Ministerio de Telecomunicaciones
y de la Sociedad de la Información

ESTRATEGIA NACIONAL DE **CIBERSEGURIDAD DEL ECUADOR**

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR

Vianna Maino

Ministra de Telecomunicaciones y de la Sociedad de la Información

La ciberseguridad es un tema de vital importancia para el Gobierno del Presidente Guillermo Lasso, estamos conscientes que resguardar la seguridad ciudadana y de los Estados en el ciberespacio es una tendencia mundial sin retorno, del que Ecuador no puede estar apartado.

Solo aquellos países que cuenten con una protección suficiente y constantemente actualizada son los que lograrán realmente triunfar en la nueva era digital que vive el mundo.

Pero, la construcción de las estrategias de protección no pueden estar apartadas del contexto mundial, la seguridad informática no entiende de fronteras físicas y un ambiente cyberseguro solo se consigue si aunamos esfuerzos y trabajamos de la mano con los países que mayor conocimiento tienen en la materia.

Por ello, debo agradecer el apoyo que hemos recibido del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, de la Organización de los Estados Americanos (CICTE/OEA); y al Proyecto de Resiliencia Cibernética para el Desarrollo, de la Unión Europa (CYBER4DEV).

Gracias a esta cooperación internacional el Ecuador cuenta con su Estrategia Nacional de Ciberseguridad, un documento que fija los lineamientos para la seguridad nacional en el ciberespacio y que contó con la participación de más de 170 actores de la sociedad civil, académicos, expertos en ciberseguridad, funciones del estado, sector privado y todas las instituciones que conforman el Comité Nacional de Ciberseguridad, organismo creado en el actual Gobierno y que aglutina los Ministerios de Telecomunicaciones y de la Sociedad de la Información, Defensa Nacional, Gobierno, Interior, Relaciones Exteriores y Movilidad Humana, el Centro de Inteligencia Estratégica y la Secretaría General de la Administración Pública de la Presidencia.

Esta Estrategia, que tendrá una aplicación de 3 años (2022-2025), se basa en seis ejes de acción que abarcan temas coyunturales y prioritarios para el país: Gobernanza y coordinación nacional; Resiliencia cibernética; Prevención y combate a la ciberdelincuencia; Ciberdefensa; Habilidades y capacidades de ciberseguridad; y Cooperación internacional.

La Estrategia Nacional de Ciberseguridad que se constituye en una herramienta más para mantenernos alertas siempre en el mundo de la tecnología donde la evolución es muy dinámica y vertiginosa.

Con ciberseguridad podemos impulsar otros desarrollos digitales como el comercio electrónico, proteger nuestra información y transacciones financieras, cuidar los datos personales de los ciudadanos e información comercial a nivel local e internacional. Porque los datos son el nuevo oro del mundo y el centro de la reorganización de los gobiernos en este siglo y por eso su resguardo es de vital importancia ahora más que nunca. En la actualidad un clic nos conecta con el mundo y por ello era de vital importancia contar con esta Estrategia efectuada bajo las mejores prácticas mundiales.

Bajo el liderazgo del Presidente Guillermo Lasso seguiremos trabajando por un Ecuador Ciberseguro y por ese Ecuador Digital de las Oportunidades.

Contenido

PANORAMA NACIONAL DE CIBERSEGURIDAD, DESAFÍOS Y OPORTUNIDADES **Pag 06**

Retos y oportunidades para la ciberseguridad Pag 07

Políticas nacionales relacionadas Pag 09

VISIÓN, PRINCIPIOS Y OBJETIVOS ESTRATÉGICOS **Pag 11**

Visión de ciberseguridad de Ecuador 2025 y propósito general de la estrategia Pag 12

Principios rectores de la estrategia Pag 12

PILARES DE LA ESTRATEGIA **Pag 13**

Objetivos estratégicos **Pag 14**

PILAR 1.
Gobernanza y coordinación nacional **Pag 16**

Objetivo 1.1: Establecer un marco integral de gobernanza de la ciberseguridad Pag 17

Objetivo 1.2: Fomentar una comunidad sólida y articulada con expertos en ciberseguridad de las múltiples partes interesadas Pag 18

Objetivo 1.3: Desarrollar un marco legal y regulatorio integral que permita la gobernanza nacional de la ciberseguridad y la ciberdefensa Pag 19

PILAR 2. **Pag 20**
Resiliencia cibernética

Objetivo 2.1: Establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación para las crisis cibernéticas con el fin de fortalecer dichas capacidades a nivel nacional Pag 21

Objetivo 2.2: Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de infraestructuras críticas digitales (ICD), Pag 23

Objetivo 2.3: Continuar desarrollando capacidades de respuesta y gestión de incidentes cibernéticos y del CERT nacional — Pag 25

Objetivo 2.4: Maximizar el uso de tecnologías avanzadas y la innovación en el diseño de políticas y procesos ágiles para el desarrollo de capacidades de Ciberinteligencia — Pag 26

PILAR 3. — Pag 27
Prevención y combate a la ciberdelincuencia

Objetivo 3.1: Actualizar el marco legal y regulatorio de Ecuador en materia de ciberdelincuencia para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio — Pag 29

Objetivo 3.2: Fortalecer la respuesta oportuna y las capacidades operacionales de investigación y judicialización de la cibercriminalidad. — Pag 29

PILAR 4. — Pag 30
Ciberdefensa

Objetivo 4.1: Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano para alcanzar la actitud estratégica defensiva definida en la Política de la Defensa Nacional , para la protección de la infraestructura crítica digital (ICD) y servicios esenciales en el ciberespacio. — Pag 32 — Pag 32

PILAR 5. — Pag 33.
Habilidades y capacidades de ciberseguridad

Objetivo 5.1: Mejorar y ampliar la concientización sobre la ciberseguridad a todos los niveles de la sociedad — Pag 35

Objetivo 5.2: Reforzar las habilidades en materia de ciberseguridad necesarias con las múltiples partes interesadas — Pag 35

Objetivo 5.3: Asegurar que el sistema educativo imparta conocimientos y fortalezca habilidades en materia de ciberseguridad — Pag 36

PILAR 6. — Pag 38
Cooperación internacional

Objetivo 6.1: Identificar las prioridades internacionales de Ecuador y desarrollar la capacidad de participar en la ciberdiplomacia regional e internacional — Pag 38

Objetivo 6.2: Fortalecer la participación de Ecuador en la cooperación bilateral, regional e internacional en respuesta a las amenazas en el ciberespacio — Pag 39

IMPLEMENTACIÓN, SEGUIMIENTO Y EVALUACIÓN — Pag 40

PANORAMA NACIONAL DE CIBERSEGURIDAD, DESAFÍOS Y OPORTUNIDADES

Retos y oportunidades para **la ciberseguridad**

Las tecnologías digitales son indispensables para un Ecuador moderno, potenciando cada vez más nuestras empresas, nuestros servicios públicos y nuestra administración pública, y ofrecen oportunidades para que cada ciudadano se beneficie de la transformación digital. Como país hemos hecho esfuerzos en los últimos años para ampliar y mejorar el acceso a Internet de nuestra población, empresas y administración pública en todo el país y para acelerar el desarrollo económico y social en toda la sociedad.

Con la digitalización que ofrece beneficios económicos y sociales evidentes, las vulnerabilidades tecnológicas y organizativas inherentes, junto con la creciente dependencia digital de la sociedad, también ponen de relieve la necesidad de mejorar la ciberseguridad y la resiliencia cibernética. La creciente sofisticación de la tecnología y su uso generalizado ha dado lugar a amenazas más sofisticadas y complejas, con nuevas dificultades a la hora de identificar, detectar, responder o recuperarse de incidentes cibernéticos. Se espera que esta tendencia continúe con las nuevas tecnologías emergentes, como la inteligencia artificial, el creciente uso de diversos dispositivos inteligentes (IoT), la computación en la nube, las herramientas biométricas, entre otros.

En el 2021, se aprobó nuestra primera Política de Ciberseguridad, publicada mediante Acuerdo Ministerial 006-2021, y se reconoció que los interesados deben fortalecer sus capacidades para identificar, gestionar, tratar y mitigar los riesgos de ciberseguridad. Desde entonces, varios incidentes cibernéticos nacionales nos han llevado a reconocer que es necesario reevaluar nuestros esfuerzos para cerrar las brechas de capacidades para que todas las múltiples partes interesadas puedan aprovechar las oportunidades actuales y futuras en el marco de la Cuarta Revolución Industrial.

Por lo tanto, hemos decidido mejorar la resiliencia cibernética de la sociedad ecuatoriana lanzando la Estrategia Nacional de Ciberseguridad. Teniendo en cuenta las iniciativas anteriores, las conclusiones de las amplias consultas con las múltiples partes interesadas y las mejores prácticas internacionales, esta estrategia se elaboró en estrecha cooperación con actores nacionales e internacionales y tiene por objeto establecer la dirección y un marco para alcanzar objetivos específicos y claros para los próximos tres años (2022-2025).

Nuestras partes interesadas a nivel nacional han sido un apoyo fundamental para los progresos que hemos logrado hasta la fecha. Al examinar nuestras necesidades para la estrategia, reconocemos la importancia de aprovechar las ventajas existentes, incluida la existencia de una política de ciberseguridad, y de órganos nacionales pertinentes, como el Comité Nacional de Ciberseguridad y el EcuCERT; así como el compromiso de las instituciones públicas de mejorar la ciberseguridad y la resiliencia cibernética.

Si bien sabemos que hay varios desafíos, también hay varias oportunidades de crecimiento en nuestra postura de ciberseguridad. Existe una colaboración prometedora tanto a nivel internacional como entre las partes interesadas nacionales que desean mejorar las prácticas existentes y colaborar por conducto de diversos grupos de trabajo.
El clima general de inversión tecnológica en nuestro país ha sido favorable, abriendo también la puerta a inversiones en ciberseguridad. Desde una perspectiva jurídica, hemos adoptado medidas para ratificar y aplicar el Convenio de Budapest sobre la Ciberdelincuencia y el país fue invitado el 30 de marzo de 2022 a adherirse al tratado, una medida que ayudará significativamente a nuestra capacidad de combatir la ciberdelincuencia transfronteriza.

Las amenazas, por otro lado, han incluido ciberataques contra nuestras infraestructuras críticas digitales (ICD), infraestructuras tecnológicas con problemas de obsolescencia, altos costos para la adquisición de tecnología y marcos legales y regulatorios desactualizados, los cuales nos han dejado vulnerables. Además, es necesario que abordemos los desafíos relacionados con la falta de presupuesto sostenido y la escasez de personal especializado en ciberseguridad en las organizaciones, y necesitamos construir sistemáticamente una cultura de ciberseguridad para que las personas y las empresas conozcan cómo protegerse en línea.

Con lo anterior en mente, planteamos las siguientes iniciativas para llevar a nuestro país a un nuevo nivel en ciberseguridad y resiliencia cibernética:

- Reforzar la capacidad institucional, reglamentaria, administrativa y de gestión para abordar las cuestiones de ciberseguridad desde el más

alto nivel, sensibilizando y formando a todas las múltiples partes interesadas;

- Aumentar la confianza digital y fomentar el uso del entorno digital nacional, fortaleciendo el nivel de seguridad de la información, adoptando medidas para gestionar los riesgos de ciberseguridad contra nuestras ICD nacionales y otros activos, y desarrollando una cooperación eficiente en la que participen múltiples partes interesadas, con el objetivo de maximizar los beneficios económicos y sociales en todos los sectores;

- Proteger los derechos digitales y demás derechos fundamentales de los ciudadanos y sus actividades económicas y sociales en el entorno digital reforzando la lucha contra la ciberdelincuencia y aplicando mecanismos de asistencia a las víctimas de este flagelo;

- La racionalización de las capacidades nacionales de defensa frente a las amenazas y a los actos hostiles en el ciberespacio que puedan afectar a la soberanía nacional, la independencia, la integridad territorial, el orden constitucional, los intereses nacionales y la prosperidad económica y social;

- Participar activamente a nivel nacional e internacional en la promoción de un entorno digital abierto, estable y fiable, y en la cooperación, colaboración y asistencia en relación con la gestión de riesgos de ciberseguridad.

A la hora de establecer estas iniciativas de ciberseguridad, tendremos en cuenta componentes como la gobernanza, la educación, la cooperación, la regulación, la investigación, la innovación, la diplomacia, el desarrollo, la protección, la seguridad y defensa de las ICD nacionales, y los intereses nacionales del Estado, entre otros. Nuestros esfuerzos estarán enfocados a los ciudadanos, a la sociedad en general, a las Fuerzas Armadas y a los sectores público y privado, para que nuestro país pueda tener una estructura social y económica que facilite el logro de nuestros objetivos nacionales.

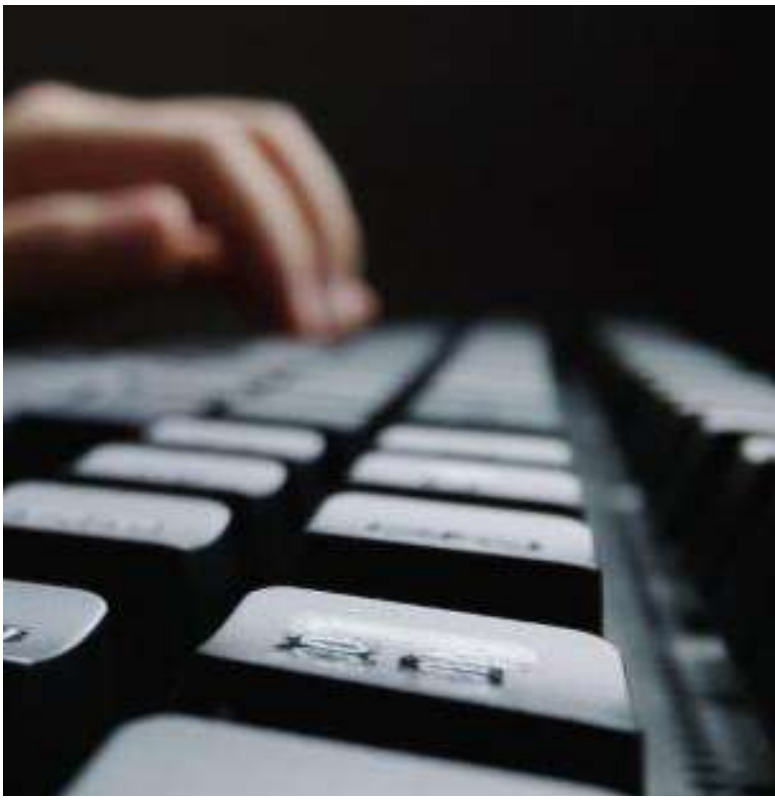
La ciberseguridad requiere una visión holística y una atención multisectorial. Por ello, en el proceso de construcción de esta estrategia, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) contó con el apoyo técnico especializado del Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) y Cyber4Dev, proyecto especial de la Unión Europea, brindando apoyo técnico internacional para involucrar a representantes de los sectores interesados en contribuir al desarrollo de esta materia en el país.

El proceso de construcción de la estrategia fue liderado por el MINTEL con la coordinación de los integrantes del Comité Nacional de Ciberseguridad, celebrando varias mesas de discusión, presenciales y virtuales, con los interesados nacionales en ciberseguridad, guiados por personal especializado de la OEA y de Cyber4Dev.

Políticas nacionales conexas

Varios documentos estratégicos nacionales y de política de alto nivel ya han reconocido objetivos estratégicos relacionados con la ciberseguridad. Por consiguiente, esta estrategia garantiza la continuidad y la complementariedad con las iniciativas existentes y las mejora aún más de éstas.

El Plan Nacional de Desarrollo 2021-2025 establece una visión de un Ecuador próspero, con una democracia liberal plena, regido por el Estado de Derecho y con instituciones eficientes, que respeten la individualidad personal al tiempo que promuevan una economía de libre mercado abierta al mundo, fiscalmente responsable y generadora de empleo. Las directrices y objetivos estratégicos establecidos por el Plan Nacional de Desarrollo incluyen el fortalecimiento de la conectividad y el acceso a las Tecnologías de Información y las Comunicaciones (TIC), el aumento de la cobertura y el acceso a los servicios móviles de alta velocidad y la mejora de la posición internacional de Ecuador en materia de ciberseguridad.



Mediante Acuerdo Ministerial No. 006-2021, emitido en la Edición Especial del Registro Oficial 479, del 23 de junio de 2021, se publicó la Política Nacional de Ciberseguridad, cuyo objetivo es construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio, encaminando acciones para garantizar un ciberespacio seguro.

El Plan Específico de Seguridad Pública y Ciudadana 2019-2030 fija objetivos para detener los delitos transnacionales, entre ellos el delito cibernético, y propone dotar de equipamiento a una Unidad de Ciberinteligencia en la Policía Nacional.

El Plan Específico de Relaciones Exteriores y Movilidad Humana 2019-2030 destaca el impacto de diversas amenazas en la economía, la seguridad integral y la información, pide una cooperación efectiva entre los Estados y resalta la viabilidad del país en el proceso de adhesión al Convenio de Budapest sobre la Ciberdelincuencia.

El Plan Específico de Defensa 2019-2030 prevé la participación activa de Ecuador en el control efectivo del territorio nacional (tierra, mar, aire y ciberespacio), promoviendo el desarrollo de políticas y estrategias relativas a la ciberseguridad y Ciberdefensa para crear las mejores condiciones para enfrentar amenazas y riesgos que afecten la paz y la seguridad. El ejercicio de la defensa en el ciberespacio se vincula con la actitud estratégica defensiva y en el concepto estratégico militar, orientado a contrarrestar las amenazas que pueden afectar la soberanía e integridad territorial en el país. El Comando de Ciberdefensa tiene la misión de ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio, para proteger y defender las ICD nacionales y servicios esenciales del Estado; así como la infraestructura critica digital del sector defensa. Para el efecto, se emplea al Comando de Ciberdefensa y Unidades de Ciberdefensa de las Fuerzas Terrestre, Naval y Aérea, con el apoyo de otras instituciones y entidades del Estado con responsabilidades en el ámbito de la ciberseguridad.

Finalmente, el Plan Estratégico de Defensa Institucional 2017-2021 encomienda a las Fuerzas Armadas de Ecuador evaluar constantemente los escenarios de amenaza y riesgo y actualizar las capacidades de defensa.

VISIÓN, PRINCIPIOS Y OBJETIVOS ESTRATÉGICOS

Visión de ciberseguridad y propósito general de la **Estrategia Nacional de Ciberseguridad del Ecuador**

La declaración sobre la visión de la ciberseguridad para nuestro país se ha formulado conjuntamente con nuestras múltiples partes interesadas de ciberseguridad durante el proceso de elaboración y consulta de la estrategia. La declaración sobre la visión expresa nuestro propósito común de promover capacidades nacionales de resiliencia cibernética, y dirige nuestras aspiraciones en este campo con una perspectiva para el período de vigencia de la estrategia (2022-2025).

Visión 2025: Ecuador es una sociedad inclusiva y competitiva en el futuro digital con capacidades nacionales para gestionar los riesgos de ciberseguridad.

Esta visión sustenta el propósito general de la Estrategia Nacional de Ciberseguridad para asegurar que todos los actores, incluyendo el Gobierno Nacional, las organizaciones públicas y privadas, la academia y la sociedad civil en Ecuador, hagan un uso responsable y seguro del entorno digital, a través del fortalecimiento de la cultura y sus capacidades para identificar y gestionar los riesgos de ciberseguridad de las actividades derivadas del uso de la información digital, maximizando los beneficios en la seguridad de los servicios para los ciudadanos y generando mayor prosperidad económica, política y social.

Principios rectores de la Estrategia Nacional de Ciberseguridad

Los principios rectores de la estrategia tienen por objetivo dirigir y orientar las actividades de todos los actores nacionales que trabajan en pro de la visión y el objetivo general de la Estrategia Nacional de Ciberseguridad. Su objetivo es proteger la soberanía del estado, la protección de la información de las instituciones y los ciudadanos, y garantizar que las acciones e iniciativas en materia de ciberseguridad sean holísticas, coherentes y estén en concordancia con los valores fundamentales compartidos.

Los siguientes principios rectores guían el desarrollo y la aplicación de esta Estrategia Nacional de Ciberseguridad:

1. **Liderazgo y responsabilidad compartida** entre todos los interesados, garantizando la máxima colaboración y cooperación en la gestión de riesgos de ciberseguridad y en la eficiente asignación de recursos.

2. **Salvaguardar los derechos digitales** de las personas, incluida la libertad de expresión, la libre circulación de la información, la protección de datos personales y privacidad, la confidencialidad, integridad y disponibilidad de la información y las comunicaciones, entre otros.

3. **Gestión de riesgos de ciberseguridad y resiliencia cibernética,** que permiten a las personas, empresas e instituciones desarrollar sus actividades de forma libre, confiable y segura en el entorno digital en evolución, así como el uso continuo de los servicios institucionales críticos provistos por las entidades gubernamentales mediante la adopción y el mantenimiento de la innovación tecnológica y herramientas, políticas y procesos de última generación.

4. **Visión inclusiva y colaborativa** que involucre activamente a la sociedad civil, academia, entidades públicas y privadas, en el desarrollo de estrategias, políticas y soluciones para establecer y mejorar las condiciones en el ciberespacio, y participar activamente en la cooperación nacional e internacional y otras alianzas estratégicas.

PILARES DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Objetivos estratégicos

La estrategia se articula en torno a seis pilares, de los cuales se derivan y definen los Objetivos Estratégicos de la Estrategia Nacional de Ciberseguridad del Ecuador:

1. Gobernanza y coordinación nacional: establecer un enfoque coordinado de la ciberseguridad nacional.

2. Resiliencia cibernética: mejorar la resiliencia cibernética a nivel nacional y organizacional para prepararse, responder y recuperarse de los incidentes cibernéticos.

3. Prevención y lucha contra la cibercriminalidad: Fortalecimiento de las capacidades para prevenir, investigar y perseguir los delitos cibernéticos.

4. Ciberdefensa nacional: reforzar las capacidades de ciberdefensa para proteger las Infraestructuras de Información Crítica (IIC) nacionales y los servicios esenciales del Estado y desarrollar capacidades en ciber inteligencia que permitan obtener información útil y oportuna de las amenazas presentes en ciberespacio para la toma de decisiones

5. Habilidades y capacidades de ciberseguridad: mejorar y ampliar las habilidades y capacidades cibernéticas de la nación en todos los niveles

6. Cooperación internacional: maximizar los beneficios de la cooperación internacional

En relación con cada pilar, se identifica un resumen de la importancia de la ciberseguridad, la situación actual y los problemas y desafíos prioritarios que hay que abordar, con los objetivos estratégicos y las líneas de acción que acompañan a las medidas y tareas que hay que cumplir.

Por último, se elaborará un Plan de Acción para identificar las acciones concretas que se van a llevar a cabo para alcanzar los objetivos estratégicos marcados, indicando las entidades responsables de cada acción, los periodos y fechas de cada objetivo, los indicadores clave de rendimiento, y los recursos necesarios que se van a comprometer para llevarlos a cabo.

Los objetivos y líneas de acción propuestos consideran las evaluaciones de ciberseguridad realizadas en colaboración de diversos actores de ciberseguridad de Ecuador, incluyendo el Gobierno nacional, el sector privado, la academia y la sociedad civil, con el apoyo y experiencia de expertos internacionales en ciberseguridad. Se han perfeccionado con el propósito de definir un conjunto necesario y alcanzable de actividades prioritarias para mejorar fundamentalmente la resiliencia cibernética y la postura de ciberseguridad de Ecuador.

PILAR 1:
GOBERNANZA Y COORDINACIÓN NACIONAL

Objetivo 1.1: Establecer un marco integral de gobernanza de la ciberseguridad

Objetivo 1.2: Fomentar una comunidad sólida y articulada con expertos en ciberseguridad de las múltiples partes interesadas

Objetivo 1.3: Desarrollar un marco legal y regulatorio integral que permita la gobernanza nacional de la ciberseguridad y la ciberdefensa

PILAR 2:
RESILIENCIA CIBERNÉTICA

Objetivo 2.1: Establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación para afrontar crisis cibernéticas con el fin de fortalecer dichas capacidades a nivel nacional

Objetivo 2.2: Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de infraestructuras de información crítica nacionales

Objetivo 2.3: Continuar desarrollando capacidades de respuesta y gestión de incidentes cibernéticos y del CERT nacional

Objetivo 2.4: Maximizar el uso de tecnologías avanzadas y la innovación en el diseño de políticas y procesos ágiles para el desarrollo de capacidades de Ciberinteligencia

PILAR 3:
PREVENCIÓN Y COMBATE A LA CIBERDELINCUENCIA

Objetivo 3.1: Actualizar el marco legal y regulatorio de Ecuador en materia de ciberdelincuencia para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio

Objetivo 3.2: Fortalecer la respuesta oportuna y las capacidades operacionales de investigación y judicialización de la cibercriminalidad.

PILAR 4:
CIBERDEFENSA

Objetivo 4.1: Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano para alcanzar la actitud estratégica defensiva definida en la Política de la Defensa Nacional, para la protección de la infraestructura crítica digital (ICD) y servicios esenciales en el ciberespacio.

PILAR 5:
HABILIDADES Y CAPACIDADES DE CIBERSEGURIDAD

Objetivo 5.1: Mejorar y ampliar la concientización sobre la ciberseguridad a todos los niveles de la sociedad

Objetivo 5.2: Reforzar las habilidades en materia de ciberseguridad necesarias con las múltiples partes interesadas

Objetivo 5.3: Asegurar que el sistema educativo imparta conocimientos y fortalezca habilidades en materia de ciberseguridad

PILAR 6:
COOPERACIÓN INTERNACIONAL

Objetivo 6.1: Identificar las prioridades internacionales de Ecuador y desarrollar la capacidad de participar en la ciberdiplomacia regional e internacional

Objetivo 6.2: Fortalecer la participación de Ecuador en la cooperación bilateral, regional e internacional en respuesta a las amenazas en el ciberespacio

FIGURA: Pilares y objetivos de la Estrategia Nacional de Ciberseguridad del Ecuador

PILAR 1

GOBERNANZA Y COORDINACIÓN NACIONAL

Relevancia y **estado actual**

La sólida colaboración y gobernanza de la ciberseguridad estratégica y operativa de Ecuador son esenciales para construir un ecosistema donde los ciberataques no puedan paralizar la economía nacional, causen el menor impacto posible a las entidades y la sociedad de Ecuador y dejen todos los esfuerzos de digitalización ineficientes y expuestos a un mayor riesgo de ciberseguridad. Así, Ecuador aspira a integrar la ciberseguridad como un elemento prioritario e integral del desarrollo digital del país que se implementa mediante un enfoque sólido y coordinado de la gobernanza nacional.

Si bien esta estrategia constituye la primera Estrategia Nacional de Ciberseguridad del Ecuador, en los últimos años se han producido avances significativos en la gobernanza operacional y estratégica de la ciberseguridad. Sin embargo, la ciberseguridad aún no tiene la prioridad suficiente y no se han adoptado medidas proactivas para introducir mejoras estratégicas y obtener mejores resultados.

En la esfera de la gobernanza y la coordinación de la ciberseguridad, hemos identificado que existe la oportunidad de redefinir una visión estratégica nacional con objetivos estratégicos claros, junto con un plan de acción para garantizar que se realicen esfuerzos y progresos centrados en el desarrollo de la ciberseguridad nacional. Actualmente no existe un marco general de gobernanza de la ciberseguridad a nivel nacional, así como roles, funciones y responsabilidades claras y un plan de cooperación. Esto plantea un desafío para la participación activa y efectiva de las múltiples partes interesadas y las alianzas entre el sector público y el privado a nivel estratégico y operacional. Es necesario revisar el marco legal y regulatorio general relacionado con el entorno digital y las medidas de ciberseguridad en Ecuador, ya que este es un aspecto crítico para garantizar la eficacia de la gobernanza general en todos los sectores relevantes.

OBJETIVOS ESTRATÉGICOS

Para hacer frente a los retos planteados, se perseguirán en este pilar los tres siguientes objetivos estratégicos junto con las acciones respectivas.

Objetivo 1.1:

Establecer un marco integral de **gobernanza de la ciberseguridad**

La Estrategia Nacional de Ciberseguridad y su plan de implementación irán acompañados de un sólido marco de gobernanza para entidades del sector público, privado y

otros sectores relevantes del país, que incluye un examen periódico de implementación del plan, ajustes ágiles durante el período de la estrategia y un ciclo de vida completo previsto con la experiencia adquirida en el nuevo período de la estrategia. La planificación estratégica y el seguimiento se apoyarán en la supervisión cuantitativa del panorama de riesgos de ciberseguridad y los progresos mediante mediciones e indicadores clave, que luego se incorporarán a los procesos nacionales de adopción de decisiones estratégicas y permitirán una asignación optimizada de los recursos para garantizar los progresos con una perspectiva clara ponderada por el riesgo. Los objetivos estratégicos se cubrirán mediante la planificación presupuestaria tanto en términos de gastos de funcionamiento como de inversiones específicas, incorporando el presupuesto nacional y los mecanismos de apoyo.

Líneas de acción

- Establecer un marco institucional con los roles, funciones y responsabilidades prescritas de todos los agentes gubernamentales pertinentes en materia de seguridad integral o seguridad del Estado en la cual se encuentra inmersa la ciberseguridad que abarque todos los objetivos estratégicos de la estrategia nacional.
- Establecer al Comité Nacional de Ciberseguridad como el órgano estratégico de coordinación y toma de decisiones junto con términos de referencia claros que describan su composición, tareas principales y procedimientos de toma de decisiones, que incorpore los mandatos individuales de los miembros del Comité.
- Fortalecer el rol de coordinador nacional de políticas de ciberseguridad en el Comité Nacional de Ciberseguridad.
- Establecer una visión holística para la asignación de recursos para el cumplimiento de los objetivos estratégicos de la estrategia nacional de acuerdo con el plan de implementación, que será supervisado por el Comité Nacional de Ciberseguridad. El presupuesto incluiría los gastos ordinarios, la incorporación en el presupuesto nacional y también la asignación específica de recursos para proyectos o iniciativas, financiados por programas especiales. Las fuentes de financiación podrían ser internas o de donantes internacionales.
- Establecer un mecanismo de seguimiento y control de indicadores clave de rendimiento y de gestión de riesgos de ciberseguridad a fin de identificar oportunidades de mejora de la ciberseguridad a nivel nacional.

Objetivo 1.2:

Fomentar una comunidad sólida y articulada con expertos en **ciberseguridad de las múltiples partes interesadas**

La gobernanza de la ciberseguridad se establecerá mediante una coordinación inclusiva de las actividades del Comité Nacional de Ciberseguridad con todas las múltiples partes interesadas pertinentes, incluidas las entidades gubernamentales, el sector privado, las Organizaciones No Gubernamentales -ONG-, la sociedad civil y el mundo académico. Los roles, funciones y responsabilidades se definirán claramente y se combinarán con instrumentos y capacidades operacionales. Esa comunidad activa, comprometida y bien organizada garantizará el intercambio de conocimientos y la cooperación para fomentar la capacidad y propiciar el desarrollo estratégico. Por otra parte, junto con los ejercicios prácticos conjuntos y las redes de intercambio, se crearían capacidades plenas y mejores expertos que podrían participar rápidamente en la cooperación operacional durante una potencial grave crisis cibernética.

Líneas de acción

- Establecer un mecanismo eficaz de asociación entre el sector público y el privado en el que participen todas las múltiples partes interesadas pertinentes de las instituciones gubernamentales, el sector privado, el mundo académico y las ONG, a fin de proporcionar una plataforma para la participación, en relación con la siguiente aportación de valor práctico:
- a. consulta y recopilación de información;
- b. intercambio de información;
- c. coordinación de actividades;
- d. cooperación operativa.

Objetivo 1.3:

Desarrollar un marco legal y regulatorio integral que permita la **gobernanza nacional de la ciberseguridad y la Ciberdefensa**

Se establecerá una estructura legal y regulatoria integral, transparente y actualizada de normas y reglamentos de ciberseguridad sobre la base de un análisis legislativo integral. El establecimiento de disposiciones jurídicas no debe considerarse un objetivo en sí mismo, sino más bien una comprensión óptima de las necesidades que se abordan en todos los objetivos estratégicos de la estrategia nacional, al tiempo que se evita la tendencia a una reglamentación excesiva para garantizar el principio de proporcionalidad considerando criterios metodológicos mediante los cuales se establezcan claramente los respectivos deberes y derechos. Un entorno jurídico que complemente el ecosistema de la ciberseguridad apoyará las opciones estratégicas y constituirá un instrumento para la aplicación de la Estrategia Nacional de Ciberseguridad.

Las disposiciones jurídicas específicas que deben establecerse se detallan en relación con cada objetivo estratégico. Las áreas prioritarias que necesitan claridad adicional en el marco legal y regulatorio han sido identificadas como:

- Ciberseguridad Nacional
- Infraestructuras críticas digitales (ICD) (detallado en el Objetivo 2.2)
- Gestión de incidentes cibernéticos (detallado en el Objetivo 2.3)
- Ciberdelincuencia (detallado en el Objetivo 3.1)

Líneas de acción

- Efectuar un análisis exhaustivo del marco legal y regulatorio vigente en todo el ámbito de la ciberseguridad para evaluar la exhaustividad y la claridad, determinar las “lagunas legales” y aclarar cualquier necesidad adicional de adopción y armonización de la legislación y los reglamentos.
- Utilizar los resultados de este análisis para:
  - Establecer de manera integral los roles y responsabilidades de los ministerios y otras agencias en ciberseguridad nacional dentro del marco legal y regulatorio de la seguridad integral del Estado.
  - Orientar los cambios legislativos necesarios para el cumplimiento de los objetivos estratégicos de la estrategia nacional.

PILAR 2

RESILIENCIA CIBERNÉTICA

La resiliencia cibernética nacional necesita establecer las líneas de acción necesarias para desarrollar la capacidad de prepararse, responder y recuperarse de crisis cibernéticas que podrían afectar a la prestación de los servicios. Esto significa realizar una identificación y gestión adecuadas de riesgos de ciberseguridad; suficiente preparación y capacidad de respuesta frente a los ciberataques para que su impacto permanezca controlado; y, en particular, la protección de las infraestructuras críticas y los servicios esenciales. Así, la resiliencia cibernética está cubierta por tres objetivos estratégicos que abordan:

1. Gestión de riesgos de ciberseguridad y preparación ante crisis cibernéticas
2. Protección de infraestructuras críticas
3. Gestión de incidentes cibernéticos

OBJETIVOS ESTRATÉGICOS

Gestión de riesgos de **ciberseguridad** y preparación para crisis cibernéticas

Relevancia y estado actual

La gestión de riesgos es una parte natural de cualquier actividad de desarrollo, incluida la transformación digital, que aporta multitud de beneficios en innovación, competitividad de la industria, desarrollo socioeconómico y calidad de los servicios gubernamentales, pero también introduce nuevas y complejas amenazas y perfil de riesgo. Un mayor nivel de dependencia digital, junto con un panorama de amenazas externas cada vez más complejo, conduce a una mayor vulnerabilidad a los incidentes cibernéticos causados por criminales, hacktivistas y otros Estados, a menos que los riesgos de ciberseguridad se gestionen adecuadamente. Además de los riesgos de ciberseguridad, también el daño físico a los activos de información, por ejemplo, a través de desastres naturales, puede llevar a la interrupción de los sistemas de información y servicios digitales que afectan a toda la sociedad ecuatoriana.

Las amenazas y los riesgos de ciberseguridad son de carácter mundial, y cada país se enfrenta a sus propias peculiaridades, derivadas del nivel de dependencia digital, la posición geopolítica, la estructura de las ICD nacionales, entre otras. A fin de identificar y gestionar eficazmente los riesgos de ciberseguridad, es esencial establecer un seguimiento continuo de las tendencias mundiales y comprender la perspectiva nacional de las amenazas en el ciberespacio. Una imagen clara del perfil de riesgo general permite tomar decisiones informadas y ponderadas por riesgo.

En la actualidad, se considera que la capacidad de respuesta de las personas y las organizaciones en Ecuador tiene una oportunidad de mejora en lo que respecta a la capacidad para resistir a los agentes adversos, teniendo en cuenta, por ejemplo, los ataques DDoS (ataques de denegación distribuida de servicios) que ha sufrido el país. Por lo tanto, Ecuador necesita fortalecer su capacidad para hacer frente a los nuevos tipos de ciberataques y ciberdelincuencia, a nivel nacional y transnacional, sobre la base de un enfoque de gestión de riesgos de ciberseguridad.

En el ámbito de la gestión de riesgos de ciberseguridad y la preparación para las crisis cibernéticas, hemos identificado áreas de mejora, incluido el hecho de que actualmente se debe reforzar de manera práctica a nivel nacional las evaluaciones de riesgos de ciberseguridad, supervisión, presentación de informes y auditoría del estado del riesgo. La adopción de un marco nacional amplio de gestión de riesgos de ciberseguridad brinda la oportunidad de establecer un enfoque basado en estos riesgos para la planificación de la capacidad de ciberseguridad a nivel nacional a fin de lograr una asignación óptima de los recursos. En la actualidad, existe la oportunidad de aumentar y reforzar la preparación para hacer frente a las crisis cibernéticas, incluidos los problemas de cooperación eficiente, intercambio de información y rutinas de escalada. El establecimiento, la prueba y el ejercicio de escenarios de riesgo de ciberseguridad pertinentes pueden proporcionar una base para planes de contingencia eficaces y capacidad de ejecución.

Objetivo 2.1:

Establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación para las **crisis cibernéticas con el fin de fortalecer dichas capacidades a nivel nacional**

Se establecerá la capacidad para identificar, analizar, evaluar y tratar los riesgos de ciberseguridad, así como para la evaluación continua, el seguimiento y la supervisión de las medidas de gestión y mitigación. Se elaborará un enfoque basado en estos riesgos para la planificación y el desarrollo de la ciberseguridad a nivel nacional, de modo que la aplicación de las medidas e inversiones en

ciberseguridad se basen en la priorización según el perfil de riesgo nacional.

Se establecerán planes de gestión de crisis cibernéticas en las instituciones gubernamentales y se motivará la colaboración del sector privado, apoyados en los formatos de asociación público-privada. Una crisis cibernética debe entenderse como el resultado de un evento o una cadena de eventos que provocan la interrupción de una operación crítica o de ICD nacionales que, a su vez, pone en riesgo la vida o la salud de muchas personas, provoca daños patrimoniales y ambientales importantes o interferencias severas y extensas en la continuidad de los servicios u operaciones viales, y cuya resolución requiere la pronta actuación coordinada. Se establecerán y adelantarán rutinas de ejercicio para practicar la gestión de situaciones de incidentes cibernéticos y crisis cibernéticas mediante pruebas de recuperación en caso de fallo, a fin de garantizar una comprensión clara de las capacidades técnicas, las líneas de comunicaciones y las rutinas de escalada.

Líneas de acción

- Adoptar un marco para el gobierno de la ciberseguridad basado en la gestión del riesgo.
- Establecer a nivel nacional el informe sobre el Panorama de Amenazas y Riesgos y monitoreo continuo, consolidando diversas fuentes de información nacionales e internacionales, incluyendo tipos comunes de ciberataques dirigidos a las ICD nacionales e instituciones gubernamentales.
- Establecer mecanismos independientes de control que incluyan la evaluación de gobierno, riesgo y pruebas periódicas de penetración para las organizaciones del sector público y los operadores de las IC.
- Identificar los operadores de servicios de telecomunicaciones para la respuesta y comunicación de emergencia.
- Crear un programa de coordinación designado para la adopción de normas de ciberseguridad y mejores prácticas tanto para los organismos gubernamentales de manera obligatoria, como para las contrapartes pertinentes del sector privado de manera voluntaria.
- Promover la creación de normas y la adaptación o adopción de mejores prácticas que hagan factible la cooperación entre las partes interesadas responsables de la ciberseguridad.
- Identificar escenarios de riesgo de ciberseguridad para los cuales se deben desarrollar planes nacionales de contingencia.
- Organizar ejercicios nacionales de ciberseguridad para probar las capacidades del personal involucrado en la ciberseguridad de las organizaciones.
- Realizar pruebas que involucren los escenarios de contingencia establecidos por las organizaciones.

Protección de Infraestructuras Críticas Digitales (ICD)

Relevancia y estado actual

La protección de infraestructuras críticas y servicios esenciales no es en sí misma una tarea nueva. A nivel regional, el Comité Interamericano contra el Terrorismo (CICTE) de la OEA define la infraestructura de información crítica como instalaciones, sistemas y redes, así como servicios, equipo físico y tecnología de la información para los cuales la falta de un funcionamiento continuo tiene un impacto negativo significativo en la población, la salud pública, la seguridad nacional, la actividad económica o el funcionamiento eficiente del Estado.

En la actualidad, la mayoría de las infraestructuras críticas y servicios esenciales, tanto públicos como privados, dependen de la tecnología de la información y son vulnerables a las violaciones o fallos de la ciberseguridad en los sistemas de información. Las ICD se definen como una parte de las infraestructuras nacionales pudiendo ser sistemas físicos o virtuales que facilitan funciones y servicios esenciales para apoyar a los sistemas más básicos a nivel social, económicos, medioambientales y políticos.

- Servicio esencial: "Es el servicio necesario para el mantenimiento de la funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas."

- Infraestructura Crítica: "Son las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales."

- Infraestructura Estratégica: "Infraestructura Estratégica: Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales."

La protección de la IC debe proveer los mecanismos necesarios para evitar que un fallo o evento inesperado en el uso de las TICs, pueda causar interrupciones, lo que tendría graves consecuencias para la sociedad y la economía.

En el ámbito de la protección de las ICD nacionales, hemos identificado ámbitos de oportunidad que debemos abordar, como la necesidad de elaborar una lista completa de todos los operadores de ICD nacionales y establecer normas nacionales, ya que la falta de esta lista plantea un desafío para establecer mecanismos eficientes de apoyo, intercambio de información y supervisión. Además, para garantizar la protección de las ICD nacionales, el establecimiento y mantenimiento de un catálogo actualizado de todos los operadores de las ICD nacionales es la base para permitir otros esfuerzos de mejora que garanticen una resiliencia cibernética suficiente. La protección de las ICD nacionales no está actualmente cubierta de forma exhaustiva por el marco jurídico, lo que plantea un desafío para la aplicación de los principios de seguridad y la supervisión normativa para garantizar el cumplimiento. El examen y la finalización del marco legal y regulatorio de conformidad con las orientaciones del análisis jurídico general y las mejores prácticas internacionales permitirán establecer mecanismos eficaces de protección de las ICD nacionales en el marco de las asociaciones entre los sectores público y privado y establecer una comunidad sólida entre los profesionales para cubrir asuntos tanto de ciberseguridad como de Ciberdefensa, promoviendo el intercambio de conocimientos, mejores prácticas y una red de cooperación consolidada de expertos.

Objetivo 2.2:

Adoptar un marco integral para la identificación, orientación y **supervisión de los operadores de Infraestructuras Críticas Digitales (ICD)**

Se identificarán los activos de las ICD tanto del sector público como del privado, que son esenciales para mantener las funciones vitales de la sociedad en el Ecuador y que se prepararán para enfrentar las amenazas actuales y emergentes dentro del entorno digital, minimizando su posible impacto.

Se establecerá y mantendrá un catálogo actualizado de todos los operadores de las ICD nacionales para garantizar la recopilación y administración de datos relativos a las ICD nacionales y mecanismos amplios de colaboración y cooperación. A fin de establecer un nivel suficiente de medidas de seguridad aplicadas, se seleccionarán normas de referencia, directrices de apoyo y mecanismos de supervisión. Un marco legal y regulatorio complementario apoyará los mecanismos de identificación, gestión de riesgos de ciberseguridad, supervisión y comunicación de las ICD nacionales.

Líneas de acción

Identificación e intercambio de información

- Documentar una metodología clara para la identificación de las ICD nacionales basada en consideraciones sociales, económicas y ambientales.
- Establecer y mantener una lista actualizada de las ICD nacionales junto con la definición de sectores estratégicos que contempla el concepto de protección de servicios e infraestructura esenciales.
- Establecer un mecanismo de cooperación y coordinación mediante asociaciones público-privadas entre todos los operadores de las ICD nacionales para apoyar el fomento de la confianza.

Norma de referencia, directrices y supervisión

- Establecer normas nacionales que consideren como referencia a estándares y mejores prácticas internacionales que se apliquen a todos los operadores de las ICD nacionales tanto en operadores de ICD del sector privado como en activos de ICD dentro de las instituciones gubernamentales.
- Emitir directrices e instrucciones para apoyar la aplicación de medidas de seguridad y lograr el cumplimiento de la norma de referencia.
- Establecer la configuración de la estrategia de auditoría de seguridad de la información.

Marco jurídico y normativo

- Definir los roles y responsabilidades a nivel nacional para la coordinación de la identificación y el seguimiento de las ICD nacionales dentro del marco legal y regulatorio.
- Establecer requisitos de ciberseguridad para los operadores de ICD nacionales en el marco legal y regulatorio, cuando se considere pertinente.

Gestión de incidentes cibernéticos

Relevancia y estado actual

En los últimos años, Ecuador ha dado pasos considerablemente notables para fortalecer sus capacidades de gestión de incidentes cibernéticos. El Equipo del Centro de Respuesta a Incidentes de Seguridad Nacional (EcuCERT), que opera bajo la Agencia para la Regulación y Control de las Telecomunicaciones (ARCOTEL) y se rige por la Ley Orgánica de Telecomunicaciones, es reconocido como un punto de contacto nacional e internacional en la coordinación de la respuesta de gestión de incidentes cibernéticos. Sin embargo, su circunscripción a nivel nacional se limita a los operadores de redes de telecomunicaciones y, por lo tanto, actualmente EcuCERT no tiene mandato ni competencias suficientes para operar íntegramente a nivel gubernamental. En el ámbito internacional, EcuCERT es un socio activo de la comunidad de CSIRTAmericas de la OEA, FIRST (Forum of Incident Response and Security Teams por sus siglas en inglés) y también tiene una relación de colaboración y dinámica con los CERT regionales.

Además de EcuCERT, las competencias de gestión de incidentes cibernéticos se complementan con numerosos CERT o CSIRT operativos en los sectores académico, privado y financiero. En el ámbito de la defensa, la gestión de incidentes cibernéticos se encomienda al CERT militar, dependiente del Comando de Ciberdefensa (COCIBER), cuyo objetivo es la protección de las ICD y la soberanía. Los CERT sectoriales han establecido relaciones de cooperación con sus homólogos internacionales con la posibilidad de colaborar en caso de incidentes cibernéticos transfronterizos.

A pesar de los esfuerzos realizados hasta ahora, EcuCERT no tiene un mandato claro para gestionar actualmente como un CERT nacional. Además, hay sectores económicos que no han establecido sus equipos de respuesta y, por lo tanto, no tienen una instancia para reaccionar a los incidentes cibernéticos de manera centralizada y coordinada. Además, no existe un enfoque unificado para la notificación de estos incidentes y los mecanismos son variables entre los CERT.

En el ámbito de la gestión de incidentes cibernéticos, se ha identificado ámbitos de oportunidad. También se aprecia que la legislación actual limita las acciones de EcuCERT a estar fuera del ámbito de las telecomunicaciones y esto debe revisarse y actualizarse en consecuencia. Además, tampoco existen controles para establecer una visibilidad de los eventos de ciberseguridad en la red de servicios gubernamentales. El marco nacional de gestión de incidentes cibernéticos debe proporcionar disposiciones de trabajo nacionales claramente definidas para el intercambio de información y la respuesta a estos incidentes, ya que la falta de un marco de apoyo plantea un riesgo para la protección adecuada de los activos de las ICD nacionales en el país. Se deben realizar esfuerzos para formalizar los mecanismos de coordinación y notificación de incidentes cibernéticos a nivel nacional, ya que se trata de un elemento clave de una respuesta bien estructurada y organizada a estos incidentes.

Objetivo 2.3:

Continuar desarrollando capacidades de respuesta y gestión de incidentes **cibernéticos y del CERT nacional**

Para fortalecer la estabilidad y seguridad del ecosistema digital, seguiremos desarrollando resiliencia cibernética tanto a nivel nacional como organizacional para prepararnos, responder y recuperarnos de los incidentes cibernéticos, así como gestionar las crisis cibernéticas de manera oportuna, eficaz y coordinada.

Líneas de acción

- El ente rector en Seguridad de la Información debe adoptar una normativa que establezca un CERT nacional, sus funciones y responsabilidades y mecanismos de supervisión para incluir la vigilancia de incidentes cibernéticos a nivel nacional, proporcionando medidas preventivas y reactivas como alertas tempranas, anuncios y difundiendo información sobre amenazas a las partes interesadas pertinentes, proporcionando análisis periódicos de riesgos de ciberseguridad e incidentes cibernéticos y coordinando la respuesta a nivel nacional.

- Habilitar procesos, herramientas y conocimientos para gestionar las amenazas e incidentes cibernéticos en la red gubernamental a fin de mejorar las capacidades. Con ese fin, Ecuador trabajará para establecer un Centro de Operaciones de Seguridad (gubernamental) nacional (GSoC) con una misión clara basada en un mandato.

- Revisar y establecer el marco jurídico necesario con competencias y tareas claras para cada una de las partes interesadas, además de estable-

cer informes de incidentes cibernéticos obligatorios para permitir modelos nacionales armonizados de gestión de incidentes cibernéticos.

- Invertir en maximizar las asociaciones dentro de comunidades CERT más amplias, particularmente a entidades públicas y privadas, con ejercicios y programas de capacitación sobre prevención, respuesta y recuperación de incidentes cibernéticos.

- Establecer un mecanismo para la emisión periódica de alertas correspondientes a eventos de seguridad, vulnerabilidades y el intercambio de información entre los operadores de las ICD nacionales y el gobierno de Ecuador.

Objetivo 2.4:

Maximizar el uso de tecnologías avanzadas y la innovación en el diseño de **políticas y procesos ágiles para el desarrollo de capacidades de Ciberinteligencia**

Líneas de acción

- Establecer las capacidades del Centro de Operaciones de Seguridad (GSoC) nacional (gubernamental) a través de esquemas de detección, investigación y herramientas que permitan identificar amenazas y mitigar riesgo en el ciberespacio, apoyando en la respuesta a incidentes para garantizar la resiliencia de las ICD nacionales, los servicios estatales esenciales.

- Articular y coordinar acciones conjuntas con los responsables de la ciberseguridad y ciberdefensa para el desarrollo de normativas y fortalecimiento interinstitucional que permita proteger el ciberespacio.

- Desarrollar un observatorio del ciberespacio para recopilar, analizar y clasificar la información sobre amenazas e incidentes cibernéticos que se utiliza para proporcionar a las empresas una visión procesable para identificar, medir y clasificar las vulnerabilidades y mitigar los riesgos cibernéticos.

- Desarrollar un sistema de alerta temprana para compartir información de amenazas detectadas, ayudando a instituciones públicas y privadas en la prevención y anticipación de ciberataques.

- Asesorar la toma de decisiones al más alto nivel del Estado sobre la situación de amenazas digitales presentes en el ciberespacio que puedan comprometer la seguridad del Estado.

- Invertir en el desarrollo de capacidades de planificación de ejecución de operaciones cibernéticas a través de detección y respuesta avanzadas a nivel táctico, estratégico y operativo.

PILAR 3

PREVENCIÓN Y COMBATE A LA CIBERDELINCUENCIA

Relevancia y **estado actual**

La creciente popularidad y uso de soluciones digitales innovadoras lleva a grupos criminales a intentar monetizar estos servicios y plataformas para obtener ganancias ilícitas. La pandemia de COVID-19 ha acelerado este proceso debido a que muchas más transacciones y actividades se realizan en línea. El número de delitos cibernéticos está aumentando en Ecuador, lo que representa una proporción cada vez mayor del total de delitos registrados. En los últimos tres años, el número de delitos cibernéticos denunciados se ha doblado. Esto sigue una tendencia común de otros países de la región y a nivel mundial, ya que la ciberdelincuencia es intrínsecamente de naturaleza transnacional. El delito cibernético también está aumentando en sofisticación técnica, complejidad y grado de organización.

De acuerdo con la evaluación de la Policía Nacional de Ecuador, la escasa alfabetización digital y la escasa conciencia de la población en materia de ciberseguridad inducen a la población a ser víctima de la ciberdelincuencia. Además, las víctimas de delitos cibernéticos no siempre son conscientes de que sus activos se han visto comprometidos; y aunque lo hagan, existe un desconocimiento generalizado sobre cómo denunciar este tipo de delitos. A menudo, no se confía en que la aplicación de la ley pueda ayudar, ya que la investigación y el enjuiciamiento pueden demorar debido a las capacidades limitadas de las autoridades encargadas. Consecuentemente, todos estos factores conducen a que a menudo el delito cibernético no se denuncie. Así mismo, los datos del Ministerio de Gobierno muestran que el fraude informático, el robo de identidad y la violación de datos personales son los delitos cibernéticos más comunes que afectan a los ecuatorianos. De los delitos relacionados con el contenido, la pornografía infantil es la principal preocupación. Las definiciones legales de delito cibernético del marco legal actual pueden considerarse como desactualizadas, lo cual muestra el área de oportunidad que existe para su mejora.

No obstante, Ecuador está haciendo esfuerzos para mejorar su capacidad para hacer frente al delito cibernético mediante la cooperación internacional, ya que se encuentra actualmente en proceso de adhesión al Convenio de Budapest sobre la Ciberdelincuencia, que permitirá armonizar leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación con otras naciones firmantes. El proceso de adhesión requiere la aplicación de las disposiciones del Convenio en la legislación nacional de Ecuador. Ecuador es miembro de AMERIPOL e INTERPOL, con acceso a intercambio de información en tiempo real. Adicionalmente, la Unidad Nacional de Ciberdelitos, que se encuentra bajo la estructura orgánica de la Dirección General de Investigación de la Policía Nacional de Ecuador, tiene más de una década de existencia y ha adquirido una notable especialización en el campo de la investigación digital, pero carece de logística y recursos humanos que le permitan evolucionar de forma sostenible. De igual manera Ecuador es miembro de AMERIPOL e INTERPOL, con acceso a intercambio de información en tiempo real.

En la esfera de la lucha contra la ciberdelincuencia, hemos identificado esferas que es posible abordar. Por ejemplo, el marco sustantivo y procesal puede actualizarse para prevenir, investigar y enjuiciar eficazmente el delito cibernético como amenaza creciente. La aplicación de la ley no puede actuar sin una base jurídica clara, por lo que deben definirse claramente las funciones y los mandatos establecidos de los diversos agentes encargados de combatir la ciberdelincuencia (la policía, la fiscalía y el sistema judicial). Además, dado el creciente volumen y el impacto de la ciberdelincuencia, la capacidad de los organismos encargados de hacer cumplir la ley no se ha mantenido al mismo nivel, con escasez de personal cualificado en el sistema policial y judicial y falta de un presupuesto específico. Para hacer un uso más eficiente de los recursos, también tendremos que trabajar de forma más inteligente racionalizando los procesos y mejorando las herramientas forenses digitales de las fuerzas del orden.

OBJETIVOS ESTRATÉGICOS

Para fortalecer la resiliencia cibernética de Ecuador contra los actores criminales que abusan del ciberespacio se implementarán acciones en dos áreas: i) actualización de la legislación sobre ciberdelincuencia en lo que respecta a la legislación sustantiva y procesal, y ii) fortalecimiento de la capacidad policial y judicial para prevenir, investigar y perseguir la ciberdelincuencia. Las medidas para mejorar la sensibilización sobre la denuncia de incidentes cibernéticos y delitos cibernéticos se abordan en el pilar 5 de esta estrategia nacional; las acciones relativas a la cooperación internacional de las fuerzas del orden se tratan en el marco del pilar 6.

Objetivo 3.1:

Actualizar el marco legal y regulatorio de Ecuador en materia de ciberdelincuencia para **garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio**

Líneas de acción

- Revisar el derecho penal existente y armonizar la normativa legal relacionada con los delitos cibernéticos y los delitos conexos (delitos contra o por medio de los sistemas informáticos o datos informáticos), considerando la armonización con los instrumentos jurídicos internacionales y regionales existentes.
- Revisar y ajustar la normativa legal relacionada con el mandato legal y la autoridad de las fuerzas del orden, las autoridades ejecutivas y los proveedores de servicios digitales a los efectos de la prevención del delito cibernético.
- Revisar y ajustar la normativa legal relacionada con las facultades y procedimientos adecuados para la aplicación de la ley, el enjuiciamiento y la judicialización para la investigación de delitos cibernéticos, incluida la recopilación y el procesamiento de pruebas electrónicas y de instrumentos.
- Establecer y aplicar instrumentos para una cooperación internacional rápida y eficaz en casos de delitos cibernéticos.
- Unirse a los mecanismos internacionales y regionales de coordinación y cooperación para combatir el delito cibernético a través del intercambio de información, investigaciones transfronterizas, operaciones, y fortalecimiento de habilidades y capacidades técnicas.

Objetivo 3.2:

Fortalecer la respuesta oportuna y las capacidades operacionales de **investigación y judicialización de la cibercriminalidad.**

Líneas de acción

- Fortalecer la unidad o unidades especializadas en ciberdelitos de la Policía Nacional de Ecuador con las capacidades logísticas, humanas y forenses digitales adecuadas, asegurando procedimientos investigativos regulados a nivel nacional.
- Fomentar la creación de programas de apoyo a la persecución penal y prevención de los delitos cibernéticos, mediante la colaboración y participación ciudadana, promoviendo canales oficiales de denuncia y el desarrollo de campañas de prevención de la ciberdelincuencia.
- Facilitar la creación de Direcciones o Unidades de Prevención de Delitos Cibernéticos especializadas, con personal profesional especializado en el campo de la informática y el derecho, así como con procedimientos preventivos estándar y mecanismos de denuncia de delitos cibernéticos, eficientes para la sociedad ecuatoriana.
- Determinar y desarrollar oportunidades de capacitación y proporcionar formación a los funcionarios encargados de hacer cumplir la ley y a los especialistas forenses sobre el derecho relativo al delito cibernético y su aplicación, incluida la salvaguarda de los derechos humanos y la colaboración con los órganos internacionales encargados de hacer cumplir la ley.
- Motivar la creación y fortalecimiento de unidades especializadas en delito cibernético a nivel nacional, en la Fiscalía General del Estado y Consejo Nacional de la Judicatura con personal profesional especializado en el campo de la informática y el derecho, contribuyendo a la adecuada administración de justicia.
- Identificar y proporcionar oportunidades de capacitación a los profesionales de la justicia penal (fiscales, jueces, abogados y otros especialistas pertinentes) sobre el delito cibernético, herramientas tecnológicas y manejo de evidencia electrónica.
- Impartir formación a los agentes del orden y a los especialistas forenses sobre la legislación en materia de ciberdelincuencia y su aplicación, incluida la protección de los derechos digitales y la colaboración con los organismos internacionales encargados de hacer cumplir la ley.

PILAR 4

CIBERDEFENSA

La **Ciberdefensa**

LA CIBERDEFENSA COMO PARTE DE LA CIBERSEGURIDAD NACIONAL Y SU ARTICULACIÓN CON **LAS INSTITUCIONES QUE CONFORMAN EL COMITÉ NACIONAL DE CIBERSEGURIDAD.**

El ciberespacio constituye un nuevo dominio para la defensa de la soberanía, integridad territorial y la seguridad del Estado, junto a los dominios tradicionales: tierra, mar, aire y espacio. En este entorno virtual, las naciones modernas, desarrollan actividades económicas, productivas y sociales, promovidas por el acelerado desarrollo tecnológico generando vulnerabilidades que pueden ser explotadas por amenazas, que pueden causar efectos estratégicos sobre la estructura, estabilidad, institucionalidad, gobernabilidad, así como, alterando la paz colectiva y la soberanía del Estado. (Estrategia de Ciberdefensa 2021).

El plan específico de la Defensa Nacional (PED) 2019-2030, reconoce al ciberespacio como un componente más del territorio ecuatoriano, considerado como un nuevo dominio en el cual se desarrollan actividades de Ciberdefensa para la protección de la infraestructura crítica digital y servicios esenciales del Estado, aportando con ello a la seguridad digital nacional.

La guía política estratégica de Ciberdefensa 2021, menciona que la defensa comprende las medidas que permiten resguardarnos de riesgos, amenazas, peligros y daños; por lo que, estar o sentirse seguro implica no solo la protección y conservación, sino también unas capacidades de respuesta. En este sentido, la Ciberdefensa se conceptualiza como la capacidad militar, intelectual y tecnológica que poseen las Fuerzas Armadas, para ejecutar operaciones en o través del ciberespacio, que permitan defender y responder a los ciberataques a la infraestructura crítica e información estratégica del Estado, así como apoyar el cumplimiento de operaciones en los otros dominios.

El Ministerio de Defensa Nacional, consciente de la necesidad de establecer objetivos y líneas de acción para avanzar en el desarrollo de capacidades de una Ciberdefensa capaz de cumplir con los objetivos estratégicos de la nación, estructuró la Estrategia de Ciberdefensa como un modelo de gestión para enfrentar las ciberamenazas que afecten a las infraestructuras críticas del Estado y servicios esenciales, así como la protección de los derechos de los ciudadanos en el ciberespacio.

El Ministerio de Defensa Nacional, como uno de sus objetivos tiene el fortalecimiento de las capacidades estratégicas conjuntas de Fuerzas Armadas; por lo que, a través del Comando Conjunto, planifica y conduce operaciones militares, entre otras, ciberoperaciones, para enfrentar las ciberamenazas de cualquier naturaleza en al marco de sus competencias; razón por lo cual, emitió la Estrategia de Ciberdefensa 2021. Esta estrategia se fundamenta en los objetivos establecidos en la Política de la Defensa, orientada a la protección efectiva de la infraestructura crítica digital y servicios esenciales de las áreas estratégicas, además de fortalecer las capacidades de Ciberdefensa, cooperación internacional y contribución al desarrollo nacional.

El control de los espacios de influencia en el combate, tanto en tierra como mar y aire, es una necesidad fundamental que tiene un Estado a través de sus Fuerzas Armadas, para cumplir la misión y ejercer el control sobre un oponente, con el fin de lograr los efectos deseados; en el ciberespacio como nuevo ámbito operacional, el control de su entorno de influencia también es necesario.

Las fuerzas armadas de un país para cumplir la misión de proteger los intereses nacionales, deben tener la capacidad de enfrentar a la amenaza allá donde se produzca, en tierra, mar, aire, espacio o ciberespacio. Para ello deben disponer de capacidades militares idóneas, que permitan combatir en el ciberespacio, con fuerzas formadas, preparadas y organizadas bajo un mando único responsable del planeamiento y la conducción de las operaciones militares.

El Ministerio de Defensa Nacional, constituye la herramienta principal a través del cual el gobierno nacional implementa la Ciberdefensa como parte de la política de defensa que, en coordinación con el resto de instrumentos del poder nacional, contribuye a la seguridad integral del

Estado ecuatoriano; en ese sentido, el Ministerio de Defensa ejercerá la rectoría de la Ciberdefensa, a través del Comando Conjunto de las Fuerzas Armadas, ente responsable de la defensa de la soberanía e integridad territorial.

RELEVANCIA Y ESTADO ACTUAL

El ciberespacio es un ámbito conceptual en donde se desarrollan actividades de Ciberdefensa; en ese sentido, la Organización de Estados Americanos (OEA), de la cual Ecuador es miembro, a través de la Junta Interamericana de Defensa (JID), emitió la Guía de Ciberdefensa, con el objetivo de orientar el diseño, planeamiento, implantación y desarrollo de la Ciberdefensa donde, entre otros aspectos, manifiesta lo siguiente:

"Reconocer al ciberespacio como otro ámbito de operaciones, enmarcado en lo establecido en la cumbre de la OTAN de Varsovia de 2016, en el punto 70 del comunicado declara: "ahora, en Varsovia, reafirmamos el mandato defensivo de la OTAN y reconocemos el ciberespacio como un dominio de operaciones en el que la OTAN debe defenderse tan efectivamente como lo hace en el aire, en tierra y en el mar". (Guía de Ciberdefensa de la Junta Interamericana de Defensa).

El ciberespacio ya no es un dominio emergente para nuestro país, este se ha constituido en el quinto dominio donde se ejecutan operaciones militares, tal como establece el Plan Específico de la Defensa. Considerar al ciberespacio como un ámbito operacional, mejorará la capacidad del Estado ecuatoriano para proteger a la sociedad de ciberamenazas y ciberataques a través de la ejecución de ciberoperaciones; por lo que, es indispensable el desarrollo de políticas conjuntamente con otros organismos públicos y privados.

La Ciberdefensa es parte de la ciberseguridad del Estado, su fin es aportar a la seguridad y defensa del Ecuador, garantizando los derechos de los ciudadanos en este dominio, como una capacidad de Fuerzas Armadas, organizada y preparada para mantener la vigilancia, control y dominio del ciberespacio, a través de actividades defensivas, de explotación (Ciberinteligencia) y ofensivas, que permitan prevenir amenazas y contrarrestar incidentes que vulneren la infraestructura critica digital y los servicios esenciales del Estado. (Estrategia de Ciberdefensa 2021).

La cooperación y coordinación nacional e internacional en el ámbito de Ciberdefensa permitirá afrontar los desafíos que se presenten en el entorno ciberespacial y neutralizar las ciberamenazas que atenten contra la seguridad de la región, mediante la colaboración mutua, el intercambio de información y buenas prácticas; así como, la investigación, desarrollo e innovación (I+D+i) en materia de Ciberdefensa por medio de ofertas académicas y ciberejercicios.

El Gobierno Nacional consciente de la importancia de defender y proteger el ciberespacio, mediante Acuerdo Ministerial No. 281, del 12 de septiembre de 2014, crea el Comando de Ciberdefensa, como un comando operacional del Comando Conjunto de las Fuerzas Armadas, con la misión de ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio, para proteger la infraestructura crítica digital y servicios esenciales del Estado e infraestructura crítica digital del sector defensa.

OBJETIVOS ESTRATÉGICOS

Objetivo 4.1:

Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano para alcanzar la actitud **estratégica defensiva definida en la Política de la Defensa Nacional, para la protección de la Infraestructura Crítica Digital (ICD) y servicios esenciales en el ciberespacio.**

Líneas de acción

- Fortalecer la Ciberdefensa a fin de cumplir la misión constitucional de defensa en el ciberespacio, y contribuir a la protección de la infraestructura crítica digital y servicios esenciales del Estado e infraestructura crítica digital del sector defensa.
- Incrementar las capacidades de defensa activa y respuesta para contrarrestar a las amenazas que puedan afectar a la soberanía e integridad territorial en el ciberespacio, y lograr un impacto estratégico
- Articular y coordinar acciones conjuntas para el desarrollo de normativas y fortalecimiento interinstitucional que permita proteger el ciberespacio.
- Intensificar la cooperación internacional con el fin de generar un espacio de intercambio y apoyo en el ámbito de la Ciberdefensa.
- Fortalecer la cultura de Ciberdefensa para reducir los incidentes de los sistemas institucionales.

PILAR 5

HABILIDADES Y CAPACIDADES DE CIBERSEGURIDAD

Relevancia y **estado actual**

Un creciente número de usuarios de internet trae consigo un aumento de la vulnerabilidad de los ciudadanos, que utilizan los canales digitales tanto de manera profesional como en la vida diaria. Sin una conciencia proporcional, los criminales pueden aprovecharse de los usuarios de internet como blancos fáciles y enlaces más débiles en los sistemas de información.

Garantizar la ciberseguridad en Ecuador, enfrenta el desafío global de la deficiencia de profesionales calificados en ciberseguridad que surge de una intensidad sin precedentes de desarrollo digital y un panorama de amenazas y riesgos de ciberseguridad cada vez más desafiante. Si bien es posible contratar especialistas extranjeros y subcontratar operaciones, ese enfoque entraña riesgos relacionados con la seguridad nacional y la inestabilidad de la cadena de suministro.

Ecuador no cuenta actualmente con un plan nacional coordinado para fomentar las inversiones y los recursos para la educación y la sensibilización en materia de ciberseguridad, así como los planes de estudio escolares no abordan el tema de manera sistemática. La Educación Superior ofrece algunos cursos relacionados con la ciberseguridad y debaten sobre la necesidad de seguir desarrollando programas de estudios e investigaciones específicos sobre ciberseguridad.

En el ámbito de las competencias y capacidades en materia de ciberseguridad, hemos identificado áreas de oportunidad, por ejemplo, hay un déficit de especialistas en ciberseguridad y una necesidad identificada de mejorar en general los conocimientos y habilidades en ciberseguridad entre una amplia variedad de profesionales, incluidos desarrolladores de tecnologías de la información (TI), expertos en gestión y asuntos jurídicos y legales. Además, se ha determinado la necesidad de mejorar la concientización sobre la ciberseguridad a todos los niveles. Se espera que los programas sistemáticos de sensibilización dirigidos a diversos grupos específicos tengan un efecto significativo en el aumento de la resiliencia cibernética general de la sociedad. Los planes de estudio escolar y universitario no proporcionan actualmente apoyo suficiente para desarrollar profesionales calificados, ni proporcionan una sensibilización de manera sistemática. La creación sistemática de planes de estudios en todos los niveles de la educación puede contribuir a la creación de una sociedad digital más competente y consciente. La entrega de valor

de las actividades de concientización y capacitación se puede optimizar al garantizar el uso de plataformas y servicios digitales de última generación, así como las mejores prácticas, lo que garantiza el alcance, la disponibilidad, la participación y la inclusión necesarios.

OBJETIVOS ESTRATÉGICOS

Objetivo 5.1:

Mejorar y ampliar la concientización sobre la **ciberseguridad a todos los niveles de la sociedad**

Se fomentarán los conocimientos sobre ciberseguridad con el objetivo de fortalecer la cultura de ciberseguridad que abarca desde los ciudadanos hasta las organizaciones públicas y privadas y genera una conciencia compartida de los riesgos de ciberseguridad y las amenazas en el ciberespacio junto con las aptitudes necesarias para un comportamiento seguro y consciente en el ciberespacio. La conciencia pública del comportamiento responsable en el ciberespacio se incrementará a través de diversas actividades para diferentes grupos destinatarios, incluyendo aquellos, que no son sujetos del sistema educativo para asegurar que la gente en Ecuador sepa cómo comportarse de manera segura en el ciberespacio.

Líneas de acción

- Crear un programa nacional coordinado de sensibilización y cultura en materia de ciberseguridad, que incluya un órgano de coordinación para la aplicación y gestión. Asignar recursos para la implementación a largo plazo del programa. El programa abordará específicamente:

  a. preparación y ejecución de un programa de sensibilización para grupos específicos de ciudadanos,

  b. desarrollo de capacidades y sensibilización de los diferentes grupos destinatarios, incluido un enfoque que tenga en cuenta la equidad de género.

- Fomentar la creación de programas de apoyo a la persecución penal y prevención del delito cibernético, a través de la colaboración y participación ciudadana, fomentando los canales oficiales de denuncia y el desarrollo de campañas de prevención del delito cibernético.

Objetivo 5.2:

Reforzar las habilidades en materia de ciberseguridad **necesarias con las múltiples partes interesadas**

Se impartirá formación y educación en materia de ciberseguridad de alta calidad para garantizar que las personas tengan las aptitudes adecuadas para satisfacer la creciente demanda de conocimientos en materia de ciberseguridad en un número cada vez mayor de profesiones, y que haya profesionales especializados en ciberseguridad en los diversos sectores que desempeñen funciones específicas en la tarea de garantizar la ciberseguridad nacional tanto en las instituciones gubernamentales, los operadores de las ICD nacionales, la industria y la investigación académica. El éxito de la ciberseguridad nacional se basa en una fuerza de trabajo calificada y cibercultura y, por tanto, en un sistema educativo capaz de desarrollar esas capacidades. El enfoque de asociación público-privada se aplicará para apoyar la planificación e implementación del desarrollo de habilidades y capacidades en ciberseguridad, que incorpora agencias gubernamentales, partes interesadas del sector privado, actores de la sociedad civil, academia y apoyo de organizaciones internacionales.

Líneas de acción

- Crear un programa de actualización continua sobre identificación, prevención, detección, respuesta y recuperación de incidentes cibernéticos para el personal de TI y Oficiales de Seguridad de la Información de las instituciones gubernamentales a fin de prepararlos para responder a estos incidentes a medida que se producen.

- Fortalecer la cultura de uso del ciberespacio mejorando las habilidades y la conciencia de ciberseguridad de las múltiples partes interesadas a través de capacitaciones técnicas especializadas de acuerdo con el desarrollo tecnológico acelerado y el panorama de riesgos y amenazas.

- Preparar un programa de desarrollo de competencias para profesionales de organizaciones públicas.

- Diseñar un programa de desarrollo de habilidades para profesionales de organizaciones privadas, haciendo énfasis en las pequeñas y medianas empresas (PYMES).

Objetivo 5.3:

Asegurar que el sistema educativo imparta **conocimientos y fortalezca habilidades en materia de ciberseguridad**

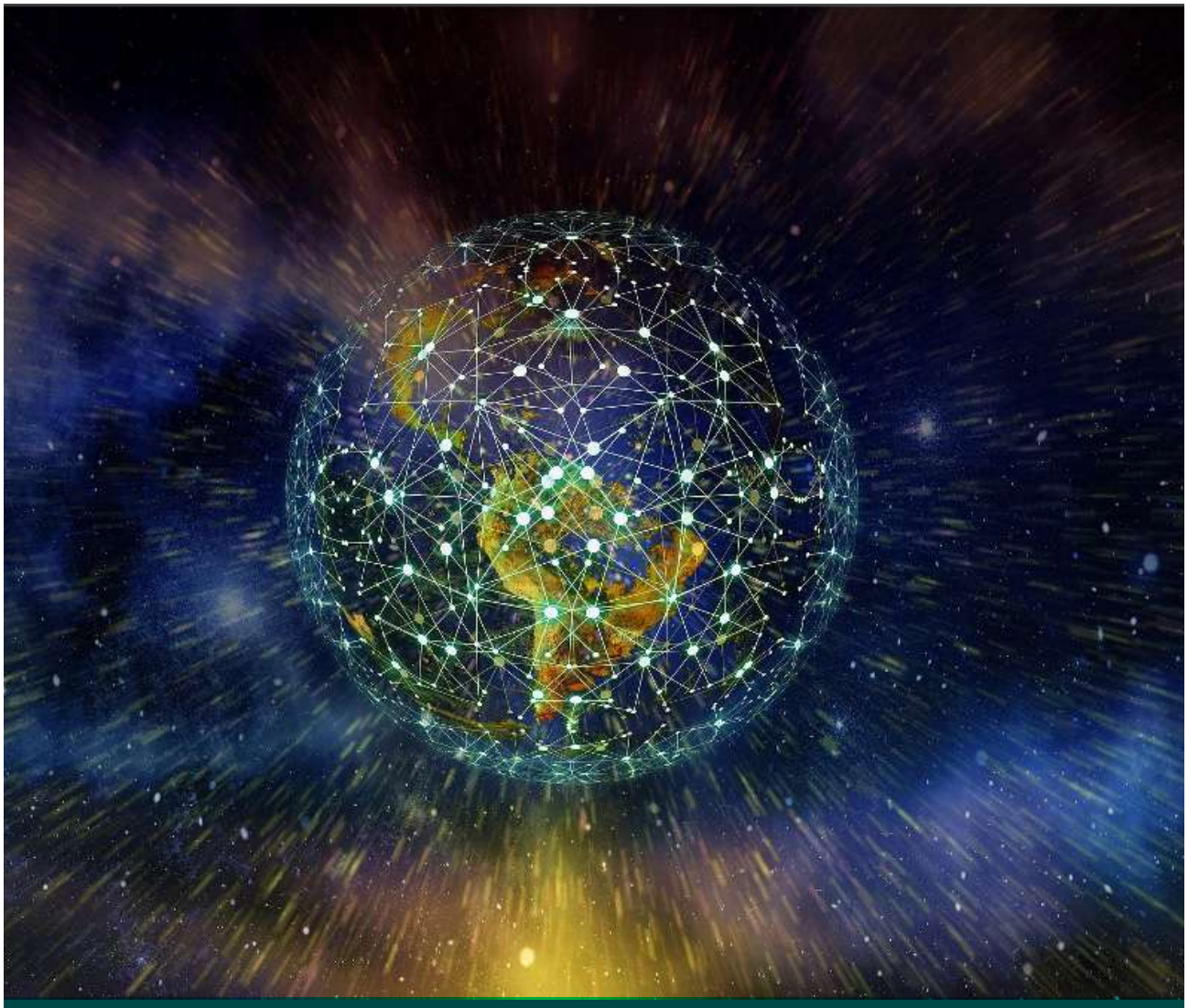
Con el fin de garantizar tanto la necesaria concientización sobre ciberseguridad como la higiene de la sociedad en general y crear una oferta de profesionales de la ciberseguridad, se establecerá un enfoque nacional coherente sobre la educación en ciberseguridad.

Se desarrollarán recursos y herramientas para currículos de ciberseguridad innovadores y dinámicos que presenten los conceptos básicos y la higiene cibernética, priorizando a la comunidad estudiantil, pero que también ofrezcan conceptos más complejos para estudiantes con un interés más profundo o en niveles educativos más altos. Dicho ciclo educativo comprende tanto la incorporación de contenidos y conocimientos sobre ciberseguridad en el sistema educativo. Un enfoque integral garantizará que los estudiantes estén equipados para manejar amenazas en entornos digitales y también ayudará a preparar a la próxima generación de fuerza laboral en el sector de ciberseguridad, pero también tendrá efectos positivos en todos los sectores laborales. Dado que el éxito de la estrategia dependerá en gran medida de contar con suficientes proveedores nacionales de productos y servicios de ciberseguridad en Ecuador, nuestras acciones ponen especial énfasis en ampliar y profundizar la educación en ciberseguridad para estimular la oferta de profesionales y emprendedores.

Líneas de acción

- Establecer una red de puntos de contacto nacionales para la educación en ciberseguridad en diferentes sectores, instituciones educativas y agencias gubernamentales.
- Elaborar un plan nacional de educación en ciberseguridad definiendo las funciones y responsabilidades para la aplicación del plan en todos los niveles del sistema educativo.
- Incluir conocimientos y habilidades en ciberseguridad en los planes de estudio de todos los niveles de educación para garantizar la oferta general de especialistas en ciberseguridad a largo plazo y establecer los requisitos previos para crear una industria nacional competitiva de productos y servicios de ciberseguridad, desarrollar la capacidad para proporcionar productos y servicios de ciberseguridad a nivel nacional para limitar los riesgos relacionados con dependencias de la cadena de suministro, y mejorar la investigación y la innovación en el área de Ciberdefensa.
- Crear contenidos educativos complementarios dirigidos a docentes y estudiantes de educación primaria, secundaria y superior.

PILAR 6



COOPERACIÓN INTERNACIONAL

Relevancia y **estado actual**

El ciberespacio es fundamentalmente transnacional y requiere un diálogo, marcos y cooperación internacional eficaces para aprovechar las oportunidades y gestionar los riesgos de ciberseguridad. Dado que la digitalización afecta a todos los ámbitos de las relaciones internacionales pertinentes para un Estado moderno, la ciberseguridad es, por lo tanto, integralmente pertinente para la política exterior de cualquier país, incluido el nuestro. Ecuador está interesado en que su voz e intereses nacionales sean escuchados en la agenda digital regional y mundial, y ha priorizado especialmente la seguridad internacional, los derechos humanos y la democracia en línea, así como el uso de las oportunidades que brinda el ciberespacio para el desarrollo sostenible, que siguen siendo temas importantes para avanzar en los foros internacionales. Un mejor enfoque y desarrollo de capacidades en esta área también tiene como objetivo crear un entorno en el que se fortalezcan la industria, la sociedad civil y la cooperación académica.

En la esfera de la cooperación cibernética internacional, hemos identificado esferas de oportunidades, ya que los esfuerzos son insuficientes y desarticulados, las prioridades reconocidas no van acompañadas de capacidad y recursos humanos y organizativos, y tenemos que concluir la armonización de nuestra legislación y procesos nacionales de acuerdo con el Convenio de Budapest sobre la Ciberdelincuencia y otros instrumentos internacionales para combatir el delito cibernético. Además, debemos fortalecer y racionalizar nuestra participación en la respuesta bilateral, regional e internacional a incidentes cibernéticos y en los formatos de lucha contra las amenazas en el ciberespacio, ya sea en el marco de respuesta a estos incidentes por parte del gobierno, aplicación de la ley o defensa nacional.

OBJETIVOS ESTRATÉGICOS PARA LA COOPERACIÓN INTERNACIONAL

Objetivo 6.1:

Identificar las prioridades internacionales de Ecuador **y desarrollar la capacidad de participar en la ciberdiplomacia regional e internacional**

Líneas de acción

- Identificar y participar en foros/iniciativas internacionales y regionales sobre normas relacionadas, derecho internacional, medidas de fomento de la confianza y creación de capacidades que configuran las reglas del ciberespacio y que son importantes para que Ecuador haga oír su voz.

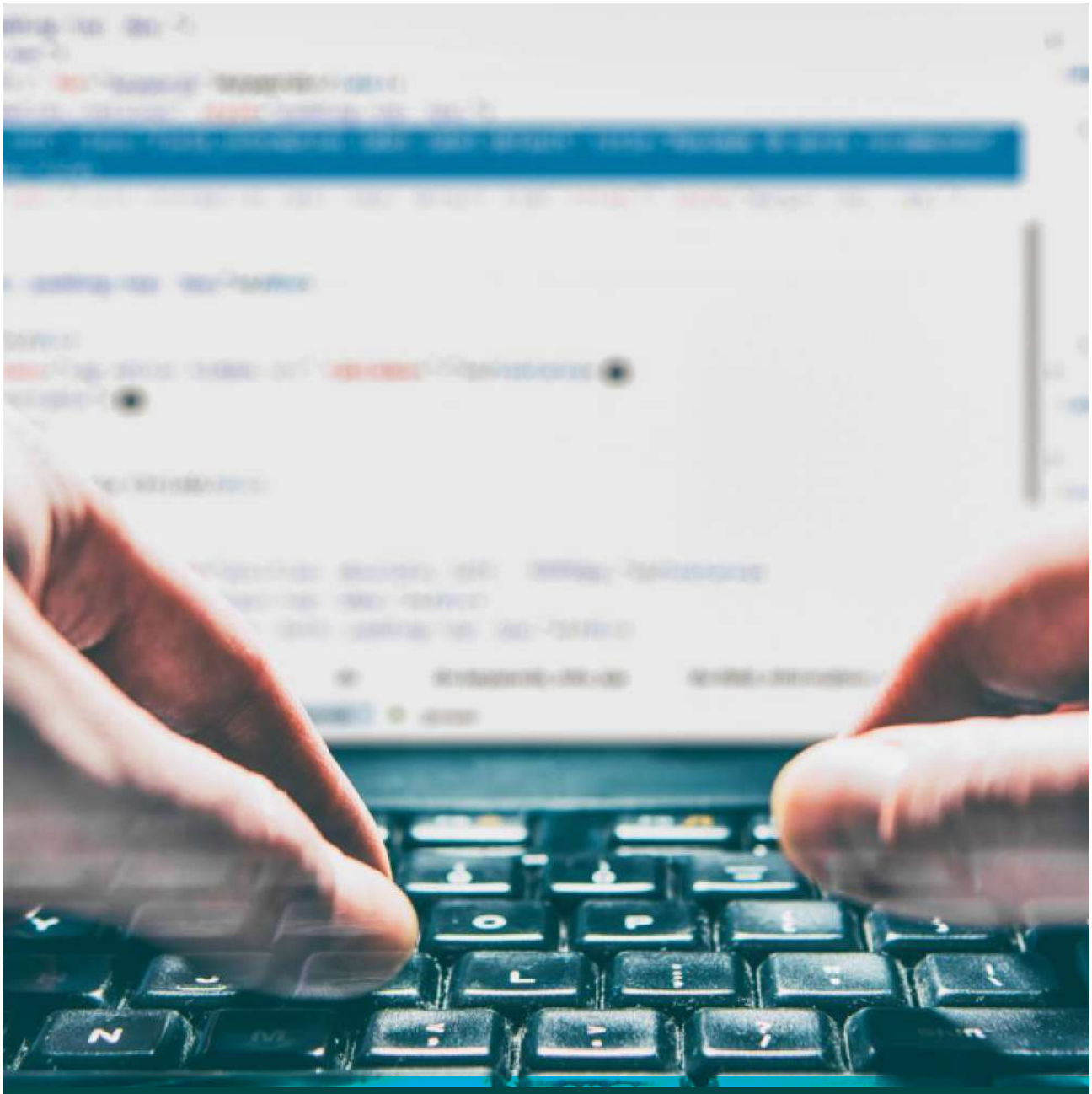
- Desarrollar conocimientos y capacidad en ciberdiplomacia para estar mejor representados en discusiones que afectan a nuestros ciudadanos y organizaciones, y ser un socio confiable y contribuyente a nivel regional y global.
- Insertar al Ecuador en la Agenda digital global y regional mediante el posicionamiento de asuntos digitales nacionales como un tema transversal de la Agenda 2030 para el Desarrollo Sostenible.
- Nombrar responsabilidades organizativas para asuntos exteriores cibernéticos (embajador cibernético u otra oficina dedicada) e informar regularmente sobre la cooperación internacional a nivel político/estratégico.
- Garantizar una participación significativa y decidida en los formatos de creación de capacidad existentes mediante la definición de áreas y objetivos prioritarios para la creación de capacidad en materia de ciberseguridad (incluidos el fomento de la resiliencia cibernética, la gestión de incidentes cibernéticos y la lucha contra la ciberdelincuencia), y promover nuevos intercambios de conocimientos y sesiones de transferencia con otros países y organizaciones regionales e internacionales en esas áreas.

Objetivo 6.2:

Fortalecer la participación de Ecuador en la cooperación **bilateral, regional e internacional en respuesta a las amenazas en el ciberespacio**

Líneas de acción

- Procurar ampliar y formalizar la cooperación con otros organismos nacionales e internacionales de respuesta a incidentes cibernéticos activos en la región.
- Profundizar y formalizar la participación en mecanismos de coordinación y cooperación internacionales y regionales para combatir el delito cibernético a través del intercambio de información, investigaciones transfronterizas, operaciones y arrestos.
- Intensificar la cooperación internacional para generar un espacio de intercambio y apoyo en el campo de la Ciberdefensa a través de alianzas estratégicas, la participación en organismos internacionales para contrarrestar amenazas de carácter común y la gestión de oportunidades para compartir información, conocimientos, buenas prácticas y realizar entrenamientos y ejercicios.
- Apoyar a las partes interesadas para que se adhieran a los mecanismos internacionales de cooperación, colaboración y asistencia (incluida la capacitación, ejercicios internacionales, entre otros).
- Participar en esfuerzos internacionales de creación de capacidades que ayuden a los organismos de aplicación de la ley a mejorar sus habilidades, conocimientos y capacidades técnicas.



PERSPECTIVAS FRENTE A LA IMPLEMENTACIÓN, SEGUIMIENTO Y EVALUACIÓN

La implementación de la Estrategia Nacional de Ciberseguridad del Ecuador estará a cargo del *Comité Nacional de Ciberseguridad,* órgano estratégico de coordinación y toma de decisiones, con el apoyo de las instituciones con competencias en la seguridad integral del Estado. La responsabilidad de la efectiva implementación de las iniciativas y acciones recae en cada una de las múltiples partes interesadas en el ecosistema de ciberseguridad de Ecuador.

El seguimiento a la ejecución física y presupuestal de las acciones propuestas para el cumplimiento de los objetivos específicos se realizará a través de un Plan de Acción que se desarrollará en mayor detalle a partir de un ejercicio de priorización y basado en este capítulo una vez aprobada la Estrategia Nacional de Ciberseguridad indicando las entidades responsables de cada acción, los periodos de ejecución de estas, los recursos necesarios y disponibles para llevarlas a cabo, así como la importancia de cada acción para el cumplimiento del propósito general y de los objetivos específicos bajo cada pilar de la estrategia nacional. Los responsables de la ejecución de las líneas de acción deberán presentar informes trimestrales al Comité Nacional de Ciberseguridad, de las actividades realizadas, de tal manera que el Comité haga el seguimiento y evaluación de la implementación de la Estrategia Nacional de Ciberseguridad y se presenten informes anuales. El Plan de Acción estará sujeto a las modificaciones que apruebe el Comité Nacional de Ciberseguridad a medida que avance la implementación de la estrategia nacional.

Ecuador adelantará el monitoreo del nivel de madurez en ciberseguridad y evaluación de las capacidades de las múltiples partes interesadas con el fin de asegurar una mejora continua, haciendo énfasis en el corto y mediano plazo. Además, se soportará en el desarrollo de auditorías sobre los procesos que llevan a cabo las entidades gubernamentales y el desarrollo de ejercicios de eficiencia comparativa basados en la recopilación y análisis de información estadística relevante a nivel nacional, así como la preparación de informes de situación sobre el estado de la ciberseguridad. Se prevé la revisión y actualización de la Estrategia cada tres (3) años o según se considere necesario.

Finalmente, se creará y ejecutará un plan estratégico de comunicación del cumplimento de los objetivos de la Estrategia Nacional de Ciberseguridad en donde se establecen tareas y acciones específicas que se realizarán en el marco de los procesos de implementación, seguimiento y monitoreo.

Pilar 1.
Gobernanza y coordinación nacional

Objetivo 1.1: Establecer un marco integral de gobernanza de la ciberseguridad

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Establecer un marco institucional con los roles, funciones y responsabilidades prescritas de todos los agentes gubernamentales pertinentes en materia de ciberseguridad que abarque todos los objetivos estratégicos de la estrategia nacional	Marco institucional con roles y responsabilidades	MINTEL	Instituciones que conforman el Comité Nacional de Ciberseguridad	X		
Fortalecer la instancia de coordinación nacional para dirigir la implementación de la política nacional y llevar a cabo un seguimiento continuo.	Definición de roles funciones y responsabilidades	Instituciones que conforman el Comité Nacional de Ciberseguridad	Comité Nacional de Ciberseguridad	X	X	X
Adaptar y fortalecer la instancia de máximo nivel intergubernamental e intersectorial para orientar estratégicamente la gestión de la ciberseguridad.	Comité Nacional de Ciberseguridad	Comité Nacional de Ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad Entidades del Gobierno	X		
Implementar una herramienta de seguimiento y evaluación del cumplimiento de los objetivos estratégicos y la asignación de recursos de la Estrategia Nacional de Ciberseguridad de acuerdo con el plan de implementación.	Herramienta de seguimiento	Instituciones que conforman el Comité Nacional de Ciberseguridad	Comité Nacional de Ciberseguridad Entidades del Estado		X	
Establecer un mecanismo regulador de supervisión y presentación de informes con indicadores clave de desempeño en materia de ciberseguridad e indicadores clave de riesgo para investigar la situación y las tendencias de la ciberseguridad a nivel nacional.	Informes e indicadores	Instituciones que conforman el Comité Nacional de Ciberseguridad	Comité Nacional de Ciberseguridad Entidades del Estado		X	X

Objetivo 1.2: Fomentar una comunidad sólida y articulada con expertos en ciberseguridad de las múltiples partes interesadas

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Establecer un mecanismo eficaz de asociación entre el sector público y el privado en el que participen todas las múltiples partes interesadas pertinentes de las instituciones gubernamentales, el sector privado, el mundo académico y las ONG, a fin de proporcionar una plataforma para la participación.	Mecanismo	Comité Nacional de Ciberseguridad	Instituciones del sector privado, organismos no gubernamentales, y Asociaciones a fines	X	X	

Objetivo 1.3: Desarrollar un marco legal y regulatorio integral que permita la gobernanza nacional de la ciberseguridad y la Ciberdefensa

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Efectuar un análisis exhaustivo del marco legal y regulatorio vigente en todo el ámbito de la ciberseguridad para evaluar, determinar las "lagunas legales" y aclarar cualquier necesidad adicional de adopción y armonización de la legislación y los reglamentos	Análisis del marco legal y regulatorio	Comité Nacional de Ciberseguridad	Asamblea Nacional del Ecuador, Función Judicial, Fiscalía General del Estado, Procuraduría General del Estado	X	X	
Establecer de manera integral los roles y responsabilidades de los principales ministerios y otras agencias en ciberseguridad nacional dentro del marco legal y regulatorio.	Roles y responsabilidades	Comité Nacional de Ciberseguridad	ARCOTEL Superintendencia de Bancos Autoridad de Protección de Datos Personales SEPS Cámaras de Comercio, Industrias y afines		X	
Orientar los cambios legislativos en todos los objetivos estratégicos de la estrategia nacional.	Propuesta de Ley de Ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad	Asamblea Nacional del Ecuador Función Judicial Fiscalía General del Estado Procuraduría General del Estado Asociaciones a fines	X	X	

Pilar 2.
Resiliencia cibernética

Objetivo 2.1: Establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación para las crisis cibernéticas con el fin de fortalecer dichas capacidades a nivel nacional

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Adoptar un marco nacional de gestión del riesgo de seguridad digital	Marco nacional de gestión del riesgo de seguridad digital	Instituciones que conforman el Comité Nacional de Ciberseguridad	Servicio Nacional de Acreditación ASOBANCA Superintendencia de Bancos SEPS Cámaras de Comercio, Industrias y afines Asociaciones a fines	X	X	
Elaborar un informe sobre el panorama de amenazas y riesgos a nivel nacional y un seguimiento continuo.	Informe sobre el panorama de amenazas y riesgos	Instituciones que conforman el Comité Nacional de Ciberseguridad	ASOBANCA Superintendencia de Bancos SEPS Cámaras de Comercio, Industrias y afines Asociaciones a fines	X		
Identificar tipos comunes de ciberataques dirigidos a las ICD nacionales e instituciones gubernamentales.	Informes periódicos con tipos comunes de ciberataques	Instituciones que conforman el Comité Nacional de Ciberseguridad	Instituciones públicas del Estado	X	X	
Establecer mecanismos independientes de control que incluyan la evaluación de riesgo de ciberseguridad y pruebas periódicas de penetración para las organizaciones del sector público y los operadores de las ICD nacionales.	Mecanismos de control	Los organismos operativos de las instituciones que conforman el Comité Nacional de Ciberseguridad	Organismo Nacional de Acreditación (INEN)		X	
Identificar los operadores de servicios de telecomunicaciones para la respuesta y comunicación de emergencia	Regulación para proveedores de redes de telecomunicaciones	MINTEL	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	
Crear un programa de coordinación designado para la adopción de normas de ciberseguridad y mejores prácticas tanto para los organismos gubernamentales como para las contrapartes pertinentes del sector privado.	Programa de coordinación y adopción de normas	Los organismos operativos de las instituciones que conforman el Comité Nacional de Ciberseguridad	Organismo Nacional de Acreditación (INEN)		X	

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Identificar escenarios de riesgo de ciberseguridad para los cuales se deben desarrollar planes nacionales de contingencia.	Informes periódicos con escenarios de riesgo de ciberseguridad	Los organismos operativos de las instituciones que conforman el Comité Nacional de Ciberseguridad	Entidades del Estado		X	
Organizar ejercicios nacionales de ciberseguridad para probar las capacidades del personal involucrado en la ciberseguridad de las organizaciones.	Ejercicios nacionales de ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad	Entidades del Estado		X	X
Realizar pruebas que involucren los escenarios de contingencia establecidos por las organizaciones	Escenarios de contingencia	Los organismos operativos de las instituciones que conforman el Comité Nacional de Ciberseguridad	Entidades del Estado		X	X

Objetivo 2.2: Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de Infraestructuras Críticas Digitales (ICD)

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Documentar una metodología clara para la identificación de las ICD nacionales basada en consideraciones sociales, económicas y ambientales	Metodología de identificación de ICD nacionales	Los organismos operativos de las instituciones que conforman el Comité Nacional de Ciberseguridad	Organismos internacionales afines	X		
Establecer y mantener una lista actualizada de las ICD nacionales junto con la definición de sectores estratégicos que contempla el concepto de protección de servicios e infraestructura esenciales.	Registro actualizado de las ICD nacionales	Coordinador Nacional de Ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad	X		
Establecer un mecanismo de cooperación y coordinación mediante asociaciones público-privadas entre todos los operadores de las ICD nacionales para apoyar el fomento de la confianza.	Mecanismo de cooperación y coordinación para las ICD nacionales	Instituciones que conforman el Comité Nacional de Ciberseguridad	Instituciones que conforman el catálogo de ICD Organismos internacionales afines	X	X	

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Establecer normas nacionales de referencia con base a estándares y mejores prácticas internacionales, que se apliquen a todos los operadores de las ICD nacionales tanto en operadores de IC del sector privado como en activos de ICD dentro de las instituciones gubernamentales	Marco normativo de referencia	Instituciones que conforman el Comité Nacional de Ciberseguridad	Organismos internacionales afines	X	X	
Emitir directrices e instrucciones para apoyar la aplicación de medidas de seguridad y lograr el cumplimiento de la norma de referencia	Directrices	Comité Nacional de Ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	
Definir los roles y responsabilidades a nivel nacional para la coordinación de la identificación y el seguimiento de las ICD nacionales dentro del marco legal y regulatorio, considerando tanto la dimensión civil como la militar.	Marco de coordinación para la identificación y el seguimiento de las ICD nacionales	Comité Nacional de Ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	
Establecer requisitos de ciberseguridad para los operadores de ICD nacionales en el marco legal y regulatorio, cuando se considere pertinente	Requisitos de ciberseguridad para las ICD nacionales	Comité Nacional de Ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X

Objetivo 2.3: Continuar desarrollando capacidades de respuesta y gestión de incidentes cibernéticos y del CERT nacional

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Crear y poner en funcionamiento un Centro de Operaciones de Seguridad (SOC) nacional (gubernamental).	GSoC del Gobierno	MINTEL	Instituciones que conforman el Comité Nacional de Ciberseguridad Instituciones del Gobierno		X	X
Establecer y ejecutar un plan para generar un marco jurídico para contar con: i) un equipo de respuesta a incidentes cibernéticos de alcance nacional y, ii) un sistema nacional de gestión y respuesta a estos incidentes.	Plan para generar un marco jurídico	MINTEL	Instituciones que conforman el Comité Nacional de Ciberseguridad Ministerio de Defensa Ministerio del Interior	X	x	
Crear un CERT a nivel nacional.	Plan para crear y fortalecer el CERT a nivel nacional	PRESIDENCIA / MINTEL	Comité Nacional de Ciberseguridad	X	X	

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Establecer un mecanismo para la divulgación periódica de vulnerabilidades y el intercambio de información entre los operadores de las ICD nacionales y el gobierno de Ecuador	Mecanismo para la divulgación periódica de la vulnerabilidad y el intercambio de información para las ICD nacionales	Instituciones que conforman el Comité Nacional de Ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad , ASOBANCA, SEPS		X	

Objetivo 2.4: Maximizar el uso de tecnologías avanzadas y la innovación en el diseño de políticas y procesos ágiles para el desarrollo de capacidades de Ciberinteligencia

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Desarrollar un observatorio del ciberespacio con roles y funciones para recopilar, analizar y clasificar la información sobre amenazas e incidentes cibernéticos que se utiliza para proporcionar a las empresas una visión procesable para identificar, medir y clasificar las vulnerabilidades y mitigar los riesgos cibernéticos	Observatorio del Ciberespacio	CIES	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Desarrollar un sistema de alerta temprana para la prevención y anticipación de Ciberamenzas avanzados para asesorar la toma de decisiones al más alto nivel del Estado.	Sistema de alerta temprana Proceso de prevención y anticipación de alertas	CIES	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	x	
Invertir en el desarrollo de capacidades de planificación para la ejecución de operaciones cibernéticas a través de detección y respuesta avanzadas.	Plan de fortalecimiento de capacidades de planificación	Coordinador Nacional de Ciberseguridad	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X
Desarrollar las capacidades del Centro de Operaciones de Seguridad (GSoC) nacional (gubernamental) a través de esquemas de investigación y herramientas de respuesta a incidentes para garantizar la resiliencia de las ICD nacionales, los servicios estatales esenciales.	Plan de fortalecimiento de capacidades de planificación	CIES	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X
Establecer los mecanismos de obtención de información y los medios de gestión de inteligencia para cada nivel del estado.	Metodología para el manejo de los tipos de inteligencia.	CIES	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	

Pilar 3.
Prevención y combate a la ciberdelincuencia

Objetivo 3.1: Actualizar el marco legal y regulatorio de Ecuador en materia de ciberdelincuencia para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Revisar el derecho penal existente y adoptar las medidas legislativas necesarias para definir claramente qué constituye delito cibernético y delitos relacionados (delitos contra o a través de sistemas o datos informáticos), considerando la armonización con los instrumentos legales internacionales y regionales existentes, en particular el Convenio de Budapest sobre la Ciberdelincuencia	Estrategia de revisión normativa	Ministerio del Interior	Instituciones que conforman el Comité Nacional de Ciberseguridad, Fiscalía General del Estado, Corte Nacional de Justicia, Consejo de la Judicatura y Asamblea Nacional del Ecuador.		X	
Revisar y ajustar los actos legales para definir el mandato legal y la autoridad de las fuerzas del orden, las autoridades ejecutivas y los proveedores de servicios digitales con fines de prevención del delito cibernético.	Mandato jurídico	Ministerio de Gobierno, Ministerio del Interior, Asamblea Nacional del Ecuador	Instituciones que conforman el Comité Nacional de Ciberseguridad, Fiscalía General del Estado, Corte Nacional de Justicia, ARCOTEL		X	X
Revisar y alinear los poderes y procedimientos apropiados para la aplicación de la ley, el enjuiciamiento y la judicialización para la investigación y el enjuiciamiento del delito cibernético, incluida la recopilación y el procesamiento de pruebas e instrumentos electrónicos para una cooperación internacional rápida y eficaz, considerando la armonización con el Convenio de Budapest sobre la Ciberdelincuencia y otros instrumentos internacionales.	Mandato jurídico	Ministerio de Gobierno, Ministerio del Interior	Instituciones que conforman el Comité Nacional de Ciberseguridad, Fiscalía General del Estado, Corte Nacional de Justicia, Consejo de la Judicatura			X

Objetivo 3.2: Fortalecer la respuesta oportuna y las capacidades operacionales de investigación y judicialización de la cibercriminalidad

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Fortalecer la unidad o unidades especializadas en ciberdelincuencia de la Policía Nacional de Ecuador con las capacidades logísticas, humanas y forenses digitales adecuadas asegurando procedimientos investigativos regulados a nivel nacional	Unidad o unidades especializadas en ciberdelincuencia	Policía Nacional	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Facilitar la creación de Direcciones o Unidades de Prevención de Delitos Cibernéticos especializadas, con personal profesional especializado en el campo de la informática y el derecho y con procedimientos preventivos estándar y mecanismos de denuncia de delitos cibernéticos, eficientes para la sociedad ecuatoriana	Direcciones o unidades especializadas en ciberdelincuencia	Ministerio del Interior Corte Nacional de Justicia	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Apoyar la creación de unidades especializadas de la fiscalía en la investigación del delito cibernético a nivel nacional, con personal profesional especializado en el campo de la informática y el derecho, contribuyendo a la adecuada administración de justicia	Direcciones o unidades especializadas en ciberdelincuencia	Fiscalía General del Estado	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Identificar y desarrollar oportunidades de capacitación a funcionarios encargados de hacer cumplir la ley y especialistas forenses sobre la ley del delito cibernético y su implementación, incluida la protección de los derechos humanos y la colaboración con los organismos internacionales encargados de hacer cumplir la ley.	Programa de capacitación para especialistas en aplicación de la ley y forenses	Ministerio del Interior Fiscalía General del Estado Consejo Nacional de la Judicatura	Instituciones que conforman el Comité Nacional de Ciberseguridad SECAP Asociaciones afines		X	

Pilar 4.
Ciberdefensa

Objetivo 4.1: Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano para alcanzar la actitud estratégica defensiva definida en la Política de la Defensa Nacional, para la protección de la infraestructura crítica digital (ICD) y servicios esenciales en el ciberespacio.

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Maximizar el uso de tecnologías avanzadas, desarrollar capacidades en el dominio ciberespacial en las Fuerzas Armadas hasta formar una Fuerza Ciberespacial Conjunta	Plan para la creación de la Fuerza Ciberespacial Conjunta (FCC)	Ministerio de Defensa Nacional (COCIBER)	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X
Planificar y participar en ciberejercicios nacionales e internacionales donde simulen escenarios de crisis que permita adiestrar en tácticas y técnicas cibernéticas para evaluar el grado de preparación del personal.	Plan de ejercicios de Ciberdefensa	Ministerio de Defensa Nacional (COCIBER)	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X
Establecer políticas y definir los recursos necesarios para la protección de la infraestructura crítica digital (ICD) y servicios esenciales del Estado.	Plan estratégico para la protección de la ICD	Ministerio de Defensa Nacional (COCIBER)	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X
Desarrollar y aplicar un sistema y plan nacional de gestión de crisis cibernéticas	Plan nacional de gestión de crisis cibernéticas	Ministerio de Defensa Nacional (COCIBER)	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Planificar pruebas periódicas de la resiliencia cibernética ante diferentes escenarios de ciberataques que afecten a las ICD.	Planificación anual de visitas a las ICD	Ministerio de Defensa Nacional (COCIBER)	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Fortalecer la cooperación nacional con el sector industrial y académico, así como, establecer acuerdos multilaterales con organismos internacionales para alcanzar los objetivos estratégicos de Ciberdefensa.	Convenios y acuerdos establecidos	Ministerio de Defensa Nacional (COCIBER)	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	X
Desarrollar doctrina conjunta para fomentar el uso efectivo de la Ciberdefensa.	Doctrina de operaciones militares de Ciberdefensa	Ministerio de Defensa Nacional (COCIBER)	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Participar en el desarrollo del derecho internacional de operaciones cibernéticas.	Manual	Ministerio de Relaciones Exteriores y Movilidad Humana y Ministerio de Defensa Nacional	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X
Desarrollar el manual de derecho de las operaciones militares en el Ciberespacio.	Manual	Ministerio de Defensa Nacional (COCIBER-COLEMI)	Asesoría Jurídica de MIDENA Y COMACO		X	X

Pilar 5.
Habilidades y capacidades de ciberseguridad

Objetivo 5.1: Mejorar y ampliar la concientización sobre la ciberseguridad a todos los niveles de la sociedad

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Elaborar y ejecutar un programa nacional coordinado de sensibilización y cultura en materia de ciberseguridad, que incluya un órgano de coordinación para su ejecución y gestión	Programa nacional de sensibilización y cultura	MINTEL SECOM	Instituciones que conforman el Comité Nacional de Ciberseguridad, Ministerio de Educación Asociaciones Afines, Medios de Comunicación Entidades del Gobierno	X	X	X
Fomentar la creación de programas de apoyo a la persecución penal y prevención del delito cibernético, a través de la colaboración y participación ciudadana, fomentando los canales oficiales de denuncia y el desarrollo de campañas de prevención del delito cibernético.	Programas de apoyo a la persecución penal y prevención del delito cibernético	MINTEL	Instituciones que conforman el Comité Nacional de Ciberseguridad, Ministerio de Educación Asociaciones Afines, Medios de Comunicación Entidades del Gobierno		X	X

Objetivo 5.2: Reforzar las habilidades en materia de ciberseguridad necesarias con las múltiples partes interesadas

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Crear un programa de formación continua sobre identificación, prevención, detección, respuesta y recuperación de incidentes cibernéticos para el personal de TI y Oficiales de Seguridad de la Información de las instituciones gubernamentales a fin de prepararlos para responder a estos incidentes a medida que se producen.	Programa de formación continua	MINTEL	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Fortalecer la cultura de defensa cibernética mejorando las habilidades y la conciencia de ciberseguridad de las múltiples partes interesadas a través de capacitaciones técnicas especializadas de acuerdo con el desarrollo tecnológico acelerado y el panorama de riesgos y amenazas cada vez más desafiante.	Capacitaciones técnicas especializadas	MINTEL	Ministerio del Trabajo, Ministerio de Finanzas, Organizaciones afines a la Gestión de Ciberseguridad / Seguridad de la Información		X	

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Preparar e implementar un programa de desarrollo de competencias para profesionales de organizaciones públicas.	Programa de desarrollo de capacidades	MINTEL	Ministerio de Trabajo, Instituciones que conforman el Comité Nacional de Ciberseguridad		X	
Preparar y aplicar un programa de desarrollo de habilidades para profesionales de organizaciones privadas, haciendo énfasis en las pequeñas y medianas empresas (PYMES).	Programa de desarrollo de capacidades	MINTEL	Instituciones que conforman el Comité Nacional de Ciberseguridad, Ministerio del Trabajo (SETEC) SECAP, Asociaciones a fines Ministerio de Producción Comercio Exterior, Inversiones y Pesca		X	

Objetivo 5.3: Asegurar que el sistema educativo imparta conocimientos y fortalezca habilidades en materia de ciberseguridad

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Establecer una red de puntos de contacto nacionales para la educación en ciberseguridad en diferentes sectores, instituciones educativas y agencias gubernamentales.	Red de puntos de contacto para la educación	MINTEL	Instituciones que conforman el Comité Nacional de Ciberseguridad, Ministerio de Educación, Asociaciones afines	X		
Elaborar y ejecutar un plan nacional de educación en ciberseguridad en las instituciones de educación.	Plan nacional de educación	MINTEL Ministerio de Educación	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	
Incluir conocimientos y habilidades en ciberseguridad en los planes de estudio de todos los niveles de educación para garantizar la oferta general de especialistas en ciberseguridad a largo plazo y establecer los requisitos previos para crear una industria nacional competitiva de productos y servicios de ciberseguridad, desarrollar la capacidad para proporcionar productos y servicios de ciberseguridad a nivel nacional para limitar los riesgos relacionados con dependencias de la cadena de suministro, y mejorar la investigación y la innovación en el área de Ciberdefensa.	Currículos educativos con contenido incluido	MINTEL Ministerio de Educación CES	Instituciones que conforman el Comité Nacional de Ciberseguridad, SENESCYT		X	X
Crear contenidos educativos complementarios dirigidos a docentes y estudiantes de educación primaria, secundaria y superior.	Contenido educativo	MINTEL, Ministerio de Educación CES	Instituciones que conforman el Comité Nacional de Ciberseguridad, SENESCYT		X	X

Pilar 6.
Cooperación internacional

Objetivo 6.1: Identificar las prioridades internacionales de Ecuador y desarrollar la capacidad de participar en la ciberdiplomacia regional e internacional

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Identificar y participar en foros/iniciativas internacionales y regionales sobre ciber normas, derecho internacional, medidas de fomento de la confianza y creación de capacidades	Participación en foros/iniciativas internacionales y regionales	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Insertar al Ecuador en la Agenda digital global y regional mediante el posicionamiento de asuntos digitales nacionales como un tema transversal de la Agenda 2030 para el Desarrollo Sostenible	Agenda 2030 actualizada	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X
Desarrollar conocimientos y capacidad en ciberdiplomacia y desarrollo, y ser un socio confiable y contribuyente a nivel regional y global.	Plan para generar capacidades en ciberdiplomacia	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	X
Nombrar responsables para asuntos exteriores cibernéticos (embajador cibernético u otra oficina dedicada) e informar regularmente sobre la cooperación internacional a nivel político/ estratégico	Responsables para asuntos exteriores cibernéticos	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	X
Garantizar una participación significativa y decidida en los formatos de creación de capacidad existentes mediante la definición de áreas y objetivos prioritarios para la creación de capacidad en materia de ciberseguridad y promover nuevos intercambios de conocimientos y sesiones de transferencia con otros países y organizaciones regionales e internacionales en esas áreas	Sesiones internacionales de transferencia e intercambio de conocimiento	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad		X	X

Objetivo 6.2: Fortalecer la participación de Ecuador en la cooperación bilateral, regional e internacional en respuesta a las amenazas en el ciberespacio

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo	Largo plazo
Ampliar y formalizar la cooperación con otros organismos nacionales e internacionales de respuesta a incidentes cibernéticos activos en la región	Acuerdos de cooperación	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	
Participar en mecanismos de coordinación y cooperación internacionales y regionales para combatir el delito cibernético a través del intercambio de información, investigaciones transfronterizas, operaciones y arrestos	Memorandos de entendimiento y acuerdos de coordinación y cooperación	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	X
Intensificar la cooperación internacional para generar un espacio de intercambio y apoyo en el campo de la Ciberdefensa a través de alianzas estratégicas, la participación en organismos internacionales para contrarrestar amenazas de carácter común y la gestión de oportunidades para compartir información, conocimientos, buenas prácticas y realizar entrenamientos y ejercicios	Alianzas estratégicas	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	X
Apoyar a las múltiples partes interesadas para que se adhieran a los mecanismos internacionales de cooperación, colaboración y asistencia	Participación de múltiples partes interesadas	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	X
Participar en esfuerzos internacionales de creación de capacidades que ayuden a los organismos de aplicación de la ley a mejorar sus habilidades, conocimientos y capacidades técnicas	Participación de organismos de aplicación de la ley	Ministerio de Relaciones Exteriores y Movilidad Humana	Instituciones que conforman el Comité Nacional de Ciberseguridad	X	X	X

Indicadores

Los siguientes indicadores claves de rendimiento serán monitoreados y evaluados por el Coordinador de Nacional de Ciberseguridad trimestralmente y presentará reportes anuales al Comité Nacional de Ciberseguridad. Los indicadores junto con las metas de cumplimiento estarán sujeto a las modificaciones que apruebe el Comité Nacional de Ciberseguridad a medida que avance la implementación de la Estrategia Nacional de Ciberseguridad.

Indicador	Unidad de medida	Periodo de medición	Corto plazo	Mediano plazo	Largo plazo	Responsable
Índice Mundial de Ciberseguridad (CGI)	Valor	Anual			51,3	MINTEL
Número de revisiones a la Estrategia Nacional de Ciberseguridad	Número	Anual	1	1	2	Comité Nacional de Ciberseguridad
Cantidad de leyes actualizadas y promulgadas	Leyes	Anual	1	1	2	Comité Nacional de Ciberseguridad Asamblea Nacional del Ecuador
Cantidad de normativas y estándares revisadas	Normas	Anual	4	6	8	Comité Nacional de Ciberseguridad Entidades Reguladoras
Numero alianzas de cooperación establecidas en materia de ciberseguridad, lucha contra el delito cibernético y Ciberdefensa.	Alianzas	Anual	5	10	15	Coordinador Ministerio de Relaciones Exteriores y Movilidad Humana
Cantidad de simulacros / simulaciones nacionales realizados en materia de crisis cibernéticas	Simulacros / Simulaciones	Anual	3	6	9	Comité Nacional de Ciberseguridad CERT Nacional EcuCERT Naciona
Porcentaje de instituciones que han adoptados normativas de ciberseguridad	Instituciones públicas	Anual	20%	40%	60%	Comité Nacional de Ciberseguridad

Indicador	Unidad de medida	Periodo de medición	Corto plazo	Mediano plazo	Largo plazo	Responsable
Porcentaje de instituciones con infraestructuras críticas digitales (ICD) cumpliendo la normativa de este tipo de infraestructura	% de instituciones	Anual	20%	40%	60%	Comité Nacional de Ciberseguridad Ministerio de Defensa
Porcentaje de PYMES sensibilizados en Ciberseguridad	% de PYMES	Anual	5%	10%	15%	Coordinador MINTEL
Porcentaje de Jueces y fiscales capacitados en Ciberseguridad	% de jueces y fiscales	Anual	10%	30%	50%	Comité Nacional de Ciberseguridad Consejo de la Judicatura Fiscalía General del Estado
Porcentaje de servidores públicos sensibilizados en Ciberseguridad	% de servidores públicos	Anual	20%	40%	60%	Coordinador MINTEL
Porcentaje de estudiantes de nivel básico sensibilizados en Ciberseguridad (sector público y privado)	% de estudiantes de nivel básico	Anual	20%	40%	60%	Coordinador Min Educación
Número de estudiantes de nivel intermedio sensibilizados en Ciberseguridad (sector público y privado)	% de estudiantes de nivel intermedio	Anual	20%	40%	60%	Coordinador Min Educación
Número de docentes de nivel básico, intermedio y nivel superior sensibilizados en Ciberseguridad (sector público y privado)	% de docentes	Anual	20%	40%	60%	Coordinador Min Educación Senescyt
Número de encuestas realizadas sobre el nivel de conocimiento en Ciberseguridad a la población	Encuestas	Anual	1	2	3	Comité Nacional de Ciberseguridad

Ministerio de Telecomunicaciones
y de la Sociedad de la Información

República
del Ecuador

Gobierno
del Encuentro

GUILLERMO LASSO
PRESIDENTE