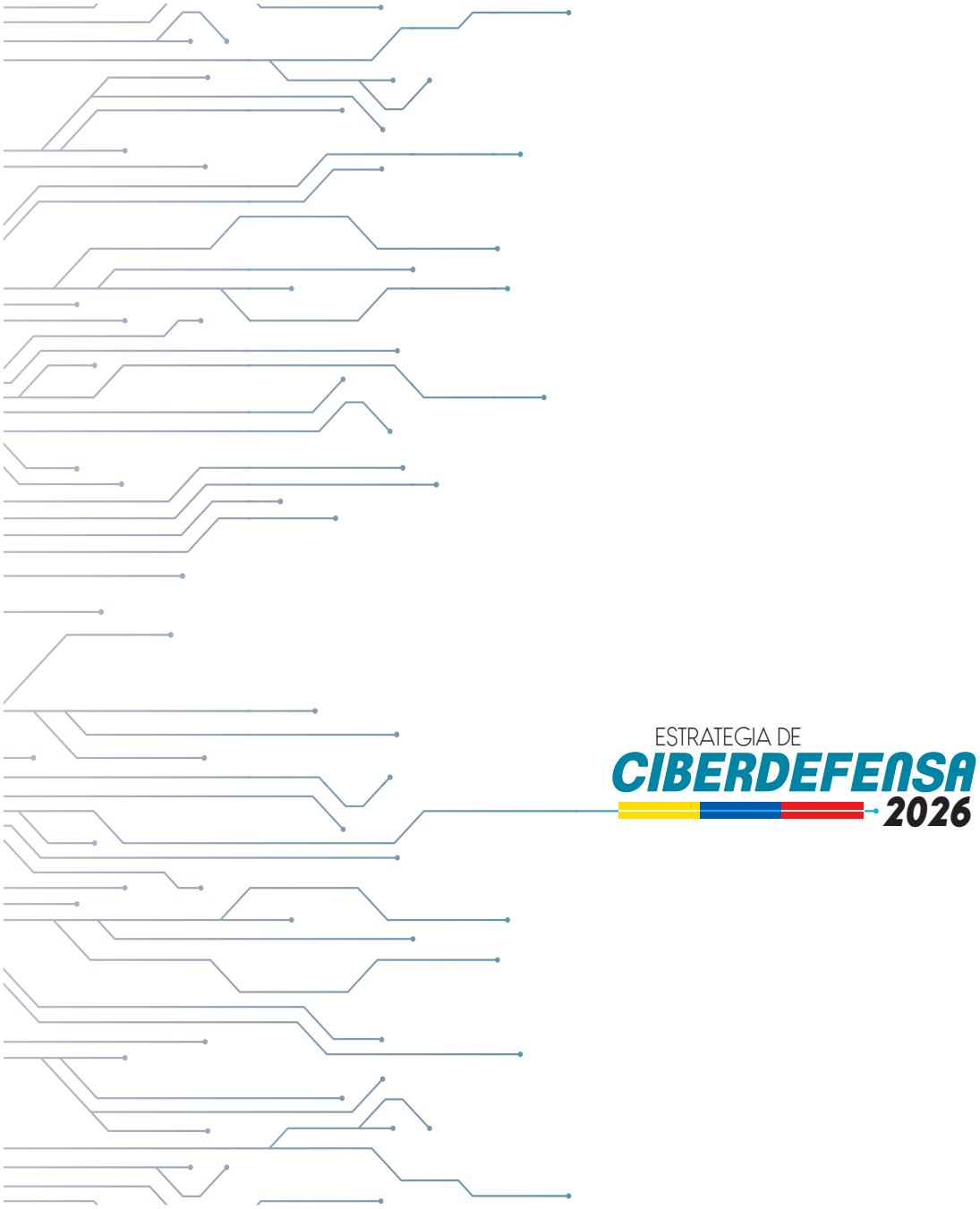
Firmado electrónicamente por:
LUIS ALBERTO ULLOA VARGAS
Validar únicamente con FirmaEC

Sr. José Francisco Zúñiga Albuja
DIRECTOR DE SECRETARÍA GENERAL

SGCP. ULLOA L

Base Legal: Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Defensa Nacional, con respecto a las atribuciones del Directorio de Secretaría General en el Art. 9 numeral 3.2.6 de Gestión de Secretaría General literal d) Instructivo para el almacenamiento y certificación de documentos institucionales firmados electrónicamente Art. 7 y 9.


MINISTERIO DE
DEFENSA
NACIONAL
PUBLICADO EN LA ORDEN
GENERAL MINISTERIAL
No. 030 DE 26-FEB-2026
ESTRATEGIA DE
CIBERDEFENSA
2026


ESTRATEGIA DE
CIBERDEFENSA
2026


CIBERSEGURIDAD

DIRECCIÓN EJECUTIVA

Grab. Landázuri Recalde Frank Patricio
SUBSECRETARIO DE DEFENSA NACIONAL
(SEPTIEMBRE 2024 – SEPTIEMBRE 2025)
Grab. Cañizares Cisneros Edwin Patricio
SUBSECRETARIO DE DEFENSA NACIONAL

COORDINADOR GENERAL

Crnl. – PhD. González Mosquera Oswaldo Mauricio
DIRECTOR DE ANÁLISIS Y PROSPECTIVA DE LA DEFENSA

EQUIPO TÉCNICO DE ELABORACIÓN

Mayo. (S.P) Recalde Herrera Luis Lenin
Líder del Equipo Técnico
Asesor de la Universidad de las Fuerzas Armadas ESPE
Mayo. Rosero Romero Cyntia Ibeth
Analista de Ciberdefensa del Ministerio de Defensa Nacional
Tnnv. Ordóñez Mancheno Giovanni Mauricio
Analista de Ciberdefensa del Ministerio de Defensa Nacional
Capt. Villareal Jiménez Lenin Ramiro
Analista de Ciberdefensa del Ministerio de Defensa Nacional
Eco. Diana Vanessa Duque Torres
Desarrollo Metodológico

DISEÑO Y DIAGRAMACIÓN

Ing. Christian Roberto Mantilla Cifuentes
Diagramador del Instituto Geográfico Militar

CORRECCIÓN IDIOMÁTICA

S.P. Juan Carlos Tobar
Corrector Idiomático del Instituto Geográfico Militar

IMPRESIÓN

Instituto Geográfico Militar

Diciembre 2025

PERSONAL TÉCNICO DE MESAS DE TRABAJO

Eje de acción legal:
Cpfg. Armijos Ramírez Álvaro Segundo*
Cpcb. Almeida Zambrano Carol Alexandra
Mayo. Vélez Andrade Hugo José*
Mayo. Legarda Valverde Oscar Javier*
Capt. Abarca Jaramillo Karla Elizabeth

Eje de acción institucional:
Crnl. Lupera Morillo Bolívar Roberto
Cpfg. Tapia Chichande Alex Paúl
Tcrn. Ramos Vargas José Gabriel
Cpcb. Reyes Chicango Rolando Patricio
Mayo. Ubilluz Zambrano Christian Marcelo

Eje de acción infraestructuras críticas:
Cpfg. Guamán Seis Joseph Alexander
Tcrn. Portilla Espinosa Luis Alfredo
Tcrn. Vizcaíno Villavicencio Christian*
Mayo. Rosero Romero Cyntia Ibeth
Mayo. Buenaño Pesántez Gabriel Alejandro

Eje de acción cooperación nacional e internacional:
Cpfg. Sánchez Villacís Carmita Lorena
Tcrn. Fierro Román Rommel Alexander
Tcrn. Santacruz González William Patricio*
Mayo. Escobar Bonilla Guillermo Santiago

Eje de seguridad de la información:
Tcrn. Ocampo Andrade Ítalo Bayardo*
Cpfg. Villalba Novoa Patricio Vicente
Mayo. Araujo Andrade Marcelo Eduardo
Tnnv. Ordóñez Mancheno Giovanni Mauricio
Tnnv. Espinosa Daquilema Eddy Roberto

Eje de capacidades estratégicas:
Cpnv. Uquillas Soto Ricardo Pio
Crnl. Chiza López Diego Fernando
Crnl. Montenegro Puga Jairo Ernesto*
Tcrn. Acosta Sánchez Bolívar Vinicio
Mayo. (S.P) Recalde Herrera Luis Lenin*

* Expertos que también formaron parte del grupo focal del tanque de pensamiento.

MINISTERIO DE DEFENSA NACIONAL

CONTENIDO

Presentación

ESTRATEGIA DE CIBERDEFENSA 2026

Presentación

Presentación

CIBERDEFENSA: EL CAMINO HACIA UNA DEFENSA INTEGRAL DEL ECUADOR

Vivimos un tiempo donde la guerra y la soberanía no solo se libran en la tierra, el mar o el aire, sino también en un territorio invisible y decisivo: el ciberespacio. Allí, donde la información se transforma en poder y los datos en instrumentos de control, se trazan las nuevas fronteras de la defensa y la libertad. En este nuevo escenario, la fortaleza de un país no se mide por el tamaño de su armamento, sino por la solidez de sus redes, la integridad de sus sistemas y la capacidad de proteger lo esencial: la estabilidad, la confianza y la unidad de la nación.

Por la paz y el bienestar de nuestras familias ecuatorianas, fortalecer nuestras capacidades en el ciberespacio es también proteger la soberanía del país. La protección digital de los ecuatorianos forma parte de esa misma misión nacional, porque detrás de cada sistema seguro hay una familia que trabaja, que estudia y que confía en que el Estado sabrá cuidarla también en el mundo digital. En este contexto, el Ministerio de Defensa Nacional del Ecuador presenta la Estrategia de Ciberdefensa, un instrumento que marca un nuevo paso en la evolución de nuestra Defensa Nacional.

Esta Estrategia nace para responder a los desafíos de un mundo interconectado, donde la innovación y la tecnología avanzan con rapidez, y solo los países que

se preparan con visión pueden transformar el riesgo en oportunidad. Su propósito es claro: proteger el ciberespacio ecuatoriano como un bien estratégico de la Nación, porque en él también se juega el destino de nuestra soberanía. Ecuador reconoce al ciberespacio como el quinto dominio de acción militar, junto con la tierra, el mar, el aire y el espacio. Por ello, fortalece su estructura de ciberdefensa en coherencia con la Política Nacional de Ciberseguridad y con los intereses superiores del Estado. La Estrategia de Ciberdefensa define los principios, objetivos y líneas de acción que orientarán el fortalecimiento de nuestras capacidades técnicas, humanas y doctrinarias. Promueve un modelo flexible, sostenible y moderno, que permita a nuestras Fuerzas Armadas actuar con autonomía y coordinación frente a las nuevas amenazas, trabajando junto a otras instituciones nacionales y socios internacionales. Porque la defensa del ciberespacio no es solo una tarea militar: es una causa de Estado, una responsabilidad compartida y una expresión de soberanía.

Nuestras Fuerzas Armadas Ecuatorianas asumen este desafío con disciplina, entrega y sentido de patria. Hoy, defender al Ecuador también significa proteger su espacio digital. Fortalecer nuestras capacidades en el ciberespacio es resguardar la vida, la tranquilidad y el futuro de nuestras familias. Porque en cada acción que fortalece nuestra defensa digital, se preservan la paz, la soberanía y el bienestar de todos.

Introducción

Introducción

La defensa nacional se ha estructurado históricamente sobre los dominios tradicionales de tierra, mar y aire, incorporando posteriormente el espacio exterior. En la actualidad, el ciberespacio se reconoce como el quinto dominio, caracterizado por su naturaleza estratégica, intangible y global, en el que las amenazas se desarrollan con creciente complejidad y alta velocidad de evolución.

En este contexto, la seguridad nacional adquiere una dimensión integral y multidominio en donde el ciberespacio representa, un campo digital de oportunidades para el desarrollo económico, social, y un entorno de riesgo donde la protección de la infraestructura crítica digital, los servicios esenciales y los datos del Estado constituyen una prioridad estratégica.

La ciberdefensa se establece como un componente fundamental de la ciberseguridad, mediante el cual el Estado fortalece sus capacidades para garantizar la soberanía digital, la integridad institucional y la seguridad de la ciudadanía frente a amenazas y agresiones que se manifiestan en el entorno digital. Este principio se enmarca en el Pilar de Soberanía y Defensa de la Política Nacional de Ciberseguridad (2021), que reconoce al ciberespacio como un dominio operativo en el cual el sector Defensa asume un rol decisivo en la protección de los intereses nacionales.

La Estrategia de Ciberdefensa se fundamenta en la misión constitucional de la Defensa Nacional, y define los objetivos y líneas de acción para fortalecer las capacidades militares orientadas a la prevención, detección y respuesta ante incidentes en el ciberespacio; asimismo, establece parámetros de actuación para las entidades competentes, regidos por los principios de soberanía, integridad y resiliencia y destaca la cooperación interinstitucional e internacional como elemento central para promover la coordinación efectiva, el intercambio ágil de información y la adopción de mecanismos de confianza y seguridad compartida entre Estados.

La acelerada evolución tecnológica, impulsada por avances en inteligencia artificial, el Internet de las Cosas (IoT) y la computación cuántica, exige la adopción de instrumentos flexibles y sujetos a permanente actualización.

En consecuencia, la Estrategia de Ciberdefensa se concibe como una herramienta normativa que orienta al sector Defensa en el ámbito del ciberespacio, fortaleciendo su posición frente a las amenazas emergentes y contribuyendo significativamente a la protección del entorno digital.

Capítulo 1

ESTRATEGIA DE CIBERDEFENSA 2026


SCAN COMPLETE
PASSWO
1234
567
89
10
HACKIN
01010101110
01010101110

Capítulo 1

1. Antecedentes

La Estrategia de Ciberdefensa se formula a partir de un análisis metodológico que considera, en primer lugar, los resultados alcanzados durante la vigencia de la Estrategia 2021, la cual constituyó un hito al marcar el inicio de la creación del sistema de ciberdefensa en las Fuerzas Armadas ecuatorianas. Este proceso inicial permitió sentar las bases institucionales, normativas y operativas necesarias para fortalecer la capacidad del Estado en la protección del ciberespacio.

Además, se enmarca en la normativa nacional relacionada con la seguridad de la información, ciberseguridad y ciberdefensa; y, en los lineamientos del Plan Nacional de Desarrollo. De esta forma, el país reafirma su compromiso con la mejora continua del entorno de confianza y seguridad en el ciberespacio, en coherencia con la normativa vigente y los estándares internacionales en materia de ciberdefensa y buenas prácticas globales.

La articulación con los diversos instrumentos de política pública y planificación nacional, aseguran la coordinación de esfuerzos institucionales hacia un objetivo común y primordial: el fortalecimiento de la seguridad digital nacional, como componente esencial para el desarrollo, la defensa y la soberanía del Estado.

Figura 1: Ecosistema de la seguridad digital

A) Marco normativo

1) Normativa Nacional

a. Constitución de la República del Ecuador (2008) Art. 3 (numerales 2 y 8), 16, 66 (numerales 19 y 21), 158, 313.

b. Código Orgánico Integral Penal (2014) Art. 190, 229-234.

c. Ley Orgánica para la Transformación Digital y Audiovisual (2023) Art. 6,17,19.

d. Ley de Seguridad Pública y del Estado (2009) Art. 10, 11, 38, 41, 42, 43.

e. Reglamento a la Ley de Seguridad Pública y del Estado (2024) Art. 66-67, 71,73.

f. Decreto Ejecutivo N.º 647 (2019) y sus reformas respectivas: Decreto Ejecutivo No. 157 (2021), Decreto Ejecutivo No. 514 (2022) y Decreto Ejecutivo No. 657 (2023).

g. Acuerdo Ministerial N.º 199 (2021).

h. Acuerdo Ministerial N.º MINTEL-MINTEL-2024-0003 (2024).

i. Plan Nacional de Desarrollo (2025-2029).

j. Política de Defensa Nacional (2019), expedida mediante Decreto Ejecutivo No. 633 del 08 de enero de 2019.

k. Política Pública de Telecomunicaciones (2023).

l. Plan Nacional de Seguridad Integral 2025-2029.

m. Plan Estratégico de las Fuerzas Armadas (2021 – 2033).

n. Plan Sectorial de la Defensa (2025- 2029).

o. Política de Ciberdefensa para el sector Defensa (2021).

p. Estrategia de Ciberdefensa (2021).

q. Normas técnicas ecuatorianas para la gestión de seguridad de la información (NTE INEN-ISO/IEC27000).

2) Lineamientos Internacionales

a. Carta de las Naciones Unidas.

b. Convenios de Ginebra y sus protocolos adicionales.

c. Declaración sobre Seguridad en las Américas de la Organización de Estados Americanos (OEA) México, 2003.

d. Estrategia de Seguridad Cibernética

e. Resolución AG/RES 2004 (XXXIV-O/ 04) de la Organización de Estados Americanos (OEA).

f. Decisión 587 de la Comunidad Andina, 10 de julio de 2004.

g. Principios y normas generales: Resoluciones UNGA 55/63 y 56/121 sobre la lucha contra el uso de la tecnología de la información con fines delictivos. Resoluciones UNGA 57/239, 58/199 y 64/211 sobre la creación de una cultura mundial de seguridad cibernética y la protección de infraestructuras críticas de la información.

h. Resolución UNGA 73/266 sobre Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional.

i. Declaración para la protección de infraestructura crítica ante las amenazas emergentes.

j. Comité Interamericano contra el Terrorismo (CICTE) de la OEA (20 de marzo de 2015).

k. Resolución CICTE/RES. 1/19 del 24 de mayo de 2019 sobre Medidas Regionales de Fomento y Confianza en el Ciberespacio (MFCS).

l. ISO/IEC 27005, Guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones.

m. ISO/IEC 27032, Gestión de Ciberseguridad.

n. LAC4, Centro de Cibercapacidades de Latinoamérica y el Caribe, para el fortalecimiento de las capacidades nacionales de ciberseguridad mediante cooperación internacional de la Unión Europea CyberNet.

B) Integración de la Ciberdefensa con el Sistema Nacional de Planificación

La Estrategia de Ciberdefensa se construye tomando como referencia los principales instrumentos de planificación nacional vigentes, en materia de seguridad y defensa.

La Política de Defensa Nacional (2019), establece de manera explícita la necesidad de contar con una estrategia específica de ciberdefensa, reconociendo que tanto las amenazas cibernéticas, como los ataques dirigidos a la infraestructura crítica digital, pueden comprometer directamente la seguridad del Estado. En este sentido, identifica al ciberterrorismo, el ciberespionaje y las infiltraciones a sistemas informáticos como formas modernas de agresión que requieren una respuesta organizada y tecnológica. De igual manera, plantea el impulso de la industria de defensa basada en Investigación, Desarrollo e Innovación (I+D+I), con el propósito de generar productos y servicios estratégicos especializados

que fortalezcan las capacidades nacionales en el ámbito de la ciberdefensa.

El Plan Nacional de Seguridad Integral (2025-2029), brinda al Estado una visión amplia de los retos de seguridad, reconociendo la naturaleza dinámica del sistema internacional y sus efectos sobre la sociedad y los individuos. Este instrumento subraya la aparición de nuevas amenazas en distintos niveles, destacando a los ciberataques como un riesgo particular, dado su carácter transversal y su capacidad de afectar simultáneamente múltiples sectores mediante el uso de la tecnología.

La Política Nacional de Ciberseguridad (2021), liderada por el Ministerio de Telecomunicaciones (MINTEL) y desarrollada de manera colaborativa con los diversos sectores vinculados a la ciberseguridad, establece los pilares, objetivos y líneas de acción necesarios para fortalecer las capacidades nacionales en la materia.

El propósito es garantizar el ejercicio de los derechos y libertades de la población, así como la protección de los bienes jurídicos del Estado en el ciberespacio, promoviendo un entorno de confianza digital que abarca todos los sectores e industrias.

El Plan Estratégico de las Fuerzas Armadas (2021), establece que el sistema de ciberdefensa de las Fuerzas Armadas (FF.AA.) se ha consolidado como ente rector en la protección del ciberespacio, mostrando avances estructurales y tecnológicos que han elevado la seguridad en operaciones militares.

Sin embargo, el entorno dinámico y la presencia de amenazas avanzadas requieren reforzar sus capacidades mediante la investigación, desarrollo y aplicación de herramientas de prevención y alerta ante incidentes cibernéticos. El objetivo estratégico 5

de este Plan, establece que es indispensable disponer un comando de ciberdefensa moderno para vigilar y controlar el ciberespacio.

Las estrategias incluyen la modernización continua del comando, la protección de la infraestructura crítica digital estatal bajo responsabilidad de las FF.AA, el fortalecimiento de la cultura de ciberseguridad y ciberdefensa para garantizar la seguridad de la información institucional, y la activa participación en iniciativas nacionales e internacionales vinculadas al ciberespacio y la defensa digital. El sistema busca garantizar la preparación, adaptación permanente y liderazgo en defensa digital, respondiendo de manera efectiva a los retos actuales del ciberespacio. Así, se fortalece la protección estatal y el avance tecnológico institucional, promoviendo altos estándares de seguridad y la coordinación nacional e internacional sólida en materia de ciberdefensa.

El Plan Sectorial de la Defensa (2021), indica en el objetivo sectorial 1, que se debe mantener la protección de la infraestructura crítica, recursos y áreas estratégicas del Estado, en donde el indicador principal es el porcentaje de infraestructura crítica y áreas estratégicas protegidas, además señala que debe existir accesibilidad de la población a los servicios críticos y que estos deben ser protegidos por FF.AA, para evitar interrupciones por un ataque.

Se asegura que el contacto ciudadano y servicios esenciales bajo resguardo de las Fuerzas Armadas no se vean interrumpidos por ataques.

El enfoque está en la continuidad operacional frente a las amenazas.

La Estrategia Nacional de Ciberseguridad (2022), reconoce a la ciberdefensa como uno de sus pilares fundamentales, en donde el objetivo principal consiste en incrementar y fortalecer las capacidades de ciberdefensa del Estado ecuatoriano, con el fin de alcanzar la actitud estratégica defensiva establecida en la Política de Defensa Nacional. Esto permitirá garantizar la protección de la infraestructura crítica digital (ICD) y los servicios esenciales en el ciberespacio. En este contexto, la presente Estrategia se construye dentro del ámbito de la ciberseguridad, asignando a la ciberdefensa un rol esencial: proteger la infraestructura crítica y responder ante incidentes y amenazas en el ciberespacio.

La Ley Orgánica de Transfor-mación Digital y Audiovisual (2023), en el artículo 19, establece la gestión del marco de seguridad digital del Estado, con un enfoque en el sector Defensa. En este contexto, el Ministerio de Defensa

Nacional, en el ámbito de sus funciones y competencias, dirige, supervisa y evalúa las normas en materia de ciberdefensa.

La Política Pública de Telecomunicaciones (2023), recomienda generar un marco normativo que permita impulsar la inclusión digital, la ciberseguridad ciudadana, el acceso a la educación y cultura, a los servicios digitales en condiciones de confianza y seguridad, a la información pública y abierta, y a los servicios financieros para el acceso universal y accesibilidad a los contenidos y productos digitales, así como impulsar la participación ciudadana a través de herramientas y medios digitales.

El Plan Nacional de Desarrollo (2025) a través de la Política 8.3, establece que el Estado debe promover la transformación digital y un modelo de gobierno abierto, asegurando la protección de la información y un entorno digital confiable y seguro en todos los niveles. Las estrategias asociadas buscan mitigar amenazas cibernéticas, proteger la infraestructura digital crítica y fomentar la implementación de sistemas de seguridad de la información en el sector público. Se destaca la importancia de fortalecer la ciberseguridad y garantizar servicios digitales confiables. Además, se promueve la gestión pública eficiente, transparente e inclusiva.

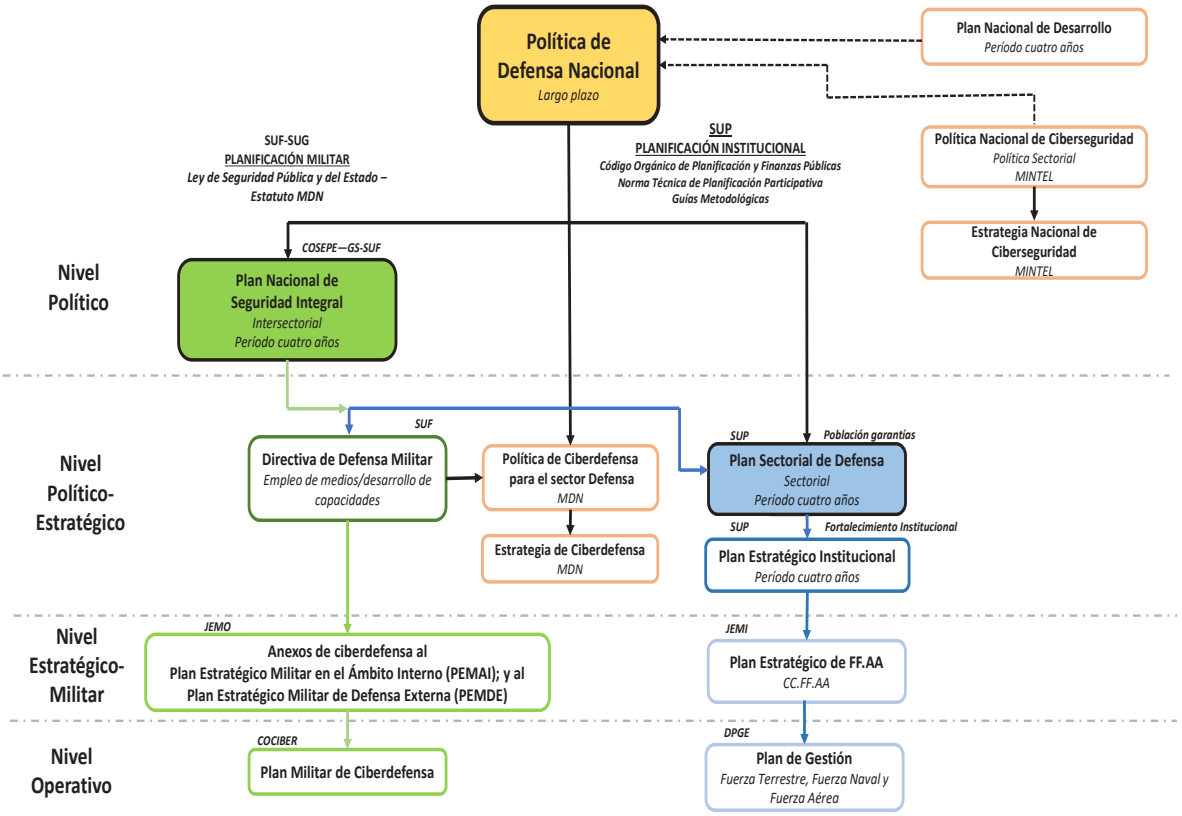


Figura 2: Articulación de la ciberdefensa en el marco de la planificación nacional.
Elaborado por: Subsecretaría de Defensa Nacional

Capítulo 2

ESTRATEGIA DE CIBERDEFENSA 2026

Capítulo 2

2. Justificación

En la sociedad actual, las naciones modernas desarrollan una amplia gama de actividades económicas, productivas y sociales en el ciberespacio. Este entorno virtual, que es transversal a todos los ámbitos, no solo impulsa la innovación y el desarrollo, sino también contribuye al bienestar de los países.

En este contexto, se vuelve imprescindible construir una estrategia sólida, robusta y coherente que permita implementar un sistema de ciberdefensa, articulado con los demás dominios tradicionales de la Defensa Nacional.

Según Barria Huidobro (2024), el rápido avance tecnológico ha convertido el ciberespacio en un lugar propicio para la explotación de vulnerabilidades. Esto puede tener consecuencias estratégicas graves como la afectación de la estructura, la estabilidad, las instituciones y la gobernabilidad del Estado. Incluso, puede llegar a perturbar la paz global y la soberanía nacional (pág. 12).

De acuerdo al Plan Estratégico Institucional de Defensa (2024), el Estado tiene el deber de defender la soberanía nacional, proteger a la sociedad de cualquier tipo de amenaza y gestionar de forma efectiva el ciberespacio para asegurar la paz y el desarrollo.

La seguridad de la información, la ciberseguridad y la ciberdefensa son componentes esenciales de la seguridad integral en el ámbito digital. En Ecuador, tanto la

ciberseguridad a nivel nacional como la ciberdefensa en el sector Defensa han experimentado avances significativos; esto se debe en gran medida, al rápido surgimiento de ciberamenazas cada vez más sofisticadas, con la capacidad de afectar la infraestructura crítica digital e interrumpir la provisión de servicios esenciales para la ciudadanía.

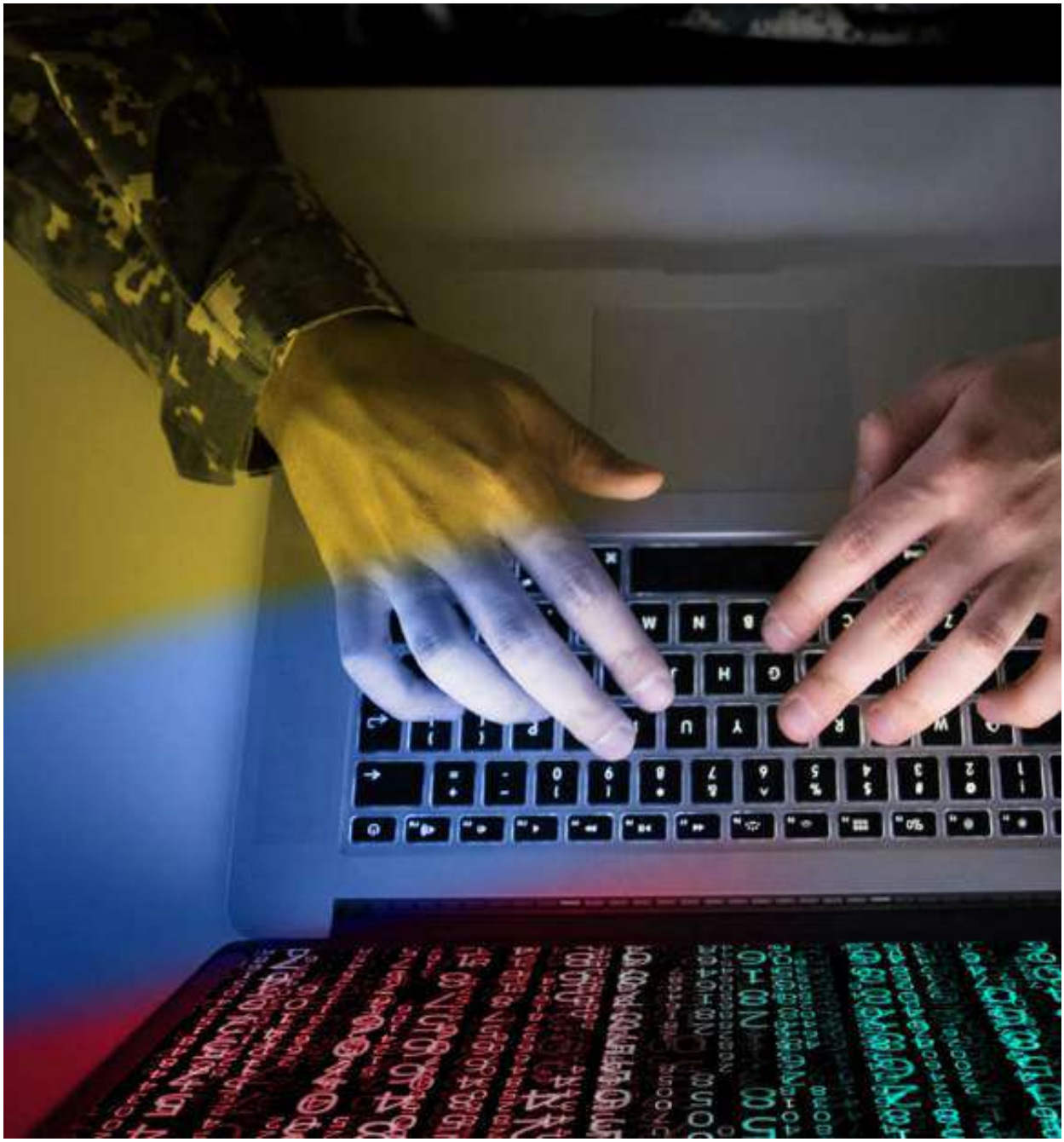
Reconociendo la importancia crítica de la ciberdefensa, en 2014 se creó el Comando de Ciberdefensa (COCIBER) como una unidad esencial dentro del Comando Conjunto de las Fuerzas Armadas (CC.FF.AA.). Esta decisión representó un hito en el fortalecimiento de las capacidades nacionales para enfrentar los desafíos del ciberespacio (Ministerio de Defensa Nacional, 2021).

El Ministerio de Defensa Nacional, como ente rector en materia de defensa, tiene entre sus objetivos prioritarios el fortalecimiento de las capacidades estratégicas conjuntas de las Fuerzas Armadas. Asimismo, procura garantizar que el COCIBER pueda responder a las ciberamenazas de cualquier naturaleza, dentro del marco de sus competencias.

En este contexto, la Estrategia de Ciberdefensa se sustenta en la Política de Defensa Nacional (2018) y el Plan Estratégico Institucional de Defensa (2024), los cuales están orientados al control efectivo del territorio nacional, al desarrollo de políticas y estrategias para la ciberseguridad, ciberdefensa y defensa aeroespacial, para afrontar las amenazas y riesgos que atenten a la paz y seguridad.

Capítulo 3

ESTRATEGIA DE CIBERDEFENSA 2026



Capítulo 3

3. Alcance de la Estrategia

3.1. Propósito

El propósito de esta Estrategia es definir las directrices para potenciar la capacidad de ciberdefensa y permitir a las Fuerzas Armadas cumplir su misión constitucional y llevar a cabo operaciones efectivas de defensa, exploración y respuesta ante ciberataques, además de garantizar la sólida protección de la infraestructura crítica digital de las Fuerzas Armadas y contribuir a la defensa de la infraestructura crítica digital del Estado.

La presente estrategia, busca fortalecer la cooperación interinstitucional y la coordinación con organismos nacionales e internacionales, elevando los estándares de preparación y resiliencia frente a amenazas emergentes. Pretende promover el desarrollo continuo de capacidades tecnológicas y talento humano especializado en ciberdefensa, asegurando una respuesta dinámica y efectiva ante riesgos cambiantes.

Finalmente, establece mecanismos para la supervisión y evaluación permanente de la Estrategia, permitiendo su actualización y mejora conforme evolucionan los desafíos en el entorno digital.

3.2. Principios rectores

Estos principios guían de manera transversal la Estrategia de Ciberdefensa y constituyen la base fundamental de todas las acciones de las Fuerzas Armadas en este ámbito.

a. **Prevención:** Es crucial desarrollar y fortalecer la capacidad de anticipar y manejar escenarios de incertidumbre para robustecer la ciberdefensa. La prevención se basa en la implementación de medidas de seguridad que rechacen ciberataques conocidos y desconocidos o que los hagan improductivos y en la capacidad de explotación que proporcione información precisa y oportuna de las Técnicas, Tácticas y Procedimiento (TTPs) de potenciales adversarios con la finalidad de anticiparse (Junta Interamericana de Defensa, 2020).

b. **Resiliencia:** El Estado ecuatoriano busca fortalecer su capacidad de resistencia y recuperación ante graves afectaciones en y a traves del ciberespacio. Dado que en este nuevo dominio algunas amenazas no pueden preverse y que reducir los riesgos es económicamente inviable. La resiliencia es fundamental para prever, soportar, recuperarse y adaptarse frente a incidentes cibernéticos adversos. A diferencia de los métodos de seguridad convencionales centrados exclusivamente en la prevención, este enfoque, parte del reconocimiento de que las brechas son inevitables. Integra de manera conjunta a las personas, los procesos y la tecnología, con el objetivo de establecer una estrategia de defensa que reduzca los impactos y asegure la continuidad de las operaciones.

   Su alcance trasciende los aspectos técnicos, ya que también comprende la gobernanza, la gestión de riesgos y la promoción de una cultura de seguridad en todos los niveles institucionales (Fortinet, 2025).

   Por su parte, las Fuerza Armadas deberán contar con la capacidad de probar la resiliencia de la infraestructura crítica digital del Estado en entornos de simulación. Esto permitirá establecer criterios razonables que confirmen la habilidad para mantener la continuidad en las operaciones de forma efectiva, incluso bajo ataque.

c. **Cooperación:** La ciberdefensa constituye una capacidad estratégica propia de las Fuerzas Armadas,

que se integra con la ciberseguridad y la protección de la información, y cuya ejecución requiere la participación conjunta de todos los actores nacionales; además, ambas demandan un esfuerzo colaborativo, cuyo logro depende de la cooperación intersectorial y del trabajo coordinado de diversas entidades.

La Agenda Global de la UIT y marcos internacionales coinciden en que la cooperación es uno de los pilares estratégicos de la ciberseguridad y la ciberdefensa, resaltando la importancia de redes de intercambio de información, ejercicios conjuntos y marcos legales comunes para enfrentar amenazas globales (United Nations Office on Drugs and Crime, 2021).

d. **Optimización de recursos:** Ante el constante advenimiento de nuevas amenazas en el ciberespacio, el Estado ecuatoriano debe prevenir y evitar la duplicación innecesaria de esfuerzos considerando las funciones, atribuciones y capacidades existentes, especialmente a escala nacional. La optimización de recursos en ciberdefensa consiste en aplicar un planeamiento estratégico, basado en la economía de medios y la concentración de esfuerzos, para asignar, integrar y aprovechar de manera eficiente los recursos humanos, tecnológicos y logísticos de manera flexible y eficiente, con la finalidad de cumplir la misión de protección digital ante amenazas crecientes y cambiantes en el entorno cibernético (). disponibles. Este enfoque permite maximizar el impacto operativo, reducir vulnerabilidades y fortalecer la capacidad de respuesta frente a amenazas en el entorno digital (Comando Conjunto de las Fuerzas Armadas, 2021).

e. **Educación y concientización:** La construcción de una cultura robusta de seguridad digital —basada en educación, sensibilización y promoción de buenas prácticas— es fundamental para fortalecer el sistema de ciberdefensa del Ecuador. Es indispensable reconocer que la tecnología, por sí sola, no garantiza la protección de los activos institucionales si los usuarios carecen de conocimiento y conciencia para

emplearla de manera segura. Este principio rector busca transformar a cada individuo en la primera línea de defensa, capacitándolo para identificar y mitigar riesgos cibernéticos de forma proactiva (European Union Agency for Cybersecurity, 2021).

f. **Investigación, desarrollo e innovación (I+D+i):** La permanente evolución tecnológica en el ciberespacio puede acelerar la aparición de nuevas amenazas y vectores de ataque. Por esta razón se requiere una constante vigilancia tecnológica, apalancada en sistemas robustos de investigación, desarrollo e innovación.

   El objetivo del I+D+i en ciberdefensa es disponer de una capacidad defensiva avanzada que permita establecer de manera eficaz en cuanto a su coste las medidas de prevención, disuasión, protección y reacción necesarias para alcanzar el estado de ciberseguridad deseado (Hinarejos Rojo & De la Peña Muñoz, 2023).

Capítulo 4

ESTRATEGIA DE CIBERDEFENSA 2026

Capítulo 4

4. Evolución y tendencia de la ciberdefensa

4.1. Concepción estratégica de la ciberdefensa

La ciberdefensa ha experimentado una importante evolución en los últimos años, impulsada por la creciente complejidad y el dinamismo del ciberespacio y las amenazas que en él se manifiestan. Esta evolución ha dado lugar a nuevos paradigmas en las estrategias de seguridad nacional (Junta Interamericana de Defensa, 2024).

La ciberdefensa en Ecuador es un componente esencial de la ciberseguridad estatal, su objetivo primordial es fortalecer la seguridad y defensa del país y salvaguardar los derechos y libertades de sus ciudadanos en el ciberespacio.

Dado que la ciberdefensa forma parte integral de la Política Nacional de Ciberseguridad, las Fuerzas Armadas, se vinculan para contribuir con diversas instituciones estatales; esta coordinación, es crucial para asegurar una respuesta rápida y completa frente a cualquier crisis que pueda surgir en el ciberespacio.

Inicialmente, la ciberseguridad se enfocaba en proteger la información y los sistemas que la almacenan, procesan y transmiten, garantizando su confidencialidad, integridad y disponibilidad. En contraste, la ciberdefensa se centra en asegurar la continuidad operativa durante la fase de funcionamiento, incluyendo la respuesta frente a acciones maliciosas. Además, abarca acciones que trascienden la defensa pasiva, incorporando la ciberinteligencia y un conjunto de medidas ofensivas, como la intrusión y la denegación de servicios (Junta Interamericana de Defensa, 2020).

Las Fuerzas Armadas comprenden que las amenazas existentes en el ciberespacio afectan a la seguridad pública y del Estado; por esta razón, esta Estrategia está vinculada con la Política de Defensa Nacional, el Plan Nacional de Desarrollo y la Política Nacional de Ciberseguridad; y, por ende, aporta al esfuerzo del Estado para mantener la soberanía del Ecuador en el ciberespacio.

El ambiente operacional del ciberespacio, donde concurren varios actores y amenazas tanto estatales como no estatales con capacidad de emplear distintos medios y recursos para afectar sistemas de mando y control, sistemas de armas y servicios esenciales, se ha convertido en un escenario clave para la competencia y confrontación de intereses políticos, económicos y militares a escala global.

La ciberdefensa, en consecuencia, trasciende el plano netamente técnico-operacional para erigirse en una capacidad estratégica esencial para defender la soberanía nacional, la estabilidad institucional y la protección de los intereses del país.

Los estados reconocen el ciberespacio como un dominio de operaciones militares, junto con tierra, mar, aire y

espacio, por lo que han creado estructuras institucionales formales de operaciones multidominio.

Los comandos conjuntos de ciberdefensa (Mando Conjunto de Ciberdefensa - MCCD en España, Comando de Defensa Cibernética - ComDCiber en Brasil, Comando de Ciberdefensa - COCIBER en Ecuador), con funciones claramente establecidas y coordinación entre estructuras civiles, militares y policiales que fortalecen su capacidad de disuasión y respuesta, integrando la ciberdefensa en la planificación y ejecución de operaciones militares conjuntas, y promoviendo la cooperación internacional para enfrentar amenazas que no conocen fronteras físicas. Por lo tanto, esta capacidad, se convierte en un instrumento clave de la política exterior y de seguridad, que permite la protección de infraestructura crítica digital, la defensa de la integridad democrática y la proyección de poder nacional en el ciberespacio.

En este contexto, la infraestructura crítica digital del sector Defensa y del Estado más los servicios esenciales que brindan, se consideran como el objetivo primordial a defender, permitiendo mantener la soberanía en el ciberespacio. Por ello, es imprescindible materializar su protección y defensa mediante la creación de un marco institucional robusto que, desde las competencias propias de Fuerzas Armadas, contribuyan eficazmente a la seguridad digital y, en consecuencia, a la seguridad integral del país.

Para cumplir esta misión en el ciberespacio, es fundamental fortalecer el desarrollo de capacidades tecnológicas avanzadas, que incluyan el despliegue de infraestructura digital segura y la implementación de sistemas de defensa cibernética.

Las tecnologías emergentes están transformando la ciberdefensa y la seguridad nacional, presentando oportunidades y desafíos complejos. La Inteligencia Artificial (IA) es crucial para la detección temprana de amenazas, la automatización de respuestas a incidentes y el análisis predictivo. Sin embargo, la misma IA puede ser usada por adversarios para lanzar ataques más sofisticados.

La expansión del Internet de las Cosas (IoT) y las redes 5G incrementan la conectividad y la velocidad, pero también ensanchan la superficie de ataque, demandando estrategias de protección más sólidas. De igual manera, la computación cuántica promete revolucionar la criptografía, aunque también introduce nuevos retos para la seguridad de la información (Herrera Guzmán, 2025).

Una preocupación creciente son los ataques ciber-físicos, que buscan comprometer infraestructuras críticas como la

energía, la salud y la banca, con el fin de maximizar el daño con el menor esfuerzo. La ciberguerra es intrínsecamente asimétrica y la dificultad para identificar a los atacantes persiste. A menudo, las herramientas defensivas son predecibles para los atacantes, y la defensa requiere de personal altamente calificado en múltiples áreas, mientras que un ataque puede ser orquestado por un grupo reducido de expertos (Cámara de Comercio Internacional (ICC), 2024).

El componente clave de la capacidad de ciberdefensa es el contar con un talento humano altamente calificado y especializado, con un alto nivel de entrenamiento y alistamiento para ejecutar las ciberoperaciones. Si bien es cierto los otros componentes: medios, infraestructura, doctrina y organización, son también importantes; es el talento humano el esencial, cuyo alistamiento demanda una importante inversión de esfuerzo y tiempo, por lo que se convierte en un recurso de larga amortización que debe ser empleado durante su carrera militar de manera óptima y eficiente.

Dada la complejidad del ciberespacio, resulta esencial establecer una articulación efectiva tanto con la industria como con la academia, promoviendo una vigilancia tecnológica constante sobre las mejores prácticas y los avances en investigación, desarrollo e innovación. Este enfoque permite incorporar los aportes de ambos sectores en materia de gobernanza, gestión de riesgos, cumplimiento, control, ciberseguridad y ciberdefensa.

La cooperación interinstitucional representa un pilar fundamental en la gobernanza de la ciberseguridad y, por extensión, en el fortalecimiento de la ciberdefensa nacional. La articulación efectiva entre los diversos actores involucrados facilita la construcción de capacidades, la respuesta coordinada ante amenazas y el desarrollo de

políticas integrales, lo que contribuye significativamente al robustecimiento de la ciberdefensa en el país. Esta labor se realiza en base a los convenios establecidos con organismos de los cuales el Ecuador es signatario; por lo tanto, es necesaria la participación en foros y mecanismos globales, regionales y nacionales, articulando esfuerzos para la lucha contra ciberamenazas y la respuesta coordinada ante ciberataques.

La ciberdefensa ha evolucionado de ser una función técnica a una prioridad estratégico-militar, que integra la ciberinteligencia, capacidades ofensivas y defensivas, y requiere una colaboración constante entre el sector público y privado, a nivel nacional e internacional, para adaptarse continuamente a las nuevas tecnologías y al panorama de amenazas en evolución.

4.2. Gobernanza de la ciberdefensa

La ciberdefensa y la ciberseguridad son parte de la seguridad digital. Ambas se interrelacionan e interactúan con el sector público y privado, con la finalidad de garantizar los derechos de las personas en el ciberespacio.

El fortalecimiento de la capacidad de ciberdefensa requiere de las alianzas estratégicas existentes y la generación de

nuevas, basadas en las necesidades institucionales. Esto, a su vez, conlleva la adhesión a organismos internacionales, y al comprometimiento en acuerdos que beneficien a todas las partes.

El Ministerio de Defensa Nacional en el marco de sus funciones y competencias emite, supervisa y evalúa las normas de la ciberdefensa en el Ecuador, con la finalidad de defender la soberanía e integridad territorial, para contrarrestar el ciberterrorismo, y fortalecer la inteligencia en el ciberespacio.

Mediante acuerdo ministerial se establece la estructura del sistema de ciberdefensa, el cual está conformado por el Ministerio de Defensa Nacional, a través de la Subsecretaría de Defensa Nacional, el Comando Conjunto de las Fuerzas Armadas, el Comando de Ciberdefensa (COCIBER), y las Unidades de Ciberdefensa de las Fuerzas Terrestre, Naval y Aérea.

4.3. Estructura militar de la ciberdefensa

I. Concepto Estratégico Militar de la Ciberdefensa

La conducción de la defensa en el ciberespacio se alinea con la actitud estratégica defensiva establecida en la Política de Defensa Nacional. Asimismo, se articula con el concepto estratégico militar establecido en dicho documento, orientado a contrarrestar las ciberamenazas que puedan comprometer la soberanía y seguridad en el ciberespacio.

Para cumplir con este cometido, se emplea al COCIBER para ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio, con el apoyo de otras instituciones nacionales y la colaboración de organismos internacionales en el ámbito de la ciberseguridad y la cooperación multilateral.

II. Organización

El Ministerio de Defensa Nacional a través de la Subsecretaría de Defensa Nacional por medio de la Gestión de Ciberdefensa y Seguridad de la Información, establece la orientación político-estratégica de la ciberdefensa. Desde este nivel de dirección, se desarrolla la emisión de directrices y lineamientos superiores en materia de seguridad de la información y ciberdefensa.

Estas atribuciones incluyen la formulación, revisión y actualización continua de políticas, reglamentos y resoluciones para la protección de la infraestructura

crítica digital, y articula estratégicamente la coordinación con los demás sectores gubernamentales y actores relevantes en el Ecuador. El Comando Conjunto de las Fuerzas Armadas planificará y conducirá estratégicamente las operaciones militares en el ciberespacio y dispondrá al COCIBER la ejecución de estas operaciones para la defensa de la infraestructura crítica digital de las Fuerzas Armadas. Además, se considera el empleo de las Unidades de Ciberdefensa para realizar operaciones de defensa y exploración en coordinación permanente con el COCIBER. Así mismo se encargarán de la formación, perfeccionamiento, especialización, adiestramiento y equipamiento en ciberdefensa.

El COCIBER y las Unidades de Ciberdefensa de cada Fuerza desarrollarán las capacidades en este campo y mantendrán el nivel óptimo de alistamiento operacional para el cumplimiento de su misión.

III. Capacidad Estratégica de Ciberdefensa

El panorama de amenazas en el ciberespacio, en constante expansión y complejidad, obliga a las Fuerzas Armadas a fortalecer de manera urgente las capacidades de ciberdefensa. Este proceso requiere la sincronización de las necesidades operativas, las misiones fundamentales y el alineamiento estratégico de todas las instituciones involucradas. Esta coordinación es imprescindible

Figura 3: Estructura de ciberdefensa de las Fuerza Armadas

debido a la criticidad de la infraestructura digital que debe protegerse. Las operaciones militares en el quinto dominio han llevado a integrar la ciberdefensa dentro de la estructura de las capacidades estratégicas conjuntas. Su inclusión en el Plan de Capacidades (2018) y el Plan de Desarrollo de Capacidades (2018), permiten alcanzar de forma planificada, los niveles de operatividad deseados para un empleo efectivo.

La capacidad de ciberdefensa se sustenta en cuatro capacidades específicas:

- Defensa: Se implementan medidas y se ejecutan acciones para proteger la infraestructura crítica digital del sector Defensa y contribuir de ser necesario a la defensa de cualquier otra infraestructura crítica del Estado y servicios esenciales que puedan ser sujetos a un ciberataque.
- Exploración: Orientada a la obtención de información vital para la planificación y conducción de ciberoperaciones. Además, contribuye al éxito de operaciones convencionales mediante el reconocimiento y análisis del entorno cibernético.
- Respuesta: Comprende la ejecución de acciones inmediatas y contundentes para contrarrestar o neutralizar un ciberataque, ya sea inminente o en curso.

4.4. Campo de acción de la ciberdefensa

El concepto de ciberespacio según la Junta Interamericana de Defensa (2020) determina que es un dominio global dinámico constituido por la interacción compleja de personas, software, servicios e infraestructuras tecnológicas conectadas a través de redes digitales. Este dominio es intangible y no posee existencia física directa, pero representa el espacio donde se desarrollan comunicaciones, operaciones y actividades que tienen impacto en la seguridad y defensa de las naciones.

Si bien es cierto que se trata de un espacio multidimensional, del cual sólo se puede captar una parte mediante un cierto esfuerzo de abstracción, la realidad del ciberespacio también es muy tangible y material, construida sobre bases de infraestructuras críticas físicas y digitales (Asma , 2022).

En este contexto la infraestructura crítica digital, es infraestructura estratégica soportada por Tecnologías de la Información y Comunicación (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Por lo tanto, la defensa de la infraestructura crítica digital requiere el monitoreo avanzado y constante de los sistemas tecnológicos, considerando interdependencias sectoriales y cuantificando el impacto de su disrupción.

Para el Ecuador, la identificación, evaluación y priorización de esta infraestructura ha sido una tarea crucial, la cual permitirá contribuir a la defensa, para la continuidad operativa y la resiliencia ante riesgos físicos y en el ciberespacio.

Mediante una metodología adecuada, el COCIBER desarrolló un procedimiento que permitió validar de manera objetiva la identificación y catalogación de la infraestructura crítica digital, generando el Catálogo de Infraestructura Crítica Digital de las Fuerzas Armadas y el Catálogo de Infraestructura Crítica Digital del Estado.

Para que una infraestructura digital sea determinada como crítica, la valoración del impacto se efectúa en cuatro aspectos: impacto poblacional, vulnerabilidades, criticidad de activos e impacto económico. Este documento debe ir anclado al diseño e implementación de planes de contingencia y protocolos de atención adecuados que permitan la acción coordinada de los sectores estratégicos, de acuerdo con sus competencias.

En el ámbito de la defensa se define a la Infraestructura Crítica Digital de la Defensa (ICDD), como aquellas infraestructuras soportadas por TIC o TO empleadas en el ámbito de la defensa para el desarrollo de operaciones militares que permiten el cumplimiento de la misión constitucional.

Capítulo 5

ESTRATEGIA DE CIBERDEFENSA 2026

Capítulo 5

5. Situación actual

5.1 Análisis global, continental, regional y nacional

La ciberdefensa se ha consolidado como un eje estratégico de la seguridad global, dada la creciente interdependencia digital, el incremento de ciberataques sofisticados y la utilización del ciberespacio como un nuevo dominio de confrontación geopolítica. El panorama actual refleja la acelerada militarización de este ámbito, donde estados, organizaciones internacionales y bloques regionales desarrollan de manera prioritaria capacidades ofensivas y defensivas para proteger su soberanía e intereses nacionales. Este escenario se caracteriza por la aparición de doctrinas específicas, la creación de mandos cibernéticos militares especializados y la integración de operaciones digitales en la estrategia de defensa tradicional (Calderón Lara, 2025). La competencia entre potencias como Estados Unidos, China y Rusia acelera esta dinámica, generando una carrera tecnológica que abarca inteligencia artificial, guerra electrónica y capacidades de negación disruptiva. Asimismo, la proliferación de actores no estatales y la mercantilización de herramientas de ciberataque amplifican las amenazas, desdibujando las líneas entre conflicto y paz.

Ámbito Global

En la Unión Europea (UE), la ciberdefensa se articula a través de la Estrategia de Ciberseguridad de la UE y se integra con la Política Común de Seguridad y Defensa (PCSD). Destacan iniciativas como el Centro de Competencia en Ciberseguridad y los proyectos de cooperación en el marco de PESCO (Cooperación Estructurada Permanente), diseñados para fortalecer las capacidades conjuntas y la resiliencia colectiva (Comisión Europea, 2025).

En la OTAN, el ciberespacio fue declarado en 2016 como un dominio operativo (junto a tierra, mar, aire y espacio). La Alianza cuenta con el Cyber Operations Centre (ubicado en el SHAPE en Bélgica) y desarrolla ejercicios regulares como Cyber Coalition, orientados a garantizar la defensa colectiva y la interoperabilidad entre los aliados. Estas capacidades se ven reforzadas por el trabajo del Centro de Excelencia en Ciberdefensa (CCDCOE).

Frente a este enfoque multilateral, el llamado bloque oriental (Rusia, China, Corea del Norte e Irán) concibe la ciberdefensa desde una perspectiva de soberanía absoluta y guerra híbrida. Sus modelos priorizan el control estatal de internet, la censura y la integración de unidades cibermilitares en sus estructuras de defensa.

China avanza hacia la "ciber-soberanía" con un enfoque ofensivo-defensivo, utilizando el espionaje para acelerar su desarrollo tecnológico. Rusia emplea capacidades cibernéticas como arma de desestabilización política y negación plausible, a menudo a través de grupos proxy. Corea del Norte e Irán utilizan operaciones cibernéticas

ofensivas para generar ingresos (ciberdelincuencia, ransomware) y proyectar poder.

Conflictos Actuales y su Dimensión Cibernética

La guerra en Ucrania ha sido un campo de pruebas sin precedentes para la guerra cibernética integrada. Rusia ha desplegado un amplio arsenal que incluye campañas de desinformación, ataques de denegación de servicio (DDoS) contra infraestructura crítica y operaciones de borrado de datos (wiper malware). Ucrania, con apoyo técnico occidental, ha demostrado una notable resiliencia, utilizando herramientas digitales para la defensa civil y la comunicación.

Israel se enfrenta a un entorno de amenazas cibernéticas persistente y sofisticado. Actores estatales y no estatales (como Hamas e Irán) ejecutan campañas de espionaje, sabotaje contra sistemas de control industrial y tácticas de influencia en redes sociales, poniendo de relieve el uso del ciberespacio como un teatro de operaciones permanente.

En Taiwán, la tensión tiene un componente cibernético crucial. China emplea campañas de espionaje a largo plazo (Amenazas Persistentes Avanzadas, APT) para robar propiedad intelectual y datos sensibles, junto a operaciones de influencia para socavar la legitimidad internacional de Taiwán, preparando el terreno operativo para una potencial escalada futura.

Ámbito Hemisférico

En el continente americano, Estados Unidos ejerce un liderazgo técnico y militar indiscutible, a través de su Estrategia Nacional de Ciberseguridad, agencias como la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) y el US Cyber Command, han definido estándares y actúan de manera proactiva frente a amenazas globales y promueven alianzas con socios estratégicos.

La Organización de los Estados Americanos (OEA) desempeña un papel articulador crucial a través del Comité Interamericano contra el Terrorismo (CICTE), que impulsa cooperación, capacitación y marcos normativos. La Comisión Interamericana de Telecomunicaciones (CITEL) complementa estos esfuerzos fortaleciendo la seguridad de la infraestructura crítica de telecomunicaciones.

Ámbito Regional

América Latina y el Caribe enfrentan un rezago significativo en capacidades de ciberdefensa, caracterizado por una alta exposición y vulnerabilidad. La región funciona a menudo como campo de pruebas y objetivo secundario para actores avanzados. Los principales desafíos son estructurales: infraestructuras críticas obsoletas, marcos legales insuficientes, dependencia tecnológica externa y una alarmante escasez de profesionales capacitados.

Pese a esto existen avances, países como: Brasil, Chile, Colombia, México y Costa Rica han desarrollado políticas nacionales, Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT) y participan activamente en ejercicios de cooperación. La OEA y el Banco Interamericano de Desarrollo (BID) proporcionan asistencia técnica crucial.

Argentina.-

En 2024, Argentina avanzó en su estrategia de ciberseguridad y ciberdefensa con la implementación de la Estrategia Nacional de Ciberseguridad 2024-2030 y la reorganización del Sistema de Inteligencia Nacional, incluyendo la

creación de la Agencia Federal de Ciberseguridad como "el órgano con competencia sobre la ciberdelincuencia, las infraestructuras críticas y objetivos de valor estratégico tecnológicos y de la información".

Brasil.-

En 2023, implementó la Política Nacional de Ciberseguridad (PNCiber), un marco integral para la protección de la infraestructura crítica del país, que incluye la cooperación entre el gobierno, la sociedad civil y expertos en el campo de la seguridad informática. El Centro Nacional de Ciberseguridad (CNCiber) coordina estas acciones, mientras que el Programa de Privacidad y Seguridad de la Información (PPSI) se enfoca en mejorar la resiliencia de las entidades públicas ante posibles ataques.

Chile.-

Ha experimentado un progreso notable en ciberseguridad, impulsado por la creación de programas educativos tanto públicos como privados, que integran formación técnica y jurídica, orientada a la especialización y actualización constante.

La Ley No 21.663, conocida como Ley Marco de Ciberseguridad, entra en vigor en 2025 con el objetivo de fortalecer las defensas digitales de Chile, proteger datos personales y establecer marcos institucionales para la respuesta a ciberataques.

Colombia.-

Este país ha dado pasos estratégicos con la inauguración del Centro de Operaciones de Seguridad Nacional (SOC) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC). El SOC, es una instalación destinada a fortalecer la protección digital de entidades gubernamentales y contribuir a la seguridad del ecosistema digital del país. Este centro está diseñado para prevenir, detectar y responder a amenazas cibernéticas en tiempo real y opera bajo la dirección del Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT).

Ecuador.-

En 2024, el país registró más de 12 millones de ciberataques, un aumento del 30% respecto al año anterior, en sectores clave como finanzas, gobierno, salud y educación siendo los más afectados. Esta situación ha impulsado un fortalecimiento de las estrategias nacionales mediante la implementación de la Estrategia Nacional de Ciberseguridad, que busca robustecer capacidades técnicas, jurídicas y de cooperación internacional. Sin embargo, persisten desafíos como la actualización constante de sistemas, la formación especializada y la construcción de una cultura digital responsable.

En este marco, el Centro de Respuesta a Incidentes Informáticos (EcuCERT) de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), juega un papel fundamental. Su misión es apoyar la prevención y resolución de incidentes de seguridad informática mediante la coordinación, capacitación y soporte técnico. Además, coordina la respuesta a incidentes y vulnerabilidades, sensibiliza sobre buenas prácticas y coopera estrechamente con otros equipos nacionales e internacionales de respuesta a incidentes (CSIRT). Este centro es clave para masificar el uso seguro de las tecnologías y fortalecer la resiliencia del país ante las ciberamenazas (El Universo, 2024).

5.2 Diagnóstico

En el año 2018, el Ministerio de Defensa Nacional plasma en la Agenda Política de Defensa que el ciberespacio es vital para la seguridad del Estado y los ciudadanos, por lo que es imperativo el desarrollo de políticas y capacidades alrededor de este aspecto.

En el año 2021 se publicó mediante acuerdo ministerial la Estrategia de Ciberdefensa, siendo el COCIBER el encargado de realizar la evaluación y seguimiento de los indicadores de gestión.

A continuación, se presenta el seguimiento de los indicadores de la Estrategia de Ciberdefensa 2021:

En cuanto al fortalecimiento de la ciberdefensa, se observa una consolidación estructural con la reforma de procesos sustantivos y la creación de direcciones y jefaturas de ciberdefensa en los niveles político-estratégico, estratégico-militar y operacional. También se han implementado unidades de ciberdefensa en las Fuerzas Terrestre, Naval y Aérea y se ha avanzado en el desarrollo de doctrina conjunta y la capacitación del talento humano a través de ejercicios y pasantías internacionales. La identificación y catalogación de la Infraestructura Crítica Digital (ICD) de la Defensa y del Estado ecuatoriano son logros significativos (Comando de Ciberdefensa, 2025).

Respecto al incremento de las capacidades de defensa activa y respuesta, se han identificado requerimientos operacionales y se ha ejecutado parcialmente el proyecto de inversión "Incrementar la Capacidad de Ciberdefensa de Fuerzas Armadas (ICCFA)". Además, se realizaron operaciones de ciberdefensa planificadas y operaciones no planificadas en diversas instituciones estatales críticas como Petroecuador, Ministerio de Economía y Finanzas y la Presidencia de la República. El incremento de la capacidad fue del 2.5% a diciembre de 2024 (Comando de Ciberdefensa, 2025).

En cuanto a la articulación interinstitucional y normativa y el fortalecimiento de la cultura de ciberseguridad, el COCIBER mantiene un canal técnico con el EcuCERT y participa en redes de confianza y foros internacionales. Ha existido una colaboración activa en propuestas de leyes de seguridad digital y modificaciones a decretos ejecutivos y leyes orgánicas. La metodología para la definición y catalogación de las infraestructuras críticas digitales (ICD) fue emitida y difundida a entidades estatales. A diciembre de 2024, se neutralizó el 47.25% de los ciberataques a la infraestructura crítica, un resultado que se ve impactado negativamente por la falta de un SOC (Comando de Ciberdefensa, 2025).

En el ámbito de la cultura de ciberseguridad, el porcentaje de personal capacitado y certificado es solo del 21% a diciembre de 2024, lo que indica una brecha considerable en el desarrollo de competencias transversales (Comando de Ciberdefensa, 2025).

Además, en este último año ha sido revisada y actualizada la planificación militar de la defensa nacional, en la que se incluye a la ciberdefensa como un ámbito de operaciones, al igual que los espacios terrestre, marítimo y aéreo.

5.3 Actores de amenazas en el ciberespacio

El panorama actual de la ciberdefensa está definido por una diversidad de actores de amenazas con diferentes motivaciones, recursos y niveles de sofisticación que incluyen desde estados hasta individuos organizados en estructuras criminales o ideológicas, lo cual representa desafíos complejos para la seguridad global. Según

el Global Threat Report (2024), el tiempo promedio de acceso no detectado (breakout time) se redujo a 62 minutos, mientras que el 75% de los ataques fueron impulsados por motivos financieros y solo el 3% de las organizaciones a nivel global cuentan con capacidades maduras de prevención. En este mismo contexto, el Informe de amenazas de ciberseguridad de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) (2024) y datos del Reporte de Ciberseguridad de Check Point Software Technologies Ltd. (2024), en promedio se registran más de 2.200 ciberataques diarios a nivel mundial y el costo global del cibercrimen alcanzaría los 10,5 billones de dólares anuales en 2025. Los ataques de ransomware crecieron un 37 % en 2023, mientras que los incidentes contra infraestructuras críticas aumentaron un 20 %, especialmente en los sectores de energía, transporte y salud.

Principales Actores de Amenazas:

1. **Estados-Nación:** Estos actores están patrocinados por gobiernos y cuentan con amplios recursos. Sus objetivos son geopolíticos y estratégicos, como el espionaje o la guerra cibernética. Sus ataques suelen ser complejos y difíciles de detectar (Junta Interamericana de Defensa, 2024)
2. **Hacktivistas:** Buscan desestabilización política o ideológica, utilizan técnicas de piratería para promover agendas políticas o sociales. Su objetivo es llamar la atención sobre una causa, avergonzar a una organización o filtrar información confidencial. Un ejemplo conocido es el colectivo Anonymous (Ortiz Correa, 2024)
3. **Ciberterrorismo:** Es la convergencia del terrorismo tradicional y el ciberespacio. Se define como el uso de medios digitales y tecnológicos para llevar a cabo actos violentos o que causan un daño grave con el propósito de generar miedo o terror generalizado en la población y, de esta forma, coaccionar a un gobierno, una sociedad o una clase dirigente para lograr un objetivo político, ideológico o religioso (Iftikhar, 2024).

Actor	Motivaciones principales	Ejemplos de actividad	Ciber-conflictos
Estados Nación	Espionaje, geopolítica, disuasión militar	Sabotaje a infraestructuras, desinformación	Rusia–Ucrania, China–Taiwán, Israel–Irán
Hacktivistas	Político-ideológicas, protesta, propaganda	DDoS, defacement, filtración de datos	Campañas pro-Rusia vs. pro-Ucrania, colectivos contra Israel y EE. UU.
Ciberterrorismo	Miedo, desestabilización, apoyo a terrorismo físico	Ataques a infraestructura crítica, propaganda	Oriente Medio (ISIS, Hamás vs. Israel)
Actores internos (Insiders)	Lucro, venganza, ideología	Filtración de secretos, sabotaje interno	Casos aislados en fuerzas armadas y gobiernos occidentales

Tabla 1: Principales actores de amenazas

4. **Actores Internos (Insiders):** Son empleados, exempleados o contratistas que tienen acceso privilegiado a los sistemas de una organización. Pueden actuar por venganza, beneficio personal o negligencia, y su acceso los convierte en un riesgo significativo. Según Verizon DBIR (2024), son los responsables del 15% de incidentes ya sea por negligencia o intencionalidad.

Técnicas y Tácticas principales de acuerdo a MITRE ATT&CK (2025):

1. **Acceso Inicial:** Phishing (35% de incidentes) y explotación de vulnerabilidades en servicios expuestos (20%).
2. **Movimiento lateral:** Uso de herramientas legítimas (Living-off-the-Land) y robo de credenciales.
3. **Exfiltración:** Transferencia encubierta de datos mediante protocolos cifrados o servicios cloud públicos.
4. **Evasión:** Ofuscación de código, ejecución en memoria y cifrado de comunicaciones.

Tipos de Ataques que afectan la ciberdefensa:

1. **Ransomware:** Afectó a 72% de organizaciones en Latinoamérica (CrowdStrike Inc., 2024).
2. **Amenazas Persistentes Avanzadas (APT):** Campañas de larga duración para robo de propiedad intelectual o inteligencia estratégica (Che Mat, Abdul Ghani, & Noor, 2024).
3. **Ataques a cadenas de suministro:** Compromiso de software legítimo para alcanzar múltiples objetivos (Check Point Software Technologies Ltd, 2024).
4. **Desinformación:** Campañas coordinadas para manipulación de la opinión pública y erosión de confianza institucional (Labrador Blanes, 2023).
5. **Ataques a Infraestructura Crítica:** El sector energético y de la salud son los más atacados 45% aumento en ICS/SCADA (Díaz, 2025).

Tendencias Críticas:

1. **IA Generativa:** Creación de phishing hiperrealista y automatización de exploits (Boonkrong, 2023).
2. **Guerra Híbrida:** Integración de ciberataques con operaciones militares convencionales (Calvo Albero, 2023).
3. **Monitoreo de Comunicaciones:** Interceptación satelital y targeting de servicios en la nube (Rivas & Tenorio, 2022).

En este contexto, la ciberdefensa moderna requiere de ciberinteligencia en tiempo real, segmentación de redes y respuestas coordinadas entre los sectores público y privado. La cooperación internacional es esencial para mitigar estas amenazas transnacionales.

Capítulo 6

ESTRATEGIA DE CIBERDEFENSA 2026

Capítulo 6

6. Objetivos estratégicos

OBJETIVO ESTRATÉGICO 1

Establecer un marco integral de gobernanza del ciberespacio para el sector Defensa, que articule normativas, capacidades institucionales y mecanismos de cooperación nacional e internacional, con el propósito de fortalecer la seguridad, coordinación y resiliencia frente a incidentes y amenazas en el ciberespacio.

LÍNEAS DE ACCIÓN				
1	2	3	4	5
Actualizar y crear normativas y resoluciones en materia relacionada al ciberespacio en el sector Defensa, con el fin de disponer de un marco jurídico dinámico, coherente con los avances tecnológicos, los estándares internacionales y las nuevas amenazas.	Actualizar un marco institucional donde se definan las competencias, atribuciones, responsabilidades y entregables del Sistema de Ciberdefensa en los niveles Político Estratégico, Estratégico Militar, Operacional y Táctico.	Suscribir instrumentos jurídicos de cooperación internacional rápida y eficaz para coadyuvar la neutralización de amenazas y mitigación de ciberataques.	Gestionar el interrelacionamiento entre los sectores: defensa, público y privado mediante la suscripción de convenios específicos, que permitan la coordinación efectiva y gestión oportuna a los incidentes de seguridad informática.	Reforzar mecanismos hemisféricos y regionales de coordinación y cooperación en el ámbito de ciberdefensa para el intercambio de información, capacitaciones, misiones, investigaciones transnacionales, operaciones y fortalecimiento de habilidades y capacidades técnicas en el ciberespacio.

OBJETIVO ESTRATÉGICO 2

Incrementar las capacidades de ciberdefensa en las Fuerzas Armadas, para la neutralización de amenazas y la mitigación oportuna de ciberataques en la ICD del sector Defensa y contribuir en la defensa de las ICD y servicios esenciales del Estado.

LÍNEAS DE ACCIÓN

1	2	3	4
Incrementar las Capacidades de Ciberdefensa que permita fortalecer la prevención, detección, respuesta y mitigación de incidentes de seguridad informática en la infraestructura crítica digital del sector Defensa.	Establecer y actualizar el marco doctrinario de operaciones en el ciberespacio, que integre todos los niveles de la planificación y conducción operativa de las Fuerzas Armadas.	Establecer un mecanismo de intercambio de productos de ciberinteligencia con indicadores de compromiso respecto a amenazas tecnológicas, con instituciones nacionales e internacionales, que garantice información oportuna para una toma de decisiones eficaz en ciberdefensa.	Desarrollar e implementar un plan de adiestramiento operacional y evaluación continua que potencie la preparación del personal militar profesional en operaciones y acciones tácticas de ciberdefensa.

OBJETIVO ESTRATÉGICO 3

Fortalecer de manera sostenible la capacitación y especialización técnica del personal de Fuerzas Armadas, mediante programas formativos y de actualización continua, con el fin de garantizar la preparación operativa y la ejecución efectiva de operaciones en el ciberespacio.

LÍNEAS DE ACCIÓN

1	2	3
Implementar un Plan Integral de Capacitación con programas estandarizados y especialización en seguridad de la información, ciberseguridad y ciberdefensa a través de convenios con la academia y aliados estratégicos internacionales.	Implementar entrenamientos prácticos y simulaciones en un entorno virtual especializado nacional, integrando ejercicios conjuntos e internacionales.	Consolidar un plan de gestión, rotación y retención de talento humano especializado en operaciones en el ciberespacio, con incentivos de carrera y convenios con la academia y sector privado acorde al art. 94 del Reglamento de la Ley Orgánica de Personal y Disciplina de las Fuerzas Armadas.

OBJETIVO ESTRATÉGICO 4

Incrementar la madurez de los Sistemas de Gestión de Seguridad de la Información (SGSI) en el sector Defensa, mediante la implementación de estándares, controles y buenas prácticas, con el fin de contribuir a la confidencialidad, integridad y disponibilidad de la información crítica digital para las Fuerzas Armadas.

LÍNEAS DE ACCIÓN

1	2	3	4
Gestión del Comité de Seguridad de la Información de FF.AA. para asegurar el proceso de mejora continua de la seguridad de la información digital de FF.AA.	Desarrollar la metodología de gestión de seguridad de la información digital para Fuerzas Armadas.	Implementación de la Gestión de Seguridad de la Información Digital en las Fuerzas Armadas, período 2026 - 2029	Fortalecer la cultura de seguridad de la información digital en FF.AA. a través de campañas de prevención y aplicación de buenas prácticas.

Capítulo 7

ESTRATEGIA DE CIBERDEFENSA 2026

Capítulo 7

OBJETIVO ESTRATÉGICO 1

Establecer un marco integral de gobernanza del ciberespacio para el sector Defensa, que articule normativas, capacidades institucionales y mecanismos de cooperación nacional e internacional, con el propósito de fortalecer la seguridad, coordinación y resiliencia frente a incidentes y amenazas en el ciberespacio.

Línea de acción 1

Actualizar y crear normativas y resoluciones en materia relacionada al ciberespacio en el sector Defensa, con el fin de disponer de un marco jurídico dinámico, coherente con los avances tecnológicos, los estándares internacionales y las nuevas amenazas.

Indicador	Porcentaje de normativas y resoluciones actualizadas y creadas.
Meta	Alcanzar el 100% respecto a la actualización y creación de normativas y resoluciones en materia de ciberespacio en las Fuerzas Armadas al II semestre del año 2029.
Periodicidad	Anual
Criterio de Cálculo	((Número de documentos actualizados y creados) / (Número total de documentos requeridos)) x 100
Responsables	Gestión de Ciberdefensa y Seguridad de la Información MDN. Jefatura de Estado Mayor Institucional CC.FF.AA. Comando de Ciberdefensa. Direcciones de Operaciones de cada Fuerza.

OBJETIVO ESTRATÉGICO 1

Establecer un marco integral de gobernanza del ciberespacio para el sector Defensa, que articule normativas, capacidades institucionales y mecanismos de cooperación nacional e internacional, con el propósito de fortalecer la seguridad, coordinación y resiliencia frente a incidentes y amenazas en el ciberespacio.

Línea de acción 2

Actualizar un marco institucional donde se definan las competencias, atribuciones, responsabilidades y entregables del Sistema de Ciberdefensa en los niveles Político Estratégico, Estratégico Militar, Operacional y Táctico.

Indicador	Porcentaje de actualización del marco institucional de ciberdefensa.
Meta	Contar con el 100% del marco institucional definido, aprobado y en ejecución al 2do semestre del año 2028.
Periodicidad	Anual
Criterio de Cálculo	((Número de elementos actualizados en el marco institucional) / (Número total de elementos requeridos en el marco institucional)) x 100
Responsables	Gestión de Ciberdefensa y Seguridad de la Información MDN. Jefatura de Estado Mayor Institucional CC.FF.AA Direcciones de Operaciones de cada Fuerza.

OBJETIVO ESTRATÉGICO 1

Establecer un marco integral de gobernanza del ciberespacio para el sector Defensa, que articule normativas, capacidades institucionales y mecanismos de cooperación nacional e internacional, con el propósito de fortalecer la seguridad, coordinación y resiliencia frente a incidentes y amenazas en el ciberespacio.

Línea de acción 3

Coordinar la suscripción de instrumentos jurídicos de cooperación internacional rápida y eficaz para coadyuvar la neutralización de amenazas y mitigación de ciberataques.

Indicador	Número de instrumentos jurídicos de cooperación internacional en Ciberdefensa suscritos.
Meta	Coordinar la suscripción de al menos 02 (DOS) instrumentos jurídicos internacionales de cooperación en ciberseguridad/ciberdefensa hasta el año 2029.
Periodicidad	Cuatrienal
Criterio de Cálculo	Número de instrumentos jurídicos de cooperación internacional en ciberseguridad / ciberdefensa suscritos.
Responsables	Gestión de Ciberdefensa y Seguridad de la Información MDN. Dirección de Relaciones Internacionales del MDN. Coordinación General de Asesoría Jurídica del MDN.

OBJETIVO ESTRATÉGICO 1

Establecer un marco integral de gobernanza del ciberespacio para el sector Defensa, que articule normativas, capacidades institucionales y mecanismos de cooperación nacional e internacional, con el propósito de fortalecer la seguridad, coordinación y resiliencia frente a incidentes y amenazas en el ciberespacio.

Línea de acción 4

Gestionar el interrelacionamiento entre los sectores: defensa, público y privado mediante la coordinación de la suscripción de convenios específicos, que permitan la coordinación efectiva y gestión oportuna a los incidentes de seguridad informática.

Indicador	Número de convenios interinstitucionales suscritos para coordinación y gestión de incidentes de seguridad informática.
Meta	Coordinar la suscripción de 03 (TRES) convenios para el año 2029.
Periodicidad	Cuatrienal
Criterio de Cálculo	Número de convenios suscritos para coordinación y gestión de incidentes de seguridad informática.
Responsables	Gestión de Ciberdefensa y Seguridad de la Información MDN. Coordinación General de Asesoría Jurídica del MDN.

OBJETIVO ESTRATÉGICO 1

Establecer un marco integral de gobernanza del ciberespacio para el sector Defensa, que articule normativas, capacidades institucionales y mecanismos de cooperación nacional e internacional, con el propósito de fortalecer la seguridad, coordinación y resiliencia frente a incidentes y amenazas en el ciberespacio.

Línea de acción 5

Reforzar mecanismos hemisféricos y regionales de coordinación y cooperación en el ámbito de ciberdefensa para el intercambio de información, capacitación, misiones, investigaciones transnacionales, operaciones y fortalecimiento de habilidades y capacidades técnicas en el ciberespacio.

Indicador	Número de participación en ejercicios, foros, capacitaciones e iniciativas hemisféricas y regionales de ciberdefensa.
Meta	Participar activamente en al menos 01 (UN) mecanismo hemisférico o regional de coordinación y cooperación en el ámbito de ciberdefensa por año, a partir de 2026.
Periodicidad	Anual
Criterio de Cálculo	Cantidad de mecanismos hemisféricos y regionales en los que se ha participado durante el año.
Responsables	Gestión de Ciberdefensa y Seguridad de la Información MDN. Dirección de Relaciones Internacionales del MDN. Coordinación General de Asesoría Jurídica del MDN.

OBJETIVO ESTRATÉGICO 2

Incrementar las capacidades de ciberdefensa en las Fuerzas Armadas, para la neutralización de amenazas y la mitigación oportuna de ciberataques en la ICD del sector Defensa y contribuir en la defensa de las ICD y servicios esenciales del Estado.

Línea de acción 1

Incrementar las Capacidades de Ciberdefensa que permita fortalecer la prevención, detección, respuesta y mitigación de incidentes de seguridad informática en la infraestructura crítica digital del sector Defensa.

Indicador	Incremento en puntos porcentuales de las capacidades de ciberdefensa.
Meta	Incremento de 30 puntos porcentuales de las capacidades de ciberdefensa para el año 2029.
Periodicidad	Cuatrienal
Criterio de Cálculo	Porcentaje de Capacidades de Ciberdefensa= ((0,70*Capacidades del Comando Conjunto de $FFAA_{t+4}$) + (0,10 * Capacidades de Ciberdefensa de la Fuerza $Terrestre_{t+4}$) + (0,10*Capacidades de Ciberdefensa de la Fuerza $Naval_{t+4}$) + (0,10* Capacidades de Ciberdefensa de la Fuerza $Aérea_{t+4}$)%) - ((0,70*Capacidades del Comando Conjunto de $FFAA_t$) + (0,10 * Capacidades de Ciberdefensa de la Fuerza $Terrestre_t$) + (0,10*Capacidades de Ciberdefensa de la Fuerza $Naval_t$) + (0,10* Capacidades de Ciberdefensa de la Fuerza $Aérea_t$)%)
Responsables	Comando de Ciberdefensa. Dirección General de Operaciones Multidominio de FF.AA. Unidades de Ciberdefensa de las FF.AA.

* t= Línea base de capacidades de Ciberdefensa (2025)
* t+1= Capacidades de Ciberdefensa (2026)
* t+2= Capacidades de Ciberdefensa (2027)
* t+3= Capacidades de Ciberdefensa (2028)
* t+4= Capacidades de Ciberdefensa (2029)

OBJETIVO ESTRATÉGICO 2

Incrementar las capacidades de ciberdefensa en las Fuerzas Armadas, para la neutralización de amenazas y la mitigación oportuna de ciberataques en la ICD del sector Defensa y contribuir en la defensa de las ICD y servicios esenciales del Estado.

Línea de acción 2

Establecer y actualizar el marco doctrinario de operaciones en el ciberespacio, que integre todos los niveles de la planificación y conducción operativa de las Fuerzas Armadas.

Indicador	Porcentaje de avance en la elaboración y actualización del marco doctrinario de operaciones en el ciberespacio.
Meta	Elaborar y actualizar el 100% de la doctrina hasta el año 2029.
Periodicidad	Cuatrienal
Criterio de Cálculo	((Número de instrumentos doctrinarios elaborados y actualizados) / (Número de instrumentos doctrinarios vigentes)) × 100
Responsables	Comando de Ciberdefensa. Dirección General de Operaciones Multidominio de FF.AA. Unidades de Ciberdefensa de las FF.AA.

OBJETIVO ESTRATÉGICO 2

Incrementar las capacidades de ciberdefensa en las Fuerzas Armadas, para la neutralización de amenazas y la mitigación oportuna de ciberataques en la ICD del sector Defensa y contribuir en la defensa de las ICD y servicios esenciales del Estado.

Línea de acción 3

Establecer un mecanismo de intercambio de productos de ciberinteligencia con indicadores de compromiso respecto a amenazas tecnológicas, con instituciones nacionales e internacionales, que garantice información oportuna para una toma de decisiones eficaz en ciberdefensa.

Indicador	Número de productos de ciberinteligencia con indicadores de compromiso compartidos.
Meta	04 (CUATRO) productos por mes con indicadores de compromiso (IOC).
Periodicidad	Mensual
Criterio de Cálculo	Número de productos de ciberinteligencia compartidos con IOC validados.
Responsables	Comando de Ciberdefensa. Dirección de Talento Humano del CC.FF.AA. Dirección de Talento Humano de cada Fuerza.

OBJETIVO ESTRATÉGICO 2

Incrementar las capacidades de ciberdefensa en las Fuerzas Armadas, para la neutralización de amenazas y la mitigación oportuna de ciberataques en la ICD del sector Defensa y contribuir en la defensa de las ICD y servicios esenciales del Estado.

Línea de acción 4

Desarrollar e implementar un plan de adiestramiento operacional y evaluación continua que potencie la preparación del personal militar profesional en operaciones y acciones tácticas de ciberdefensa.

Indicador	Porcentaje de personal militar profesional entrenado y evaluado en operaciones y acciones tácticas de ciberdefensa.
Meta	70% del personal técnico entrenado y evaluado en operaciones y acciones tácticas de ciberdefensa hasta 2029.
Periodicidad	Cuatrienal
Criterio de Cálculo	((Número de militares técnicos entrenados y evaluados en operaciones y acciones tácticas de ciberdefensa) / (Número total de militares técnicos entrenados y evaluados del sistema de ciberdefensa)) * 100
Responsables	Dirección de Personal del CC.FF.AA. Comando de Ciberdefensa. Fuerzas: Terrestre, Naval y Aérea.

OBJETIVO ESTRATÉGICO 3

Fortalecer de manera sostenible la capacitación y especialización técnica del personal de Fuerzas Armadas, mediante programas formativos y de actualización continua, con el fin de garantizar la preparación operativa y la ejecución efectiva de operaciones en el ciberespacio.

Línea de acción 1

Coordinar la implementación de un Plan Integral de Capacitación con programas estandarizados y especialización en seguridad de la información, ciberseguridad y ciberdefensa a través de convenios con la academia y aliados estratégicos internacionales.

Indicador	Porcentaje de Implementación del Plan Integral de Capacitación en seguridad de la información, ciberseguridad y ciberdefensa.
Meta	100% anual de cumplimiento de programas planificados.
Periodicidad	Anual
Criterio de Cálculo	(Número de programas de capacitación y especialización ejecutados) / (Número de programas de capacitación y especialización planificados) × 100
Responsables	Dirección de Educación y Doctrina de las FF.AA. Comando de Ciberdefensa.

OBJETIVO ESTRATÉGICO 3

Fortalecer de manera sostenible la capacitación y especialización técnica del personal de Fuerzas Armadas, mediante programas formativos y de actualización continua, con el fin de garantizar la preparación operativa y la ejecución efectiva de operaciones en el ciberespacio.

Línea de acción 2

Implementar entrenamientos prácticos y simulaciones en un entorno virtual especializado nacional, integrando ejercicios conjuntos e internacionales.

Indicador	Número de ejercicios realizados en el año.
Meta	02 (DOS) ejercicios anuales.
Periodicidad	Anual
Criterio de Cálculo	Número de ejercicios ejecutados.
Responsables	Comando de Ciberdefensa. Unidades de Ciberdefensa de las FF.AA.

OBJETIVO ESTRATÉGICO 3

Fortalecer de manera sostenible la capacitación y especialización técnica del personal de Fuerzas Armadas, mediante programas formativos y de actualización continua, con el fin de garantizar la preparación operativa y la ejecución efectiva de operaciones en el ciberespacio.

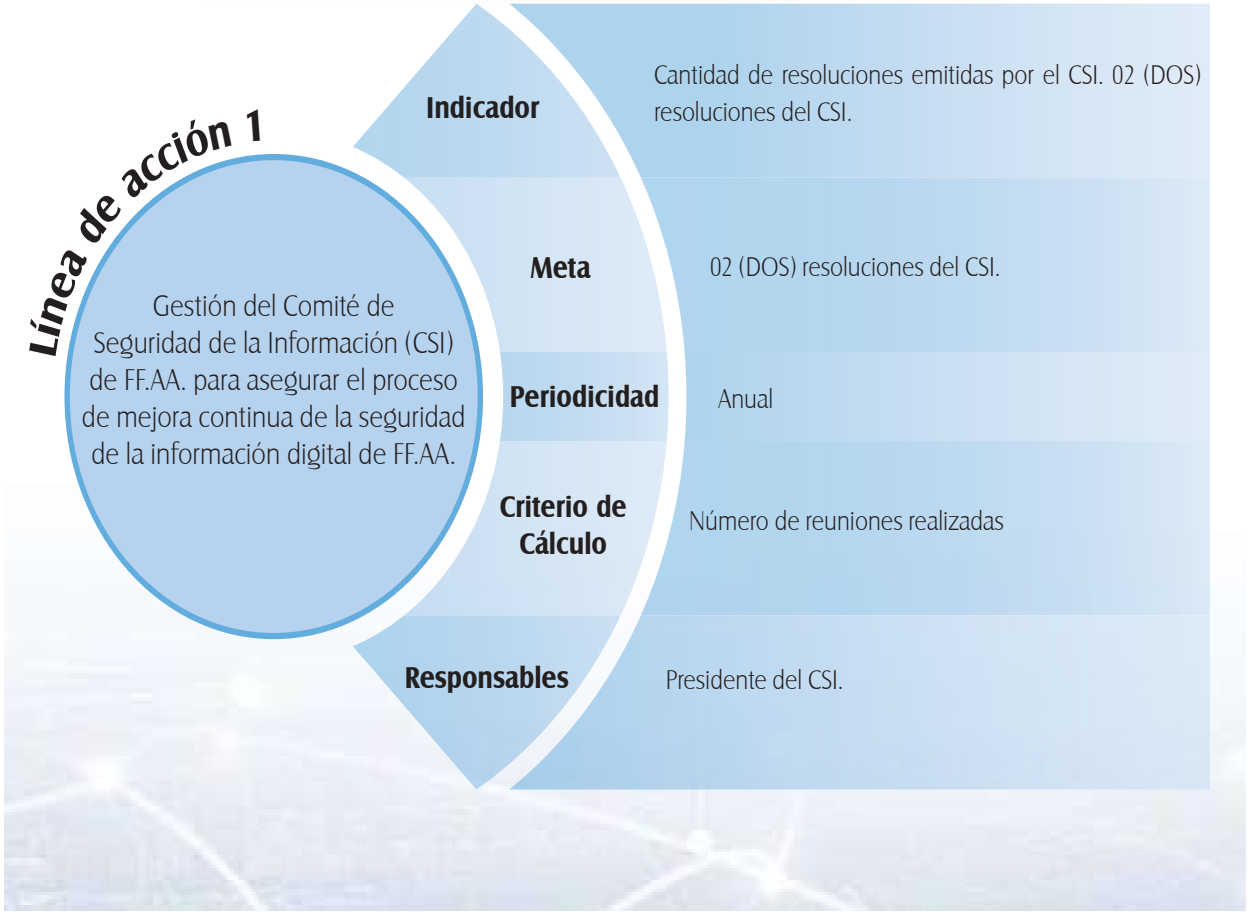
Línea de acción 3

Coordinar la elaboración e implementación de un plan de gestión, rotación y retención de talento humano especializado en operaciones en el ciberespacio, con incentivos de carrera y convenios con la academia y sector privado acorde al art. 94 del Reglamento de la Ley Orgánica de Personal y Disciplina de las Fuerzas Armadas.

Indicador	Tasa de retención (%) de personal especializado en ciberdefensa.
Meta	50% de retención del Personal Militar Profesional (PMP) técnico de ciberdefensa durante cinco años.
Periodicidad	Anual
Criterio de Cálculo	((Número de PMP técnico retenido 5 años) / (Número de PMP técnico asignado a unidades de ciberdefensa)) × 100
Responsables	Dirección de Talento Humano del CC.FF. AA. Comando de Ciberdefensa. Dirección de Talento Humano de cada Fuerza.

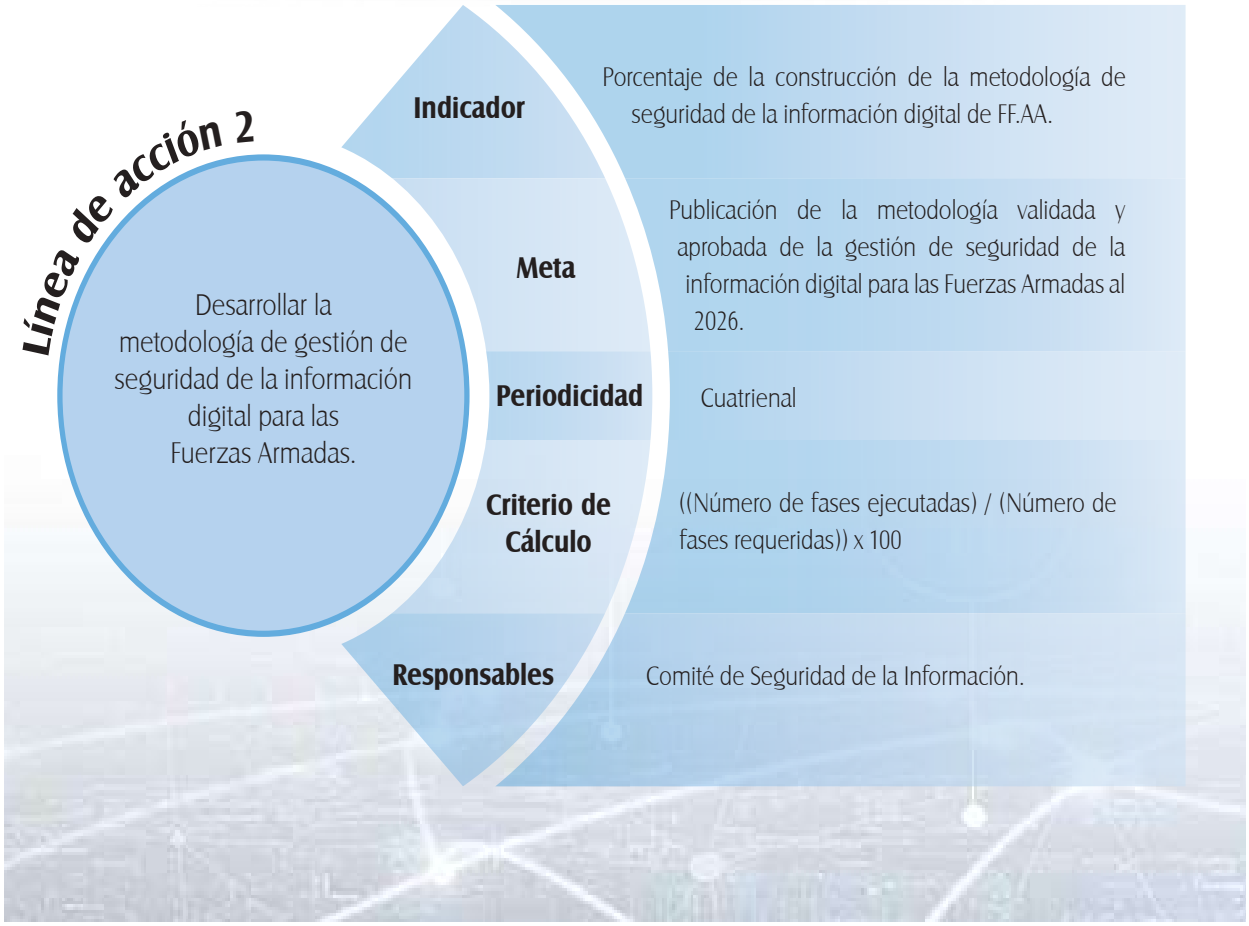
OBJETIVO ESTRATÉGICO 4

Incrementar la madurez de los Sistemas de Gestión de Seguridad de la Información (SGSI) en el sector Defensa, mediante la implementación de estándares, controles y buenas prácticas, con el fin de contribuir a la confidencialidad, integridad y disponibilidad de la información crítica digital para las Fuerzas Armadas.



OBJETIVO ESTRATÉGICO 4

Incrementar la madurez de los Sistemas de Gestión de Seguridad de la Información (SGSI) en el sector Defensa, mediante la implementación de estándares, controles y buenas prácticas, con el fin de contribuir a la confidencialidad, integridad y disponibilidad de la información crítica digital para las Fuerzas Armadas.



OBJETIVO ESTRATÉGICO 4

Incrementar la madurez de los Sistemas de Gestión de Seguridad de la Información (SGSI) en el sector Defensa, mediante la implementación de estándares, controles y buenas prácticas, con el fin de contribuir a la confidencialidad, integridad y disponibilidad de la información crítica digital para las Fuerzas Armadas.

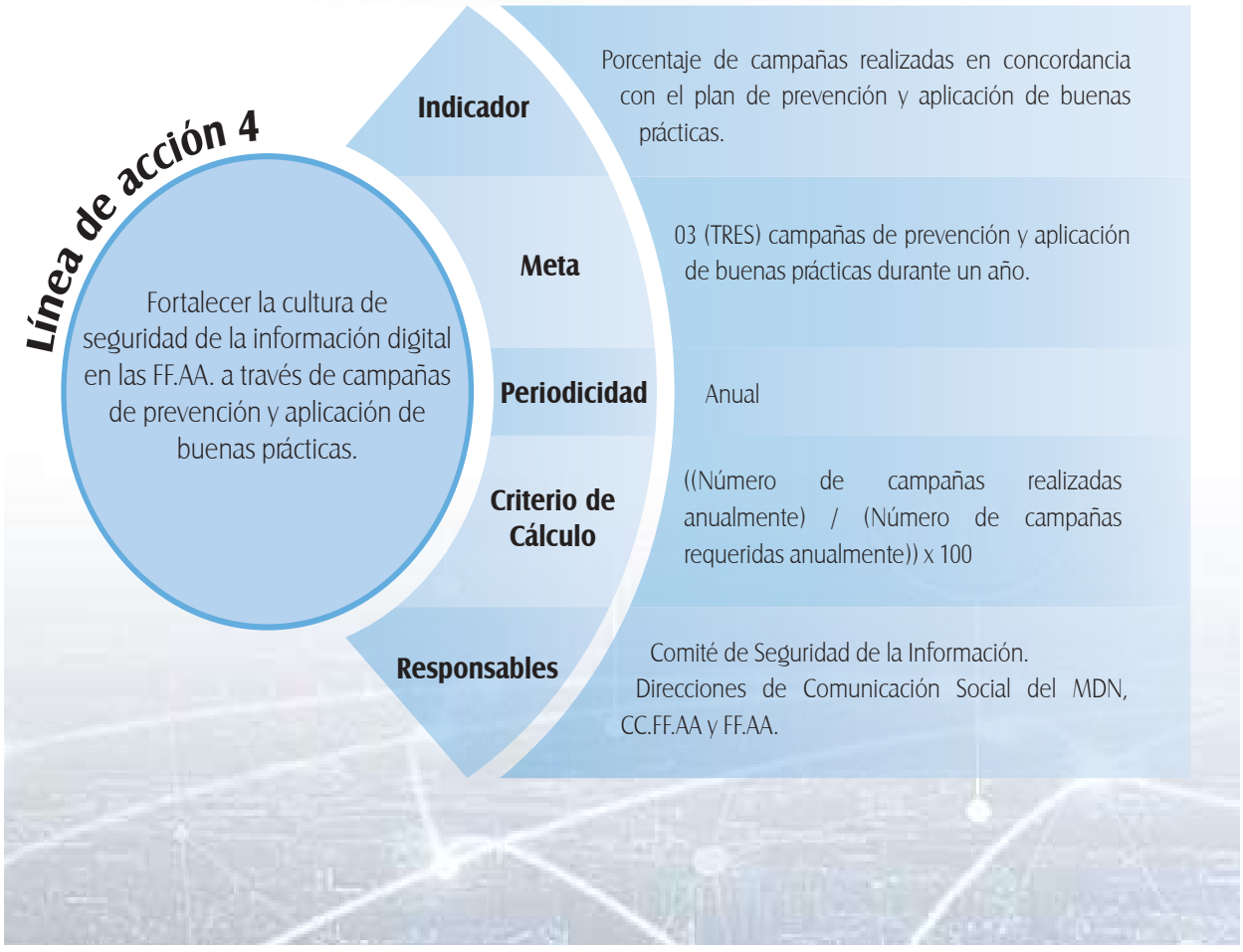
Línea de acción 3

Implementación de la Gestión de Seguridad de la Información Digital en las Fuerzas Armadas, período 2026 - 2029

Indicador	Porcentaje de implementación del Plan de Gestión.
Meta	Implementar al 100% el Plan de Gestión de Seguridad de la Información Digital en las Fuerzas Armadas.
Periodicidad	Anual
Criterio de Cálculo	((Número de fases ejecutadas) / (Número de fases planificadas)) x 100
Responsables	Comité de Seguridad de la Información.

OBJETIVO ESTRATÉGICO 4

Incrementar la madurez de los Sistemas de Gestión de Seguridad de la Información (SGSI) en el sector Defensa, mediante la implementación de estándares, controles y buenas prácticas, con el fin de contribuir a la confidencialidad, integridad y disponibilidad de la información crítica digital para las Fuerzas Armadas.




101

Glosario de Términos

Blockchain:

Tecnología que permite almacenar y compartir información digital de forma segura, transparente y confiable, revolucionando procesos en sectores como finanzas, gobierno, logística y muchos más (García Tardón, Olivares, & Guzmán, 2023).

Ciberdefensa:

La ciberdefensa es un complemento de la ciberseguridad, que provee la defensa contra las amenazas en el ciberespacio en beneficio de toda la población. Es la capacidad del Estado, organizada y preparada para ejecutar operaciones militares que permitan prevenir y contrarrestar las ciberamenazas, ciberataques, incidentes en el ciberespacio o actos hostiles que afecten a la soberanía e integridad territorial, el orden constitucional y los intereses nacionales (Cardona, 2021).

Ciberinteligencia:

La ciberinteligencia es el proceso de recopilar, analizar y transformar información del ciberespacio en conocimiento útil para anticipar, detectar y mitigar las ciberamenazas. Se basa en evidencias y permite a organizaciones, instituciones y Estados tomar decisiones informadas frente a riesgos y actores hostiles en el ciberespacio. Los productos de ciberinteligencia son:

- Boletín de Ciberinteligencia
- Apreciación de Ciberinteligencia (Clasificación Reservado)
- Informe de Ciberinteligencia (Clasificación Reservado)

Ciberseguridad:

Conjunto de herramientas, políticas, técnicas de seguridad, directrices, métodos de gestión de riesgos y tecnologías que puedan utilizar- se para proteger los activos de información, durante su procesamiento, almacenamiento, transporte y uso, a fin de prevenir, reducir, neutralizar e investigar los riesgos, amenazas y delitos en el ciberespacio a las que están expuestas todas las personas naturales y jurídicas en el territorio ecuatoriano (Zuluaga, 2020).

Ciberespacio:

Dominio caracterizado por el uso de las tecnologías de la información TI, tecnologías de operación TO, Internet de las cosas IoT y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas de red e infraestructuras asociadas (López de Vallejo, 2021).

Ciberataque:

Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información, mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas

de información y telecomunicaciones o las infraestructuras que los soportan (Microsoft Corporation, 2021)

Ciberinteligencia:

Es la disciplina especializada dentro de la ciberdefensa que se enfoca en la identificación, recolección, análisis y difusión de información relacionada con amenazas técnicas en el ciberespacio. Incluye la detección de vulnerabilidades, malware, TTP (tácticas, técnicas y procedimientos) de actores hostiles, y actividades de APT (Amenazas Persistentes Avanzadas), utilizada por las Fuerzas de Ciberdefensa para la ejecución de ciberoperaciones defensivas y ofensivas, a fin de anticipar, mitigar o explotar amenazas en el dominio ciberespacial. A diferencia de la inteligencia en el ciberespacio, que es de carácter informativo y analítico sobre actores o contextos digitales, ya que la ciberinteligencia tiene un enfoque técnico operacional centrado en amenazas y vulnerabilidades del entorno ciberespacial, indispensable para las operaciones de ciberdefensa (De la Peña, 2024).

Ciberterrorismo:

Ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar, con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente (Sánchez-Jijón, 2021).

Ciberconflicto:

Lucha armada (en este caso las armas son las TIC) entre dos o más naciones o entre bandos de una misma nación, en la que se utiliza el ciberespacio como campo de batalla (Maness & Valeriano, 2020).

Ciberarma:

Programa o código malicioso que sirve para atacar o defenderse en el ciberespacio (Realpe Díaz, 2024).

Computación cuántica:

La computación cuántica utiliza principios de la mecánica cuántica, como la superposición y el entrelazamiento, para realizar cálculos complejos. Busca resolver problemas que están más allá de la capacidad de las computadoras clásicas, ofreciendo un potencial revolucionario en campos como la criptografía y el descubrimiento de fármacos (IBM Corporation, 2021).

Defensiva:

Son operaciones, pasivas y activas, destinadas a preservar la capacidad para utilizar el ciberespacio propio (azul) y proteger nuestros datos, redes, dispositivos, capacidades centradas en la red y otros sistemas asignados, que son amenazados por actividades ciberespaciales maliciosas en curso o inminentes (Realpe Díaz, 2024).

Evento:

Ocurrencia o cambio de un conjunto particular de circunstancias (ISO/IEC 27000, 2018).

Exploit:

Es un fragmento de código, software o técnica diseñado para aprovechar una vulnerabilidad en un sistema, aplicación o red, con el objetivo de alterar su funcionamiento normal

Exploración o explotación:

Son operaciones pasivas y activas destinadas a la obtención de información de fuentes abiertas o en fuentes cerradas (intrusivas), para la producción de ciberinteligencia y la

conducción de operaciones defensivas y de respuesta u otras operaciones convencionales (Junta Interamericana de Defensa, 2020).

Incidente de Seguridad:

Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información (ESET Latinoamérica, 2022).

Infraestructura crítica:

Sistemas y activos, físicos o digitales, esenciales para el Estado cuya perturbación o destrucción tendrá un impacto en la seguridad, economía nacional, salud pública, medio ambiente o cualquier combinación de estos aspectos (Lisa Institute, 2025).

Infraestructura crítica de la Defensa:

Sistemas y activos, físicos o digitales, cuyo funcionamiento es indispensable para el Sector Defensa, por lo que su perturbación o destrucción pueden causar un estado de vulnerabilidad para la seguridad en las operaciones o el incumplimiento de la misión (Espinoza Jaramillo, 2023).

Infraestructura crítica digital:

Son las instalaciones, redes, sistemas y equipos físicos de tecnologías de información y operación sobre las que se soporta el funcionamiento de los servicios esenciales de la infraestructura crítica y de las áreas estratégicas del Estado (Cedeño & Espinoza, 2023).

Inteligencia artificial:

La Inteligencia Artificial (IA) es un campo de la informática que se dedica a la creación de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. Esto incluye el aprendizaje, la toma de decisiones, la resolución de problemas y la comprensión del lenguaje (Martínez, 2023).

Inteligencia en el ciberespacio:

Permite obtener información del ciberespacio (redes sociales, foros, sitios web, bases de datos abiertas o restringidas, etc.) con fines de perfilamiento, vigilancia estratégica, análisis de comportamientos y apoyo a operaciones de inteligencia tradicional. Utiliza medios tecnológicos como OSINT, SOCMINT, y otras técnicas de recopilación digital. Su objetivo principal es producir inteligencia útil para ser empleada por cualquier ámbito, unidad u organismo. (Vásquez & Pérez, 2024).

Proteger en el ciberespacio:

Significa aplicar medidas y políticas para resguardar sistemas informáticos, redes, dispositivos y datos contra amenazas digitales, como accesos no autorizados, ciberataques y violaciones de datos, garantizando la confidencialidad, integridad y disponibilidad de la información y sistemas online.

Resiliencia:

Capacidad de las organizaciones de recuperarse rápidamente de ataques deliberados, o incidentes que impliquen el uso de las tecnologías de la información y la comunicación.

Respuesta:

Son operaciones destinadas a proyectar el poder y la aplicación de la fuerza en y a través del ciberespacio (Realpe Díaz, 2024)

Riesgo:

Significa tener un proceso integral de gestión de riesgos de TI (Sánchez, 2022).

Seguridad de la información:

Conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información. Es el gran paraguas que abarca a la ciberseguridad y ciberdefensa (Sánchez, 2022).

Servicios esenciales:

Los servicios cuya interrupción podría poner en peligro la vida, la seguridad, la defensa, la educación, el bienestar social y económico de una comunidad, o el eficaz funcionamiento de las Instituciones del Estado y administraciones públicas (Lisa Institute, 2025).

Control de Supervisión y Adquisición de Datos (SCADA):

Es un sistema informático utilizado para supervisar, controlar y automatizar procesos industriales y de infraestructuras críticas tales como: plantas de energía, sistemas de agua, fábricas, sector petrolero, transporte, entre otras, que permite la recolección de datos en tiempo real desde sensores y dispositivos, el monitoreo centralizado, el control remoto de equipos y la generación de reportes sobre el funcionamiento de los sistemas.

Tecnologías de la Operación:

Conjunto de tecnologías que se utilizan en los procesos industriales y en la gestión de infraestructuras destinadas a realizar la operación de estas (Rockwell Automation, 2022).

Tecnologías de la Información:

Las Tecnologías de la Información (TI) se refieren al uso de cualquier computadora, almacenamiento, redes y otros dispositivos físicos, herramientas y procesos para crear, procesar, almacenar, asegurar e intercambiar datos electrónicos. Son fundamentales para la operación y gestión de las organizaciones modernas (Lisa Institute, 2025).

Tecnologías emergentes:

Las tecnologías emergentes son innovaciones que están en desarrollo o que han sido recientemente desarrolladas y se espera que tengan un impacto significativo en el futuro. Ejemplos incluyen la realidad virtual, el blockchain y la biotecnología avanzada, con el potencial de transformar múltiples industrias y aspectos de la vida cotidiana (Espinoza Jaramillo, 2023).

Acrónimos

ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones.
CC.FF.AA	Comando Conjunto de las Fuerzas Armadas.
CERT	Centro de Respuesta a Emergencias de Seguridad Informática.
CICTE	Comité Interamericano Contra el Terrorismo.
CIRT	Centro de Respuesta a Incidentes Informáticos.
CITEL	Comisión Interamericana de Telecomunicaciones.
COCIBER	Comando de Ciberdefensa.
CSIRT	Centro de Respuesta a Incidentes de Seguridad Informática.
DCSI	Dirección de Ciberdefensa y Seguridad de la Información.
DDOS	Ataques Distribuidos de Denegación de Servicios.
DOS	Ataques de Denegación de Servicios.
ECUCERT	Centro de Respuesta a Incidentes Informáticos del Ecuador.
EGSI	Esquema Gubernamental de Seguridad de la Información.
FIRST	Foro Global de Equipos de Seguridad y Respuesta a Incidentes.
IA	Inteligencia Artificial.
IC	Infraestructura Crítica.

ICDF	Infraestructura Crítica Digital de la Defensa.
ICD	Infraestructura Crítica Digital.
IoT	Internet de las cosas.
MINTEL	Ministerio de Telecomunicaciones.
ONU	Organización de las Naciones Unidas.
OTAN	Organización del Tratado del Atlántico Norte.
SOC	Centro de Operaciones de Seguridad T.I.
TCP / IP	Transport Control Protocol / Internet Protocol.
TI	Tecnologías de la Información.
TIC	Tecnologías de la Información y Comunicaciones.
TO	Tecnologías de la Operación.
UE	Unión Europea.
UIT	Unión Internacional de Telecomunicaciones.
UCD	Unidad de Ciberdefensa.
VPN	Virtual Private Network, red privada virtual.
URL	Localizador uniforme de recursos.
IOC	Indicador de Riesgo.

Referencias

1. Asamblea Nacional. (2023). Ley Orgánica para la Transformación Digital y Audiovisual. Quito.
2. Asma, M. (16 de septiembre de 2022). El Grand Continent. Obtenido de Tecnopolítica del ciberespacio: https://legrandcontinent.eu/es/2022/09/16/tecnopolitica-del-ciberespacio/
3. Barria Huidobro, C. (2024). Navegando la soberanía digital del ciberespacio. Centro de Investigaciones y estudios estratégicos, 6-22.
4. Boonkrong, S. (2023). Modelos generativos y ciberataques automatizados. Journal of Cybersecurity Research, 201-220.
5. Calderón Lara, N. (2025). El ciberespacio como escenario de conflicto en el siglo XXI. ¿Hacia la Militarización de la ciberseguridad? Razón Crítica, 21.
6. Calvo Albero, J. (2023). Ciberseguridad y guerra híbrida: La ampliación del espectro. Obtenido de https://www.unav.edu/web/global-affairs/detalle/-/blogs/ciberseguridad-y-guerra-hibrida-la-ampliacion-del-espectro
7. Cámara de Comercio Internacional (ICC). (Julio de 2024). Protección de la ciberseguridad de las infraestructuras críticas y sus cadenas de suministro. París, Francia.
8. Cardona, A. (2021). Ciberdefensa-Ciberseguridad: Riesgos y amenazas. Revista Seguridad y Defensa, 35-50.
9. Cedeño, M., & Espinoza, A. (2023). Estrategia nacional de ciberseguridad del Ecuador. Obtenido de Asobanca: https://asobanca.org.ec/wp-content/uploads/2023/04/Estrategia-Nacional-de-Ciberseguridad-del-Ecuador.pdf
10. Che Mat, N., Abdul Ghani, M., & Noor, R. (2024). Revisión sistemática de la literatura sobre comportamientos de detección de amenazas persistentes avanzadas (APT). Journal of Information Security, 161-177.
11. Check Point Software Technologies Ltd. (2024). 2024 Cyber Security Report. Tel Aviv.
12. Comando Conjunto de las Fuerzas Armadas. (2018). Plan de Capacidades. Quito.
13. Comando Conjunto de las Fuerzas Armadas. (2018). Plan de Desarrollo de Capacidades. Quito.
14. Comando Conjunto de las Fuerzas Armadas. (2021). Plan Estratégico de las Fuerzas Armadas 2021-2033. Quito.
15. Comando de Ciberdefensa. (2025). Informe de indicadores de la Estrategia de Ciberdefensa. Quito.
16. Comisión Europea. (04 de abril de 2025). Comisión Europea. Obtenido de Ciberseguridad: https://digital-strategy.ec.europa.eu/es/policies/cybersecurity

17. Corporación MITRE. (2025). Attack. Mitre.Org. Obtenido de Mitre Attack: attack.mitre.org

18. CrowdStrike Inc. (2024). CrowdStrike Global Threat Report. Austin.

19. De la Peña, A. (2024). Ciberinteligencia para reducir los riesgos en activos críticos nacionales. Revista Estudios y Perspectivas, 71-84.

20. Díaz, R. (2025). Vulnerabilidades y ciberseguridad en sistemas SCADA: Análisis de riesgos en infraestructuras críticas. Obtenido de Investigarmqr.com

21. El Universo. (28 de agosto de 2024). Ecuador enfrenta aumento de ciberataques mientras la inversión en ciberseguridad crece. Obtenido de LEXIS Noticias: https://www.lexis.com.ec/noticias/ecuador-enfrenta-aumento-de-ciberataques-mientras-la-inversion-en-ciberseguridad-crece

22. ESET Latinoamérica. (2022). ESET Security Report. El 48% de las empresas sufrió algún tipo de incidente de seguridad.

23. Espinoza Jaramillo, P. (2023). Seguridad militar inteligente: integración de tecnologías emergentes y gobernanza contractual en la protección de infraestructuras estratégicas del Ejército Ecuatoriano. Revista Pacha, 44-56.

24. European Union Agency for Cybersecurity (ENISA). (2021). Raising awareness of cybersecurity. En ENISA.

25. European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. Madrid.

26. Fortinet. (2025). Fortinet. Obtenido de Ciberresiliencia: https://www.fortinet.com/lat/resources/cyberglossary/cyber-resilience

27. García Tardón, Y., Olivares, M., & Guzmán, F. (2023). Blockchain: Aplicación en el comercio internacional y en la gestión documental. Revista Brasileira de Gestão de Negócios, 97-110.

28. Herrera Guzmán, E. (2025). Inteligencia Artificial y Ciberseguridad: Transformación Digital de la Seguridad Nacional en el Siglo XXI. Revista Inclusiones, 20.

29. Hinarejos Rojo, A., & De la Peña Muñoz, J. (2023). I+D+i y ciberseguridad: análisis de una relación de dependencia. Ciberseguridad: la cooperación público-privada, 247-290.

30. IBM Corporation. (2021). IBM Corporation. Obtenido de ¿Qué es la computación cuántica?: https://www.ibm.com/mx-es/topics/quantum-computing

31. Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Computer Science, 32.

32. ISO/IEC 27000. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. International Organization for Standardization.

33. Junta Interamericana de Defensa. (2020). Guía de Ciberdefensa . Washington D.C.

34. Junta Interamericana de Defensa. (2024). Tecnologías Emergentes en Ciberdefensa. Washington.

35. Labrador Blanes, M. (2023). Análisis comparativo de la desinformación verificada por plataformas digitales en el proceso electoral chileno 2022–2023. InMediaciones de la Comunicación, 1-23.

36. Lisa Institute. (2025). Infraestructuras críticas: definición, planes, riesgos y amenazas. Blog Lisa Institute.

37. López de Vallejo, I. (2021). El ciberespacio como escenario para enfrentar los delitos informáticos. Revista de Estudios y Perspectivas en Ciencia y Tecnología, 45-58.

38. Maness, R., & Valeriano, B. (2020). El poder en la era digital: perspectivas sobre el ciberpoder. Revista de Estudios Digitales, 60-79.

39. Martínez, M. (2023). Inteligencia artificial en la informática. Recimundo, 98-110.

40. Microsoft Corporation. (2021). Ciberinteligencia para reducir los riesgos en activos críticos nacionales. Revista Estudios y Perspectivas, 71-84.

41. Ministerio de Defensa Nacional (2019). Política de Defensa Nacional del Ecuador "Libro Blanco". Quito.

42. Ministerio de Defensa Nacional. (2019). Plan Nacional de Seguridad Integral 2025-2029. Quito.

43. Ministerio de Defensa Nacional. (2021). Estrategia de Ciberdefensa 2021. Quito.

44. Ministerio de Defensa Nacional. (2021). Plan Sectorial de la Defensa 2025-2029. Quito.

45. Ministerio de Defensa Nacional. (2024). Plan Estratégico Institucional 2024-2025. Quito.

46. Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). Política Nacional de Ciberseguridad. Quito.

47. Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). Estrategia Nacional de Ciberseguridad del Ecuador 2022-2025. Quito.

48. Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2023). Política Pública de Telecomunicaciones 2023-2025. Quito.

49. Ministerio de Telecomunicaciones y Sociedad de la Información. (17 de mayo de 2021). Ministerio de Telecomunicaciones y de la Sociedad de la Información. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

50. Muñoz-Pallaroso, E. K., Romero-Vásquez, X. M., Pallaroso-Granizo, R. Y., & Oviedo-Bayas, B. (2025). Gobernanza digital y transformación del Estado. Impacto de la tecnología en la gestión pública. Revista Metropolitana de Ciencias Aplicadas, 96-100.

51. Ortiz Correa, Y. (2024). Hacktivismo como acción política. Caldas.

52. Presidencia de la República del Ecuador. (2025). Plan Nacional de Desarrollo 2025-2029. Quito.

53. Realpe Díaz, C. (2024). El concepto de ciberdefensa activa. Real Instituto Elcano.

54. Realpe Díaz, M. E. (2024). Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio. En M. E. Realpe Díaz, & A. González González. Bogotá: Sello Editorial ESDEG.

55. Rivas, M., & Tenorio, F. (2022). Sistema de monitoreo de señales en tierra usando enlaces satelitales de bajo costo y procesamiento en la nube. Revista de Comunicaciones, 15-30.

56. Rockwell Automation. (2022). Preparación de ciberseguridad en infraestructura crítica. Informe de Investigación.

57. S2Grupo. (26 de junio de 2025). Exploits: qué son, cómo se utilizan y cómo mitigar sus riesgos. Obtenido de https://s2grupo.es/exploits-que-son-como-se-utilizan-y-como-mitigar-sus-riesgos/

58. Sánchez, F. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. Revista de Ciencias Sociales, 243–258.

59. Sánchez-Jijón, L. (2021). Repensando el concepto de ciberterrorismo. Revista de Ciencias de la Seguridad, 137-160.

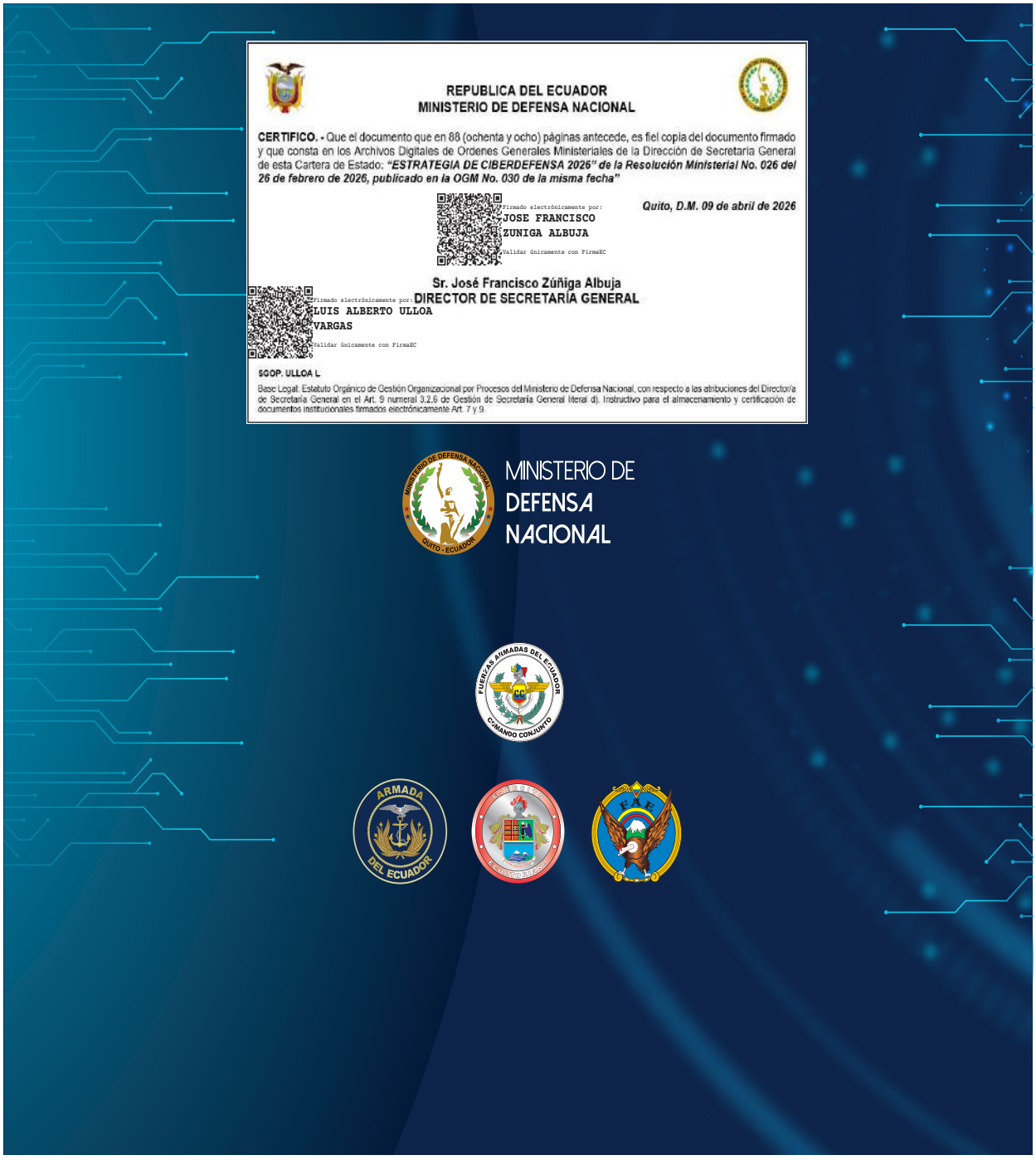
60. United Nations Office on Drugs and Crime. (2021). United Nations Office on Drugs and Crime. Obtenido de International cooperation on cybersecurity matters: https://sherloc.unodc.org/cld/zh/education/tertiary/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

61. Vásquez, A., & Pérez, L. (2024). Inteligencia de amenazas y ciberataques: fundamentos para la defensa activa en ciberseguridad. Revista ITECSUR, 22-36.

62. Verizon DBIR. (2024). Data Breach Investigations Report. Nueva Jersey.

63. Zuluaga, J. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global. Revista de Derecho y Tecnologías, 120-135.

MINISTERIO DE
DEFENSA
NACIONAL



REPUBLICA DEL ECUADOR
MINISTERIO DE DEFENSA NACIONAL

CERTIFICO. - Que el documento que en 88 (ochenta y ocho) páginas antecede, es fiel copia del documento firmado y que consta en los Archivos Digitales de Ordenes Generales Ministeriales de la Dirección de Secretaría General de esta Cartera de Estado: ***"ESTRATEGIA DE CIBERDEFENSA 2026" de la Resolución Ministerial No. 026 del 26 de febrero de 2026, publicado en la OGM No. 030 de la misma fecha"***

Firmado electrónicamente por:
JOSE FRANCISCO ZUNIGA ALBUJA
Validar únicamente con FirmaEC

Quito, D.M. 09 de abril de 2026

Sr. José Francisco Zúñiga Albuja
DIRECTOR DE SECRETARÍA GENERAL

Firmado electrónicamente por:
LUIS ALBERTO ULLOA VARGAS
Validar únicamente con FirmaEC

SGOP. ULLOA L

Base Legal: Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Defensa Nacional, con respecto a las atribuciones del Director/a de Secretaría General en el Art. 9 numeral 3.2.6 de Gestión de Secretaría General literal d). Instructivo para el almacenamiento y certificación de documentos institucionales firmados electrónicamente Art. 7 y 9

MINISTERIO DE DEFENSA NACIONAL

Mgs. Jaqueline Vargas Camacho
DIRECTORA (E)

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Atención ciudadana
Telf.: 3941-800
Ext.: 3134

www.registroficial.gob.ec

MG/FA

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"