ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR
Versión 1.1

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR

Borrador 1.1

PRÓLOGO DEL MINISTRO

[Posteriomente se redactará]

TABLA DE CONTENIDO

IMPLEMENTACIÓN, SEGUIMIENTO Y EVALUACIÓN

PANORAMA NACIONAL DE CIBERSEGURIDAD, DESAFÍOS Y OPORTUNIDADES

Para el lector (para la versión borrador): *Esta sección proporciona una descripción de alto nivel del contexto nacional actual y la perspectiva estratégica para la ciberseguridad en Ecuador, reflejando una evaluación de las fortalezas, oportunidades, debilidades y amenazas identificadas en evaluaciones anteriores y por los interesados nacionales en el taller de estrategia en marzo de 2022; y el marco político, jurídico y organizativo existente al que se conecta la estrategia nacional.*

Retos y oportunidades para la ciberseguridad

Las tecnologías digitales son indispensables para el 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. La creciente sofisticación de la tecnología y su uso generalizado ha dado lugar a ciberamenazas 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, etc.

En 2021, se aprobó nuestra primera Política de Ciberseguridad, y se reconoció que los interesados deben fortalecer sus capacidades para identificar, gestionar, tratar y mitigar los riesgos de ciberseguridad. Desde entonces, varios incidentes 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 una nueva 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 los objetivos para los próximos tres años (2022-2025).

Nuestras partes interesadas de nivel nacional han sido un apoyo fundamental para los progresos que hemos logrado hasta la fecha. Al examinar nuestras necesidades para una nueva estrategia, reconocemos la importancia de aprovechar las ventajas existentes, incluida la existencia de una política de ciberseguridad emitida según el Acuerdo Ministerial 006-2021 y de los 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.

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 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 un alto número de ciberataques maliciosos contra nuestra infraestructura crítica nacional, infraestructura tecnológica con problemas de obsolescencia, altos costos para la adquisición de tecnología y marcos legales y regulatorios desactualizados, todos los cuales nos han dejado vulnerables. Además, es necesario abordar 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 sepan cómo protegerse en línea.

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

- 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, adoptando medidas para gestionar los riesgos cibernéticos contra nuestras infraestructuras críticas nacionales y otros activos contra los riesgos cibernéticos, 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 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 cibernéticas 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 seguridad digital.

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 infraestructuras críticas, 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, que celebró varias mesas de discusión presenciales y virtuales con los interesados nacionales en ciberseguridad, guiados por personal especializado de la OEA y 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 con las iniciativas existentes y las mejora aún más.

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 TIC, el aumento de la cobertura y el acceso a los servicios móviles de alta velocidad y la mejora de la posición internacional del Ecuador en materia de ciberseguridad.

El *Plan Específico de Seguridad Pública y Ciudadana 2019-2030* fija objetivos para detener los delitos transnacionales, entre ellos el cibercrimen, 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 cibernéticas en la economía, la seguridad integral y la información, pide una cooperación efectiva entre los Estados y señala que se está analizando la viabilidad del país en adherirse al Convenio de Budapest sobre la Ciberdelincuencia.

El *Plan Específico de Defensa 2019-2030* prevé la participación activa del 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 *Plan Estratégico de Defensa Institucional 2017-2021* encomienda a las fuerzas armadas de Ecuador evaluar constantemente los escenarios de amenaza y riesgo, incluidos los relacionados con las amenazas cibernéticas, y actualizar las capacidades de defensa. El comando de ciberdefensa protege la infraestructura digital crítica del sector defensa y las áreas estratégicas del Estado, promoviendo la coordinación interinstitucional de la ciberdefensa en el marco de la ciberseguridad nacional, y aumentando las capacidades estratégicas conjuntas de las Fuerzas Armadas.

VISIÓN, PRINCIPIOS Y OBJETIVOS ESTRATÉGICOS

Para el lector (para la versión borrador): *Esta sección presenta:*

- *Declaración de Ecuador sobre la visión de la ciberseguridad para el año 2025*
- Principios rectores, priorizados y reformulados durante el taller de interesados en marzo de 2022
- Resumen de los objetivos estratégicos de la estrategia

Visión de ciberseguridad y propósito general de la estrategia de 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 sus capacidades nacionales de resiliencia cibernética, y dirige nuestras aspiraciones en este campo con una perspectiva para el período de estrategia (2022-2025).

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

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 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

Los principios rectores de la estrategia tienen por objeto 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 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 del entorno digital y en la eficiente asignación de recursos.
2. *Salvaguardar los derechos humanos y los valores fundamentales* de las personas, incluida la libertad de expresión, la libre circulación de la información, la confidencialidad de la información y las comunicaciones, entre otros.
3. *Gestión de riesgos y resiliencia*, que permiten a las personas y entidades el desarrollo libre, fiable y seguro de sus actividades en el entorno digital.

4. *Visión inclusiva y colaborativa* que involucre activamente a la sociedad civil, academia, entidades públicas y privadas, así como otros actores que permita establecer y mejorar las condiciones en el ciberespacio.

PILARES DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Objetivos estratégicos

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

1. Gobernanza y coordinación: *Establecer un enfoque coordinado de la ciberseguridad nacional*
2. Ciber resiliencia: *Mejorar la resiliencia a nivel nacional y organizacional para prepararse, responder y recuperarse de los incidentes cibernéticos*
3. Lucha contra la cibercriminalidad: *fortalecimiento de las capacidades para prevenir, investigar y perseguir los delitos cibernéticos*
4. Ciberdefensa nacional / Ciberinteligencia: *Reforzar las capacidades de ciberdefensa y desarrollar capacidades en ciberinteligencia 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 ciber 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 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 del Ecuador del gobierno, sector privado, academia y 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 del Ecuador.

Pilar 1: Gobernanza y coordinación nacional

Objetivo 1.1: Establecer un marco integral de gobernanza de la ciberseguridad
Objetivo 1.2: Apoyar a una comunidad sólida y bien conectada de expertos en ciberseguridad de las múltiples partes interesadas y comprometerse con ella
Objetivo 1.3: Desarrollar un marco legal y regulatorio integral que permita la gobernanza nacional de la ciberseguridad

Pilar 2: Resiliencia cibernética

Objetivo 2.1: Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de infraestructuras de información críticas nacionales

Objetivo 2.2: Establecer un proceso integral para la gestión de riesgos y preparación para las crisis con el fin de fortalecer dichas capacidades a nivel nacional

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

Pilar 3: Lucha contra la ciberdelincuencia

Objetivo 3.1: Actualizar el marco legal y regulatorio del Ecuador en materia de ciberdelincuencia

Objetivo 3.2: Fortalecer las capacidades judiciales y aplicación de la ley

Pilar 4: Ciberdefensa nacional y Ciberinteligencia

Objetivo 4.1: Fortalecer las capacidades institucionales y operativas de defensa, actuación y respuesta a los ciberataques

Objetivo 4.2: Establecer un proceso integral para desarrollar capacidades de ciberinteligencia

Pilar 5: Habilidades y capacidades de ciberseguridad

Objetivo 5.1: Mejorar y ampliar la concienciación sobre la ciberseguridad a todos los niveles

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

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

Pilar 6: Cooperación internacional

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

Objetivo 6.2: Fortalecer la participación del Ecuador en escenarios de cooperación bilateral, regional e internacional de respuesta a incidentes y de lucha contra la ciberdelincuencia

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

PILAR 1. GOBERNANZA Y COORDINACIÓN NACIONAL

Para el lector (para la versión borrador): *en esta sección y en las subsiguientes, se proporcionará una breve descripción del entorno actual en el Ecuador en relación con el pilar en particular, destacando las tendencias clave, los mecanismos organizacionales y jurídicos/normativos existentes y los principales desafíos percibidos.*

El enfoque consiste en definir las declaraciones claras como retos y oportunidades, que a su vez deben ser abordados por los Objetivos y Líneas de Acción. El resultado debería ser que no se detectaran problemas importantes sin una acción planificada y que no se realizarán actividades sin una justificación subyacente en los problemas identificados.

Relevancia y estado actual

La sólida colaboración y gobernanza de la ciberseguridad estratégica y operativa del Ecuador son esenciales para construir un ecosistema donde los ciberataques no puedan paralizar la economía y la sociedad del Ecuador y dejar todos los esfuerzos de digitalización ineficientes y expuestos a un mayor riesgo. Así, el 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 para 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 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 el Ecuador, ya que este es un aspecto crítico para garantizar la eficacia de la gobernanza general en todos los sectores relevantes.

Objetivos estratégicos

Para el lector (para la versión borrador): *en esta sección se establecen las principales líneas de acción y actividades prioritarias. Las declaraciones tienen por objeto reflejar ambiciones y compromisos: qué es lo que queremos y podemos comprometernos a lograr en el período de la estrategia 2022-2025, teniendo en cuenta que también nos gustaría informar de casos de éxito al final del período de la estrategia.*

Para hacer frente a los retos planteados, se perseguirán en este pilar los tres objetivos estratégicos siguientes y 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 una **sólida gobernanza**, incluido 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 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 por única vez, incorporando el presupuesto nacional y los mecanismos de apoyo.

Líneas de acción

- Establecer un marco institucional funcional con las funciones y responsabilidades prescritas de todos los agentes gubernamentales pertinentes en materia de ciberseguridad que abarque todos los objetivos estratégicos de la estrategia nacional.
- Fortalecer el rol de coordinador nacional de políticas de ciberseguridad en el MINTEL.
- Designar al Comité Nacional de Ciberseguridad como un órgano estratégico de coordinación y toma de decisiones .
- 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 es 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 presentación de informes periódicos para los indicadores clave de rendimiento y los indicadores clave de riesgo de la ciberseguridad a fin de sondear la situación y las tendencias de la ciberseguridad a nivel nacional.

Objetivo 1.2: Apoyar a una comunidad sólida y bien conectada de expertos en ciberseguridad de las múltiples partes interesadas

La gobernanza de la ciberseguridad se establecerá mediante una **coordinación inclusiva de las actividades de todas las múltiples partes interesadas pertinentes**, incluidas las entidades gubernamentales, el sector privado, las Organizaciones No Gubernamentales -ONG- y el mundo académico. Las 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 la red de intercambio, se crearía una capacidad plena de 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

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. 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.

Líneas de acción

- Efectuar un análisis exhaustivo del marco legal y regulatorio 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:
    - Definir las principales funciones y responsabilidades de ciberseguridad a nivel nacional en el marco legal y regulatorio correspondientes cuando sea necesario.
    - Orientar los cambios legislativos en todos los objetivos estratégicos de la estrategia nacional.

PILAR 2. RESILIENCIA CIBERNÉTICA

La resiliencia cibernética nacional necesita garantizar la capacidad de prepararse para los ataques cibernéticos, responder a ellos y recuperarse de ellos. Esto significa garantizar una identificación y gestión adecuadas de los riesgos cibernéticos; suficiente preparación y capacidad de respuesta frente a los ciberataques para garantizar que su impacto permanezca contenido; y, en particular, la salvaguardia de las infraestructuras y los servicios que son los más críticos para el funcionamiento de la sociedad. Así, la resiliencia cibernética está cubierta por tres objetivos estratégicos que abordan:

1. Protección de infraestructuras de información críticas nacionales
2. Gestión de riesgos y preparación ante crisis
3. Gestión de incidentes

Objetivos estratégicos

Infraestructuras de información crítica nacionales

Relevancia y estado actual

La salvaguardia de infraestructuras 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 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 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. La Infraestructura de Información Crítica (IIC) nacional se define como una parte de la infraestructura y los servicios críticos, que comprende sistemas de información y comunicación que son esenciales para el buen funcionamiento de la sociedad. La protección de la IIC debe garantizar la resiliencia frente a las infracciones o fallos en el entorno digital que puedan causar interrupciones, lo que tendría graves consecuencias para la sociedad y la economía.

En el ámbito de la protección de las IIC, hemos identificado ámbitos de oportunidad que debemos abordar, como la necesidad de elaborar una lista completa de todos los operadores de IIC a nivel nacional, 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 IIC, el establecimiento y mantenimiento de un catálogo actualizado de todos los operadores de IIC a nivel nacional es la base para permitir otros esfuerzos de mejora que garanticen una resiliencia suficiente. La protección de las IIC a nivel nacional 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 permitirán establecer mecanismos eficaces de protección de las IIC en el marco de las asociaciones entre los sectores público y privado.

Objetivo 2.1: Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de infraestructuras de información críticas nacionales

Se identificarán los activos de las IIC tanto del sector público como del privado, que son esenciales para mantener las funciones vitales de la sociedad en el Ecuador y que serán resistentes a las amenazas actuales y emergentes dentro del entorno digital. Se establecerá y mantendrá un catálogo actualizado de todos los operadores de las IIC para garantizar la recopilación y administración de datos relativos a las IIC a nivel nacional y mecanismos amplios de colaboración y cooperación. A fin de garantizar un nivel suficiente de medidas de seguridad aplicadas, se establecerán normas de referencia, directrices de apoyo y mecanismos de supervisión. Un marco legal y regulatorio complementario apoyará los mecanismos de identificación, gestión de riesgos, supervisión y comunicación de las IIC.

Líneas de acción

Identificación e intercambio de información

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

Norma de referencia, directrices y supervisión

- Establecer normas nacionales de referencia que se apliquen a todos los operadores de IIC tanto en operadores de IIC del sector privado como en activos de IIC 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

- Establecer requisitos de ciberseguridad para los operadores de IIC en el marco legal y regulatorio, cuando sea pertinente.

Gestión de riesgos y preparación para crisis

Relevancia y estado actual

La asunción 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 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 cibernéticos 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 la infraestructura de información crítica nacional, etc. A fin de identificar y gestionar eficazmente los riesgos en el ciberespacio, es esencial establecer un seguimiento continuo de las tendencias mundiales y comprender la perspectiva nacional de las ciberamenazas. 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 resistencia de las personas y las organizaciones en el Ecuador está a la zaga en lo que respecta a la capacidad para resistir a los agentes adversos, teniendo en cuenta, por ejemplo, los ataques DDoS que ha sufrido el país. Por lo tanto, el Ecuador necesita fortalecer su capacidad para hacer frente a los nuevos tipos de 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 y la preparación para las crisis, hemos identificado áreas de mejora, incluido el hecho de que actualmente se debe reforzar de manera práctica a nivel nacional las evaluaciones de riesgos, supervisión y presentación de informes. La adopción de un marco nacional amplio de gestión de los riesgos cibernéticos brinda la oportunidad de establecer un enfoque basado en los 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 ciber riesgo pertinentes pueden proporcionar una base para planes de contingencia eficaces y capacidad de ejecución.

Objetivo 2.2: Establecer un proceso integral para la gestión de riesgos y preparación para las crisis con el fin de garantizar fortalecer dichas capacidades a nivel nacional

Se establecerá la capacidad para identificar, analizar y evaluar los riesgos cibernéticos, así como para la presentación continua de informes, el seguimiento y la supervisión de las medidas de mitigación. Se elaborará un enfoque basado en los 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 de las prioridades según el perfil de riesgo nacional.

Se establecerán planes de gestión de crisis para preparar la gestión de crisis cibernéticas en las instituciones gubernamentales y el sector privado. Se establecerán y adelantarán rutinas de ejercicio para practicar la gestión de situaciones de incidente y crisis 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 directrices y un marco para la gestión del riesgo cibernético en el sistema nacional de gestión del riesgo de ciberseguridad
- 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 ataques dirigidos a las IIC e instituciones gubernamentales.

- Establecer un mecanismo de pruebas periódicas de penetración para las organizaciones del sector público y los operadores de las IIC.
- Identificar las dependencias de telecomunicaciones para la respuesta y comunicación de emergencia. Expedir regulaciones a los proveedores de redes de telecomunicaciones para que tengan redes con opciones de redundancia adecuadas.
- 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.
- 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 cibernético para los cuales se deben desarrollar planes nacionales de contingencia.
- Organizar ejercicios nacionales de ciberseguridad para probar la eficacia de los planes de contingencia.

Gestión de incidentes cibernéticos

Relevancia y estado actual

En los últimos años, Ecuador ha dado pasos bastante notables para fortalecer sus capacidades de gestión de incidentes cibernéticos. El Equipo 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. Sin embargo, su circunscripción a nivel nacional se limita a los operadores de redes de telecomunicaciones y, por lo tanto, 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 FIRST y también tiene una relación de colaboración y dinámica con los CERT regionales.

Además de EcuCERT, las competencias de gestión de incidentes se complementan con numerosos CERT operativos en los sectores académico, privado y financiero. En el ámbito de la defensa, la gestión de incidentes se encomienda al CERT militar, dependiente del Comando de Ciberdefensa (COCIBER), cuyo objetivo es la protección de la infraestructura crítica y la soberanía. Los CERT sectoriales han establecido relaciones de cooperación con sus homólogos internacionales y es probable que puedan 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 incidentes y los mecanismos son variables en las organizaciones comunitarias objetivo entre los CERT.

En el ámbito de la gestión de incidentes, hemos identificado los ámbitos de oportunidad, como 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 debe proporcionar disposiciones de trabajo nacionales claramente definidas para el intercambio de información y la respuesta a incidentes, ya que la falta de un marco de apoyo plantea un riesgo para la protección adecuada de los activos de infraestructura crítica en el país. Se deben realizar

esfuerzos para formalizar los mecanismos de coordinación y notificación de incidentes a nivel nacional, ya que se trata de un elemento clave de una respuesta bien estructurada y organizada a los incidentes.

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

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

Líneas de acción

- A fin de mejorar las capacidades de gestión de incidentes, es de suma importancia habilitar procesos, herramientas y conocimientos para gestionar las amenazas e incidentes de ciberseguridad en la red gubernamental. Con ese fin, el Ecuador trabajará para establecer un Centro de Operaciones de Seguridad (gubernamental) nacional (gSOC) con una misión clara basada en un mandato.
- Para permitir modelos nacionales armonizados de gestión de incidentes cibernéticos, revisaremos y estableceremos el marco legislativo necesario con competencias y tareas claras para cada una de las partes interesadas, además de establecer informes de incidentes obligatorios. Adoptaremos una normativa que establezca un CERT nacional, sus funciones y responsabilidades y mecanismos de supervisión para incluir la vigilancia de incidentes a nivel nacional, proporcionando alertas tempranas, anuncios y difundiendo información sobre amenazas a las partes interesadas pertinentes, proporcionando análisis periódicos de riesgos e incidentes y coordinando la respuesta a incidentes a nivel nacional.
- Invertiremos en maximizar las asociaciones dentro de las comunidades del CERT con ejercicios y programas de capacitación sobre prevención, respuesta y recuperación de incidentes cibernéticos.
- Estableceremos un mecanismo para la divulgación periódica de vulnerabilidades y el intercambio de información entre los operadores de las IIC y el gobierno de Ecuador.

PILAR 3. LUCHA CONTRA 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 criminales. La pandemia de COVID-19 ha acelerado este proceso debido a muchas más transacciones y actividades que se mueven en línea. El número de delitos cibernéticos está aumentando en el 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.

Según la evaluación de la Policía Nacional del 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; aunque lo hagan, no saben cómo denunciar este tipo de incidentes; y a menudo no confían en que la aplicación de la ley puede ayudar, ya que la investigación y el enjuiciamiento tardan mucho debido a las capacidades limitadas de la aplicación de la ley. Todos estos factores conducen a que el delito cibernético no se denuncie.

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.

El débil marco legal ha sido un problema durante mucho tiempo, con definiciones legales de delito cibernético obsoletas y deficientes. El Ecuador se encuentra actualmente en proceso de adhesión a la Convención de Budapest sobre el Delito Cibernético, que debería ayudar tanto al enjuiciamiento nacional como a la agilización de la cooperación internacional en materia de delito cibernético. El proceso de adhesión requiere la aplicación de las disposiciones de la Convención en la legislación nacional del Ecuador.

La Unidad de Investigación de Delitos Tecnológicos de la Policía Nacional del Ecuador existe desde hace más de una década y ha adquirido notables conocimientos especializados, pero carece de financiación específica y de una perspectiva de personal sostenible. Ecuador es miembro de AMERIPOL e INTERPOL, con acceso a intercambio de información en tiempo real.

En la esfera de la lucha contra la delincuencia cibernética, 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 de Ecuador contra los actores criminales que abusan del ciberespacio, se implementarán acciones en dos áreas: actualización de la legislación sobre ciberdelincuencia en lo que respecta a la legislación sustantiva y procesal, y 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 y delitos 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 del Ecuador en materia de ciberdelincuencia

Líneas de acción

- Adoptar medidas legislativas para definir claramente lo que constituye delito cibernético y los delitos conexos (delitos contra o por medio de los sistemas informáticos o datos informáticos), teniendo en cuenta la armonización con los instrumentos jurídicos internacionales y regionales existentes, en particular el Convenio de Budapest sobre el delito cibernético.
- Adoptar medidas legislativas para definir el mandato legal y la autoridad de las fuerzas del orden, las autoridades ejecutivas y los proveedores de servicios digitales a efectos de la prevención del delito cibernético.
- Adoptar medidas legislativas para establecer facultades y procedimientos adecuados para la aplicación de la ley, el enjuiciamiento y la judicialización para la investigación y el enjuiciamiento de delitos cibernéticos, incluida la recopilación y el procesamiento de pruebas electrónicas y de instrumentos para una cooperación internacional rápida y eficaz en armonía con la Convención de Budapest y otros instrumentos internacionales.

Objetivo 3.2: Fortalecer las capacidades judiciales y de aplicación de la ley

Líneas de acción

- Dotar a la unidad o unidades especializadas en delitos tecnológicos de la Policía Nacional de las capacidades forenses digitales apropiadas, procedimientos operativos estándar y mecanismos de denuncia de delitos comunicados al público.
- 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.
- Identificar y desarrollar oportunidades de capacitación y proporcionar 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.

PILAR 4. Ciberdefensa nacional y ciberinteligencia

Relevancia y estado actual

El ciberespacio ha sido reconocido como un componente adicional del territorio ecuatoriano, según el Plan Específico de Defensa Nacional 2019-2030. La ciberdefensa juega un papel predominante en el sistema nacional de ciberseguridad para mitigar las amenazas en el ciberespacio para todos los ecuatorianos. Defender la infraestructura de información crítica, tanto en Ecuador como en sitios diplomáticos, bases militares, oficinas consulares y oficinas comerciales, es uno de los principales objetivos de la ciberdefensa.

En la actualidad, las estructuras nacionales de defensa y seguridad dependen en gran medida del uso de las tecnologías de la información y las comunicaciones (TIC) y de una variedad de infraestructuras digitales esenciales. El desarrollo de operaciones en el ámbito de la defensa tiene por objeto contribuir a la ciberseguridad nacional, con el objetivo último de proteger la soberanía del país. Ecuador está comprometido a contribuir al desarrollo de la capacidad nacional de resistencia, para enfrentar las amenazas que surgen en el ciberespacio, manteniendo la paz y protegiendo a la población y sus recursos.

En el ámbito de la ciberdefensa nacional, hemos identificado áreas de oportunidad para abordar, incluyendo la falta de entendimiento común sobre la naturaleza de la escalada de los ciber eventos que, a su vez, plantea desafíos para prevenir y resistir los ciberataques y crisis a gran escala. La dinámica cambiante de las amenazas cibernéticas requiere un enfoque holístico y una cooperación más estrecha, así como líneas de acción coordinadas entre los CERT (nacional, de sectores y militares) para garantizar la protección nacional de alto nivel de la infraestructura digital crítica y los servicios esenciales.

Objetivos estratégicos

Objetivo 4.1: Reforzar las capacidades institucionales y operativas de defensa, actuación y respuesta a los ciberataques

Líneas de acción

- Redactar escenarios de ciber crisis para la defensa y probar medidas de respuesta de ciberdefensa
- Redactar lineamientos para la defensa del IIC en las áreas reservadas de seguridad en el ciberespacio en coordinación con la política exterior ecuatoriana
- Desarrollar y aplicar un sistema y plan nacional de gestión de crisis.
- Desplegar pruebas periódicas de la resiliencia cibernética ante diferentes escenarios de ataques cibernéticos que afecten la seguridad del estado.
- Desarrollar ciber simulacros nacionales con métricas definidas para evaluar los resultados e involucrar a las múltiples partes interesadas relevantes del ecosistema
- Contribuir a la resiliencia cibernética colaborativa nacional a través de ejercicios técnicos y juegos de guerra cibernética junto con el CERT, los operadores de IIC y los proveedores de servicios esenciales.

Objetivo 4.2: Establecer un proceso integral para desarrollar capacidades de ciberinteligencia

Líneas de acción

- Desarrollar un observatorio del ciberespacio
- Desarrollar actividades de prevención y anticipación de alertas tempranas de ciberataques avanzados que sirva para asesorar en la toma de decisiones al más alto nivel del Estado
- Redactar procesos y procedimientos para el ciclo de inteligencia, así como para llevar acabo los tipos de ciberinteligencia como estratégica, técnica y táctica.
- Establecer herramientas de ciberinteligencia y métodos para compartir las alertas con las instituciones

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 el 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 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 y los planes de estudio escolares no abordan el tema de manera sistemática. Las universidades ofrecen algunos cursos relacionados con la ciberseguridad en universidades públicas y privadas 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 para abordar, 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 legales. Además, se ha determinado la necesidad de mejorar la concienciación 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 escolares y universitarios no proporcionan actualmente apoyo suficiente para desarrollar profesionales calificados, ni proporcionan una ciber 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.

Objetivos estratégicos

Objetivo 5.1: Mejorar y ampliar la concienciación sobre la ciberseguridad a todos los niveles

Se fomentarán los conocimientos sobre ciberseguridad con el objetivo de fortalecer la cultura de ciberseguridad que abarca desde los ciudadanos hasta las entidades públicas y privadas y genera una conciencia compartida de los riesgos y 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 (ancianos, jóvenes, profesionales, funcionarios gubernamentales) 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.

Objetivo 5.2: Reforzar las habilidades de ciberseguridad necesarias en 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 que desempeñen funciones específicas en la tarea de garantizar la ciberseguridad nacional tanto en las instituciones gubernamentales, los operadores de las IIC, la industria y la investigación académica. El éxito de la ciberseguridad nacional se basa en una fuerza de trabajo calificada y ciberculta y, por tanto, en un sistema educativo capaz de desarrollar esas capacidades.

Líneas de acción

- Crear un programa de formación continua sobre prevención, 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 los incidentes a medida que se producen.
- Preparar un programa de desarrollo de competencias para profesionales de organizaciones públicas.
- Desarrollar un programa de desarrollo de habilidades para profesionales de organizaciones privadas, haciendo énfasis en las pequeñas y medianas empresas (PYMES).

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

Líneas de acción

- Establecer una red de puntos de contacto 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 materia de ciberseguridad en los planes de estudio de todos los niveles educativos.
- 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 en el ciberespacio. 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. El Ecuador está interesado en que su voz e intereses sean escuchados en la agenda digital mundial y regional 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.

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 con la Convención de Budapest sobre el Delito Cibernético 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 y en los formatos de lucha contra la ciberdelincuencia.

Objetivos estratégicos para la cooperación internacional

Objetivo 6.1: Identificar las prioridades internacionales del 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 cibernormas, 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 diplomacia cibernética y desarrollo 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.
- Posicionar los 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, la gestión de incidentes 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 2: Fortalecer la participación del Ecuador en escenarios de cooperación bilateral, regional e internacional de respuesta a incidentes y de lucha contra la ciberdelincuencia

Líneas de acción

- Procurar ampliar y formalizar la cooperación con otros organismos nacionales e internacionales de respuesta a incidentes activos en la región, como el FIRST (Forum of Incident Response and Security Teams).
- Profundizar y formalizar la participación en mecanismos de coordinación y cooperación internacionales y regionales para combatir el cibercrimen a través del intercambio de información, investigaciones transfronterizas, operaciones y arrestos.
- Apoyar a las partes interesadas para que se adhieran a los mecanismos internacionales de cooperación, colaboración y asistencia (incluida la capacitación, ejercicios internacionales, etc.)
- 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 (GLACY+, INTERPOL, OEA, entre otros)

IMPLEMENTACIÓN, SEGUIMIENTO Y EVALUACIÓN

La implementación de la Estrategia Nacional de Ciberseguridad del Ecuador estará a cargo del *Comité Nacional de Ciberseguridad* con el apoyo del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). 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 del 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 desarrolla en mayor detalle en este capítulo e indicará las entidades responsables de cada acción, los periodos de ejecución de estas, los recursos necesarios y disponibles para llevarlas a cabo, y la importancia de cada acción para el cumplimiento de la propósito general y de los objetivos específicos bajo cada pilar de la estrategia nacional. El *Coordinador Nacional de Ciberseguridad* adelantará trimestralmente actividades de monitoreo y evaluación de la implementación de la Estrategia y presentará informes anuales al *Comité Nacional de Ciberseguridad*.

Ecuador adelantará 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.

Por último, también se prevé la revisión y actualización de la Estrategia cada tres (3) años o según sea necesario.

Pilar 1. ***Gobernanza y coordinación nacional***

Objetivo 1: ***Establecer un marco integral de gobernanza de la ciberseguridad***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Fortalecer la instancia de coordinación nacional para dirigir la implementación de la política nacional y llevar a cabo un seguimiento continuo	Comité/Consejo Nacional de Ciberseguridad	PRESIDENCIA	MINTEL	X	X	x	X
Adaptar y fortalecer la instancia de máximo nivel intragubernamental e intersectorial para orientar estratégicamente la gestión de la ciberseguridad	Comité/Consejo Nacional de Ciberseguridad	MINTEL	Entidades del Gobierno	X			
Establecer y poner en marcha un marco de gobernanza con las funciones y responsabilidades prescritas	Marco de gobernanza	MINTEL	MINTEL	X			
Crear una herramienta de seguimiento y evaluación del cumplimiento de los objetivos estratégicos de la Estrategia Nacional de Ciberseguridad de acuerdo con el plan de implementación.	Herramienta de seguimiento	MINTEL	Comité Nacional de Ciberseguridad Entidades del Gobierno		X	X	
Establecer un mecanismo regular 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	MINTEL	Comité Nacional de Ciberseguridad Entidades del Gobierno		X	X	X

Pilar 1. ***Gobernanza y coordinación nacional***

Objetivo 2: ***Apoyar a una comunidad sólida y bien conectada de expertos en ciberseguridad de las múltiples partes interesadas y comprometerse con ella***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Establecer y poner en marcha un mecanismo efectivo de asociación entre los sectores público y privado para la consulta sobre cuestiones cibernéticas, el intercambio de información y la coordinación de actividades en las que participen una amplia gama de interesados pertinentes de las instituciones gubernamentales, el sector privado, el mundo académico y las ONG.	Mecanismo	MINTEL	Comité Nacional de Ciberseguridad Policía Nacional Ministerio de Defensa Nacional Asociaciones a fines	X	X		

Pilar 1. ***Gobernanza y coordinación nacional***

Objetivo 3: ***Desarrollar un marco legal y regulatorio integral que permita la gobernanza nacional de la ciberseguridad***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Establecer y ejecutar un plan de actualización y reforma detallada del marco legal vigente e identificar oportunidades de mejora para recomendar y aplicar las modificaciones correspondientes	Plan de actualización	MINTEL Ministerio de Defensa Nacional Función Judicial Asamblea Nacional del Ecuador Fiscalía General del Estado	Comité Nacional de Ciberseguridad Entidades del Gobierno Asociaciones a fines		X	X	
Establecer y ejecutar una plan de actualización y reforma periódica del marco regulatorio, considerando la naturaleza cambiante de la materia.	Plan de actualización	MINTEL Ministerio de Gobierno	ARCOTEL Superintendencia de Bancos Autoridad de Protección de Datos Personales SEPS Cámaras de Comercio, Industrias y afines		X	X	
Coordinar la entrega de una propuesta de Ley de Ciberseguridad	Propuesta de Ley de Ciberseguridad	MINTEL Ministerio de Gobierno Ministerio de Defensa Nacional Función Judicial Asamblea Nacional del Ecuador Fiscalía General del Estado	Comité Nacional de Ciberseguridad Entidades del Gobierno Asociaciones a fines		X	X	

Pilar 2: ***Resiliencia cibernética***

Objetivo 1: ***Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de infraestructuras de información crítica nacionales (IIC)***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Establecer un marco normativo y una metodología para la identificación de las IIC	Marco normativo y metodología	MINTEL	Comité Nacional de Ciberseguridad Ministerio de Defensa Nacional	X			
Definir los sectores estratégicos que contemplan el concepto de protección de servicios e infraestructura esencial	Sectores estratégicos	Ministerio de Defensa Nacional	Comité Nacional de Ciberseguridad MINTEL	X			
Identificar y mantener un registro actualizado de los operadores de las IIC basado en consideraciones sociales, económicas y ambientales, incluyendo un único punto de contacto asignado para cada operador	Registro actualizado de operadores de las IIC a nivel nacional	Ministerio de Defensa Nacional	Coordinador Nacional MINTEL	X			
Establecer y poner en marcha un mecanismo de cooperación y coordinación de las asociaciones público-privadas entre los operadores de las IIC basado en la creación de confianza	Mecanismo de cooperación y coordinación para las IIC	MINTEL	Comité Nacional de Ciberseguridad Ministerio de Defensa		X	X	
Establecer y poner en marcha un mecanismo de divulgación periódica de vulnerabilidades, e intercambio de información entre los operadores de IIC y el gobierno del Ecuador	Mecanismo para la divulgación periódica de la vulnerabilidad y el intercambio de información para las IIC	MINTEL	Comité Nacional de Ciberseguridad Ministerio de Defensa Nacional ASOBANCA		X	X	
Establecer y aplicar un estándar de referencia nacional para los operadores de IIC, aplicable tanto a los operadores de IIC del sector privado como a los activos de IIC de las instituciones públicas	Estándar de referencia nacional para el operador IIC	MINTEL	Comité Nacional de Ciberseguridad Ministerio de Defensa Nacional		X	X	X
Preparar y publicar guías con medidas, buenas prácticas y directrices para los operadores de las IIC	Directrices para las IIC	MINTE	Comité Nacional de Ciberseguridad Ministerio de Defensa Nacional		X	X	X
Establecer y ejecutar planes de protección y defensa para las IIC	Planes de protección y defensa para las IIC	MINTEL	Coordinador Nacional Ministerio de Defensa Nacional		X	X	X
Establecer e implementar una estrategia de evaluación de ciberseguridad para los operadores de IIC	Estrategia de auditoría de ciberseguridad para IIC	MINTEL	Coordinador Nacional Ministerio de Defensa Nacional		X	X	X

Pilar 2: ***Resiliencia cibernética***

Objetivo 2: ***Establecer un proceso integral para la gestión de riesgos y preparación para las crisis con el fin de fortalecer dichas capacidades a nivel nacional***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
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	MINTEL	Comité Nacional de Ciberseguridad MINTEL ASOBANCA Superintendencia de Bancos SEPS Cámaras de Comercio, Industrias y afines Asociaciones a fines	X			
Establecer y aplicar un marco de gestión de riesgos cibernéticos para el sistema nacional de gestión de riesgos de seguridad cibernética	Marco de gestión del riesgo cibernético	MINTEL	Coordinador Nacional	X	X		

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Identificar tipos comunes de ataques contra el IIC y las instituciones gubernamentales	Informes periódicos con tipos comunes de ataques	MINTEL	Coordinador Nacional Ministerio de Defensa Nacional	X	X		
Establecer un mecanismo de pruebas periódicas de penetración para las organizaciones del sector público y los operadores de las IIC	Mecanismo de las pruebas de penetración	MINTEL Ministerio de Defensa Nacional	Coordinador Nacional		X	X	
Crear un programa de coordinación designado para la adopción de normas de ciberseguridad y mejores prácticas	Programa de adopción de normas	MINTEL	Comité Nacional de Ciberseguridad MINTEL		X	X	
Establecer planes de gestión de crisis cibernéticas	Planes de gestión de crisis cibernéticas	MINTEL	Comité Nacional de Ciberseguridad MINTEL		X	X	
Identificar escenarios de riesgo cibernético para los cuales se deben desarrollar planes nacionales de contingencia.	Informes periódicos con escenarios de riesgo	MINTEL	Comité Nacional de Ciberseguridad		X	X	
Organizar ejercicios nacionales de ciberseguridad para probar la eficacia de los planes de contingencia.	Ejercicios nacionales de ciberseguridad	MINTEL	Comité Nacional de Ciberseguridad Ministerio de Defensa Nacional		X	X	X

Pilar 2: ***Resiliencia cibernética***

Objetivo 3: ***Continuar desarrollando capacidades de respuesta y gestión de incidentes y el CERT nacional***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Crear un CERT a nivel nacional	Plan para crear y fortalecer el CERT a nivel nacional	MINTEL	Comité Nacional de Ciberseguridad	x	X		
Crear y ejecutar una estrategia para crear nuevos equipos de respuesta CSIRT y fortalecer los actuales	Estrategia de equipos de respuesta CSIRT	MINTEL	Coordinador Nacional Ministerio de Defensa CEDIA ARCOTEL CERT privados		x	X	
Establecer y ejecutar un plan para generar un marco jurídico para contar con: i) un equipo de respuesta a incidentes de alcance nacional y, ii) un sistema nacional de gestión y respuesta a incidentes	Plan para generar un marco jurídico	MINTEL	Comité Nacional de Ciberseguridad Ministerio de Defensa Ministerio del Interior	x	x	x	
Crear y poner en funcionamiento un Centro de Operaciones de Seguridad (SOC) nacional (gubernamental)	gSOC del Gobierno	MINTEL	Coordinador Nacional Ministerio de Defensa Nacional Instituciones públicas			x	X

Pilar 3: ***Lucha contra la ciberdelincuencia***

Objetivo 1: ***Actualizar el marco legal y regulatorio del Ecuador en materia de ciberdelincuencia***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Establecer y ejecutar una estrategia nacional de revisión de la legislación penal nacional con miras a definir claramente lo que constituye delito cibernético y delitos conexos (delitos contra o por medio de sistemas o datos informáticos), considerando la posibilidad de armonizar con los instrumentos jurídicos internacionales y regionales existentes (incluido el Convenio de Budapest)	Estrategia de revisión normativa	Ministerio de Gobierno	Coordinador Nacional MINTEL Fiscalía General del Estado Asamblea Nacional del Ecuador Corte Nacional de Justicia		X	X	
Definir 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.	Mandato jurídico	Ministerio de Gobierno	Coordinador Nacional MINTEL Ministerio de Defensa Nacional Policía Nacional Fiscalía General del Estado		X	X	X
Establecer facultades procesales adecuadas para la aplicación de la ley, el enjuiciamiento y el poder judicial para la investigación y el enjuiciamiento de delitos cibernéticos, incluida la recopilación y el procesamiento de pruebas electrónicas,	Mandato jurídico	Ministerio de Gobierno	Coordinador Nacional MINTEL Ministerio de Defensa Nacional Policía Nacional Fiscalía General del Estado Corte Nacional de Justicia			X	X
Establecer y aplicar instrumentos para una cooperación internacional rápida y eficaz en casos de delitos cibernéticos	Instrumentos de cooperación internacional	Ministerio de Relaciones Exteriores y Movilidad Humana	Coordinador Nacional MINTEL Ministerio de Defensa Nacional Policía Nacional Fiscalía General del Estado Corte Nacional de Justicia		X	X	X
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 arrestos.	Acuerdos de cooperación internacional	Ministerio de Relaciones Exteriores y Movilidad Humana	Comité Nacional de Ciberseguridad MINTEL Ministerio de Defensa Nacional Policía Nacional		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 como (GLACY+, INTERPOL, OEA, entre otros)	Acciones de cooperación internacional	Ministerio de Relaciones Exteriores y Movilidad Humana	Comité Nacional de Ciberseguridad MINTEL Ministerio de Defensa Nacional Policía Nacional		X	X	X

Pilar 3: ***Lucha contra la ciberdelincuencia***

Objetivo 2: ***Fortalecer las capacidades judiciales y de aplicación de la ley***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Establecer unidades especializadas en delitos cibernéticos dentro de las entidades encargadas, dotándolas de capacidades forenses digitales apropiadas, procedimientos operativos estándar y mecanismos de denuncia de delitos divulgados públicamente.	Unidad o unidades especializadas en ciberdelincuencia	Ministerio de Gobierno Fiscalía General del Estado Corte Nacional de Justicia	Comité Nacional de Ciberseguridad MINTEL Policía Nacional Ministerio de Relaciones Exteriores y Movilidad Humana	X	X		
Establecer y ejecutar un plan de formación para fiscales y jueces especializados en casos de delitos cibernéticos y casos relacionados con pruebas electrónicas	Plan de formación	Consejo de la Judicatura/Fiscalía General del Estado	Comité Nacional de Ciberseguridad MINTEL Fiscalía General del Estado Corte Nacional de Justicia Policía Nacional SECAP	X	X		

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
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 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	Comité Nacional de Ciberseguridad MINTEL SECAP Policía Nacional		X	X	
Establecer y ejecutar un programa de capacitación y educación para profesionales de la justicia penal (jueces, fiscales, abogados y otros)	Programa de capacitación para profesionales de la justicia penal	Ministerio de Educación Fiscalía General del Estado/Consejo de la Judicatura	Comité Nacional de Ciberseguridad MINTEL Asociaciones a fines Ministerio del Interior		X	X	
Establecer y ejecutar un programa de capacitación para el personal involucrado y contar con educación superior especializada para contar con un conjunto de herramientas existentes, aprovechando al máximo la tecnología en la lucha contra el delito cibernético.	Programa de formación	SENESCYT	Comité Nacional de Ciberseguridad MINTEL CES		X	X	

Pilar 4: ***Ciberdefensa nacional y Ciberinteligencia***

Objetivo 1: ***Reforzar las capacidades institucionales y operativas de defensa, actuación y respuesta a los ciberataques***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Identificar tácticas, técnicas, procedimientos y lecciones aprendidas, más utilizadas en el marco de operaciones cibernéticas aplicables a Seguridad y Defensa	Informes periódicos con tácticas, técnicas, procedimientos y lecciones aprendidas	Ministerio de Defensa Nacional	Comité Nacional de Ciberseguridad MINTEL	X	X		
Establecer y ejecutar un plan para generar un marco legal que fortalezca y proteja la infraestructura de defensa y seguridad nacional.	Plan para generar un marco legal	Ministerio de Defensa Nacional	Comité Nacional de Ciberseguridad MINTEL	X	X		
Desarrollar un Plan de Ejercicio de Ciberdefensa para fortalecer las operaciones de ciberdefensa.	Plan de ejercicios de ciberdefensa	Ministerio de Defensa Nacional	Coordinador Nacional MINTEL	X	X	X	
Elaborar una propuesta de Estrategia de Ciberdefensa para el sector militar del país	Estrategia de ciberdefensa	Ministerio de Defensa Nacional	Coordinador Nacional MINTEL	X	X	X	
Establecer y ejecutar un programa para fortalecer las capacidades cibernéticas de los responsables de la seguridad nacional y la infraestructura de defensa.	Programa de fomento de la capacidad	Ministerio de Defensa Nacional	Coordinador Nacional MINTEL		X	X	X
Establecer y ejecutar un programa de fortalecimiento de las capacidades de ciberseguridad y ciberdefensa de los responsables de la infraestructura informática en las unidades militares.	Programa de fomento de la capacidad	Ministerio de Defensa Nacional	Coordinador Nacional MINTEL		X	X	X

Pilar 4: ***Ciberdefensa nacional y Ciberinteligencia***

Objetivo 2: ***Establecer un proceso integral para desarrollar capacidades de ciberinteligencia***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Establecer con roles y funciones el observatorio del ciberespacio	Observatorio del Ciberespacio	CIES	Comité Nacional de Ciberseguridad MINTEL	X	X		
Establecer el proceso de prevención y anticipación de alertas tempranas ante ciberamenazas avanzadas	Proceso de prevención y anticipación de alertas	CIES	Comité Nacional de Ciberseguridad MINTEL	X	X	X	
Establecer el ciclo de inteligencia y sus fases aplicados a la ciberinteligencia	Ciclo de ciberinteligencia	CIES	Comité Nacional de Ciberseguridad MINTEL	X	X	X	
Establecer los tipos de ciberinteliencia y como actuar homologada mente con las instituciones del estado.	Metodología para el menejo de los tipos de inteligencia.	CIES	Comité Nacional de Ciberseguridad MINTEL	X	X	X	

Pilar 5: ***Habilidades y capacidades de ciberseguridad***

Objetivo 1: ***Mejorar y ampliar la concienciación sobre la ciberseguridad a todos los niveles***

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	Coordinador Nacional Ministerio de Educación	X	X	X	

Pilar 5: ***Habilidades y capacidades de ciberseguridad***

Objetivo 2: ***Reforzar las habilidades de ciberseguridad necesarias en las múltiples partes interesadas***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Desarrollar e implementar un programa de capacitación permanente sobre prevención, respuesta y recuperación de incidentes cibernéticos para el personal de TI en las instituciones gubernamentales a fin de prepararlos para responder a los incidentes a medida que ocurren	Programa de formación continua	MINTEL	Coordinador Nacional MINTEL	X	X	X	
Establecer un perfil y roles así como actividades para el Oficial de Seguridad de la Información en las instituciones de la administración pública central	Aprobación de perfil y rol del OSI en el Ministerio del Trabajo	MINTEL/MINISTERIO DEL TRABAJO	Asociaciones a fines Superintendencia de Bancos		X	X	
Preparar e implementar un programa de desarrollo de habilidades para profesionales de organismos públicos	Programa de desarrollo de capacidades	Ministerio de Trabajo	Coordinador Nacional MINTEL		X	X	
Preparar y aplicar un programa de desarrollo de competencias para profesionales de organizaciones privadas, con especial hincapié en las PYMES	Programa de desarrollo de capacidades	MINTEL Ministerio del Trabajo (SETEC) SECAP	Coordinador Nacional Asociaciones a fines Ministerio de Producción Comercio Exterior, Inversiones y Pesca		X	X	

Pilar 5: ***Habilidades y capacidades de ciberseguridad***

Objetivo 3: ***Permitir 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 para la educación en ciberseguridad en diferentes sectores, instituciones educativas y agencias gubernamentales	Red de puntos de contacto para la educación	MINTEL	Comité Nacional de Ciberseguridad Ministerio de Educación	X			
Elaborar y ejecutar un plan nacional de educación en ciberseguridad en las instituciones de educación	Plan nacional de educación	Ministerio de Educación	Comité Nacional de Ciberseguridad MINTEL		X	X	
Crear contenidos educativos complementarios dirigidos a docentes y estudiantes de educación primaria, secundaria y superior	Contenido educativo	Ministerio de Educación CES	Comité Nacional de Ciberseguridad MINTEL SENESCYT		X	X	
Incluir contenidos educativos en los planes de estudio de todos los niveles educativos	Currículos educativos con contenido incluido	Ministerio de Educación CES	Comité Nacional de Ciberseguridad MINTEL SENESCYT			X	X

Pilar 6: ***Cooperación internacional***

Objetivo 1: ***Identificar las prioridades internacionales del Ecuador y desarrollar la capacidad de participar en la ciberdiplomacia regional e internacional***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Establecer y aplicar una estrategia de intercambio y transferencia de conocimientos	Estrategia de intercambio y transferencia de conocimientos	Ministerio de Relaciones Exteriores y Movilidad Humana	Coordinador Nacional MINTEL	X	X		
Identificar y participar en espacios/escenarios/debates internacionales	Espacios / escenarios / debates internacionales	Ministerio de Relaciones Exteriores y Movilidad Humana	Coordinador Nacional MINTEL Ministerio de Defensa Nacional Policía Nacional	X	X	X	X
Preparar informes periódicos para supervisar la cooperación internacional	Informes periódicos	Ministerio de Relaciones Exteriores y Movilidad Humana	Coordinador Nacional MINTEL		X	X	X

Pilar 6: ***Cooperación internacional***

Objetivo 2: ***Fortalecer la participación del Ecuador en escenarios de cooperación bilateral, regional e internacional de respuesta a incidentes y de lucha contra la ciberdelincuencia***

Acción	Entregable	Responsable	Soporte	Corto plazo	Mediano plazo		Largo plazo
Definir y aplicar mecanismos de cooperación, colaboración y asistencia internacionales	Cooperación, colaboración y mecanismos de asistencia	Ministerio de Relaciones Exteriores y Movilidad Humana	Coordinador Nacional MINTEL Ministerio de Defensa Nacional Policía Nacional	X	X		
Continuar la adhesión a los instrumentos internacionales de lucha contra la ciberdelincuencia	Adhesión a instrumentos internacionales	Ministerio de Relaciones Exteriores y Movilidad Humana	Coordinador Nacional MINTEL Ministerio de Defensa Nacional Policía Nacional	X	X	X	X
Identificar y adherirse a los acuerdos de cooperación bilaterales y multilaterales pertinentes en el ámbito de la ciberseguridad y la lucha contra la ciberdelincuencia	Acuerdos de cooperación bilaterales y multilaterales	Ministerio de Relaciones Exteriores y Movilidad Humana	Coordinador Nacional MINTEL Ministerio de Defensa Nacional Policía Nacional	X	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*.

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 el Ecuador
Cantidad de normativas y estándares publicados	Normas	Anual	4	6	8	MINTEL Entidades Reguladoras
Numero alianzas de cooperación establecidas en materia de ciberseguridad, ciberdelito y ciberdefensa.	Alianzas	Anual	5	10	15	Coordinador Ministerio de Relaciones Exteriores y Movilidad Humana
Cantidad de simulacros nacionales realizados en materia de crisis cibernética	Simulacros	Anual	3	6	9	MINTEL CERT Nacional EcuCERT Nacional
Porcentaje de instituciones que han adoptados normativas de ciberseguridad	Instituciones públicas	Anual	20%	40%	60%	Coordinador MINTEL
Porcentaje de instituciones con infraestructura critica cumpliendo la normativa de infraestructura crítica	% de instituciones	Anual	20%	40%	60%	Coordinador 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%	Coordinador MINTEL 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 MinEducación
Número de estudiantes de nivel intermedio sensibilizados en Ciberseguridad (sector público y privado)	% de estudiantes de nivel intermedio	Anual	20%	40%	60%	Coordinador MinEducación
Número de docentes de nivel básico, intermedio y nivel superior sensibilizados en Ciberseguridad (sector público y privado)	% de docentes	Anual	20%	40%	60%	Coordinador MinEducación Senescyt
Número de encuestas realizadas sobre el nivel de conocimiento en Ciberseguridad a la población	Encuestas	Anual	1	2	3	Coordinador MINTEL