REPÚBLICA DEL ECUADOR

ASAMBLEA NACIONAL

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

HWCPOAOXQK

Trámite 359393
Código validación HWCPOAOXQK
Tipo de documento MEMORANDO INTERNO
Fecha recepción 28-mar-2019 16:57
Numeración documento 032-jcy-an-2019
Fecha oficio 28-mar-2019
Remitente YAR ARAUJO JUAN CARLOS
Función remitente ASAMBLEISTA
Revise el estado de su trámite en:
http://tramites.asambleanacional.gob.ec/dts/estadoTramite.jsf

Oficio : 1 foja
anexo : 13 fs

Quito, 28 de marzo del 2019
Oficio-N° 032-JCY-AN-2019

Economista
Elizabeth Cabezas
Presidenta de la Asamblea Nacional.

Presente

De mi consideración

Con un cordial y atento saludo deseándole éxitos en el desarrollo de sus funciones.

De conformidad con lo establecido en el numeral 1 del artículo 134 de la Constitución de la República del Ecuador, en concordancia con el numeral 1 del artículo 54 de la Ley Orgánica de la Función Legislativa remito a usted el ''PROYECTO DE LEY DE SEGURIDAD DIGITAL'' a fin de que se proceda con dar el trámite legal correspondiente.

Adjunto a la presente se servirá encontrar las firmas de apoyo correspondientes.

Con sentimientos de consideración y estima.

Atentamente,

Juan Carlos Yar

Asambleísta por la Provincia del Carchi

REPÚBLICA DEL ECUADOR

ASAMBLEA NACIONAL

FIRMAS DE APOYO A LA LEY DE SEGURIDAD DIGITAL

NOMBRE	FIRMA
Gissela Acosta	
Javier Belisario Marín	
Kevin Plaza C.	
Kharla Chavez	
Rafael Quijije	
CESAR CARRIÓN	
Daniel Mendoza	
Ximena Peña	
JORGE CORDOVA	

EXPOSICIÓN DE MOTIVOS

La Constitución de la República del Ecuador, en el año 2018, reconoció la seguridad como integral, y categorizarla como seguridad ciudadana y seguridad humana, porque que el articulo 3, numeral 8, garantiza el deber fundamental del estado ecuatoriano a sus ciudadanos el derecho de una cultura de paz.

El Ecuador necesita un instrumento legal que normativice la seguridad digital procura crear las condiciones normativas para la protección del bien jurídico de la paz social, de acuerdo a los nuevos avances tecnológicos y la globalización en general.

Es importante destacar que el proyecto de ley que se pone a consideración de la Asamblea Nacional contempla el rediseño de la institucionalizada cargo de la seguridad, reglamentando y facultando la inteligencia cibernética en relación a un sistema conciso necesario para nuestro país.

A ese respecto, es preciso señalar que la Ley de Seguridad Digital debe cumplir como propósito básico el ser un instrumento del Estado de Derecho para garantizar la vigencia plena de los derechos humanos y la paz social, la soberanía e integridad territorial del Estado ecuatoriano, el combate al crimen organizado en todas sus formas y para servir como medio para la mitigación de riesgos derivados de conflictos externos y domésticos, situaciones de grave conmoción interna y desastres naturales.

La Seguridad Digital servirá para detectar y bloquear a los hackers que intenten hacer interferencias y romper las redes informáticas de todos los sistemas que existen en el país, contando con una cooperación internacional.

Es importante destacar que existe un único Instrumento Internacional, como el Convenio de Budapest, que el Ecuador no ha signado su adherencia, lo que ha dejado que no estemos en las mismas condiciones como nuestros países vecinos que han hecho esfuerzos en el desarrollar normativa en Seguridad Digital o Ciberseguridad.

Este Proyecto de Ley debe ser considerada como una primera respuesta a las Amenazas y los riesgos globales en razón que afectan tanto a la seguridad interna y externa se está desvaneciendo como resultado de cambios como el de la globalización de la inseguridad.

La gravedad y frecuencia de los fenómenos criminales afectan radicalmente la vida delos ciudadanos de la región, generando tensiones y un clima de inseguridad en determinados espacios geográficos.

La realidad actual del crimen y violencia organizada y el carácter transnacional con el que opera, obliga a los países a tomar medidas legales y a reorganizar sus estrategias tendientes a neutralizar este fenómeno que está afectando la protección de los derechos humanos, la gobernabilidad, el sistema democrático y el desarrollo de los Estados.

Es de imperiosa necesidad que se determine los riesgos y amenazas, que conviven en el escenario internacional que podrían ser factores potenciadores que pueden generar nuevos riesgos o amenazas o multiplicar y agravar efectos.

El comercio en línea de bienes y servicios ilícitos se ha expandido constantemente en los últimos años, lo que se requiere de una estructura, organización y prevención de delitos.

Es innegable que existe una serie de plataformas en internet, con accesos restringidos que se pueden obtener todos las herramientas ilícitas para causar daños a bienes públicos y privados a través de la red.

En el futuro, las plataformas en línea emergerán como una plataforma de distribución clave para todo tipo de bienes ilícitos, así como tentar a la seguridad nacional de lo países.

Actualmente, los ataques y riesgos a los estados, se están generando mediante ataques cibernéticos, como ya ha sucedido con el a personas y compañías de Ecuador.

Se han dado casos conocidos 16 de mayo de 2017, en el que tres empresas de seguridad cibernética señalaron que unas 15 000 personas y 27 empresas fueron amenazadas y afectadas por el WannaCry, el virus que las mafias liberaron el viernes 12 de mayo de 2017, en nuestro país se identifico alertas en Quito, Guayaquil y Manta, en el que virus había intentado penetrar las cuentas personales y corporativas, para apoderarse de los equipos.

No obstante a nivel mundial ya se han dado casos que mediante la web han logrado paralizar servicios públicos, hospitales, trenes, y otros, que han llegado que se atenten contra la de los seres humanos, siendo esto ya amenazas o atentados realizados mediante la web.

De acuerdo a lo manifestado por expertos de ciberseguridad, se ha determinado que el Ecuador, diariamente cuenta con miles de ataques cibernéticos, a instituciones publicas y privadas, por lo que es de imperiosa necesidad, que se creen una normativa adecuada que regule organice, institucionalice estas actuaciones, hasta poder llegar a prevenir este tipo de ilícitos, que podrían afectar a la seguridad interna y externa del pais.

ASAMBLEA NACIONAL

EL PLENO

CONSIDERANDO

Que el Estado ecuatoriano debe regirse por normativa clara, legítima, efectiva y eficaz en el ordenamiento jurídico que la rige;

Que la seguridad humana debe estar regulada por una normativa que garantice los derechos de la Constitución, amparándose en lo que se establece en ella;

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

Que el artículo 83 de la Norma Suprema, determina los deberes y responsabilidad de las ecuatorianas y ecuatorianos, siendo uno de ellos: "(...)4. Colaborar en el mantenimiento de la paz y de la seguridad.";

Que la Constitución de la República del Ecuador en el artículo 147, de las atribuciones y deberes del Presidente de la República establece en su numeral 17, velar por el mantenimiento de la soberanía y la independencia del Estado, del orden interno, la seguridad pública, y ejercer la dirección política de la defensa nacional;

Que los numerales primero, segundo y tercero del artículo 133 de la Constitución señalan que serán orgánicas aquellas leyes que regulen la organización y funcionamiento de las instituciones creadas por la Constitución; las que determinen el ejercicio de los derechos y garantías constitucionales; las que regulen la organización, competencias, facultades y funcionamiento de los gobiernos autónomos descentralizados;

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

Que el artículo 260 de la Constitución de la República del Ecuador dispone que las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal, ejercerán solamente las competencias y facultades que le sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución;

Que el artículo 261 numeral 1 de la Constitución de la República del Ecuador, otorga competencias a la Función Ejecutiva para definir las políticas de protección interna y orden público;

Que el artículo 277 de la Constitución de la República del Ecuador, prescribe que, para la consecución del buen vivir, es deber del Estado garantizar los derechos de las personas y las colectividades, así como generar y ejecutar las políticas públicas y controlar y sancionar su incumplimiento;

Que la Constitución de la República del Ecuador, en su "Título VII Del Régimen del Buen Vivir", artículo 340 define al sistema nacional de inclusión y equidad social como: "(...) el conjunto articulado y coordinado de sistemas, instituciones, políticas, normas, programas y servicios que aseguran el ejercicio, garantía y exigibilidad de los derechos reconocidos en la Constitución y el cumplimiento de los objetivos del régimen de desarrollo.";

Que de conformidad con el inciso tercero del artículo 340 de la Norma Suprema dispone: "El sistema nacional de inclusión y equidad social se compone de los ámbitos de la educación, salud, seguridad social, gestión de riesgos, cultura física y deporte, hábitat y vivienda, cultura, comunicación e información, disfrute del tiempo libre, ciencia y tecnología, población, seguridad humana y transporte.";

Que es necesario contar con una Ley de Seguridad, que busque procedimientos ágiles, con implicaciones, alcances y duración de las intervenciones en materia de defensa de la soberanía, seguridad pública, Sistema Nacional de Inteligencia.

Que el Pleno de la Asamblea Nacional, aprobó el 10 de abril de 2018 una Resolución en la que se compromete a generar reformas a las principales leyes en materia de seguridad.

En uso de su atribución que le confiere el número 6 del artículo 120 de la Constitución de la República, expide la siguiente:

PROYECTO DE LEY DE SEGURIDAD DIGITAL

SISTEMA NACIONAL DE SEGURIDAD DIGITAL

TÍTULO I

OBJETIVO Y ÁMBITO DE APLICACIÓN

Artículo 1.- Objetivo.- El Sistema Nacional de Seguridad Digital tiene como objetivo investigar, mitigar y neutralizar las amenazas y reducir el nivel de los riesgos del ciberespacio que puedan afectar la soberanía del país y seguridad ciudadana. Se promoverá la asistencia, colaboración y cooperación nacional e internacional en lo referente a Ciberseguridad y Ciberdefensa.

Artículo 2.- Ámbito de aplicación.- Se establecerá políticas, estrategias, planes y programas que permitan garantizar el desarrollo de las actividades de seguridad digital a fin de garantizar la Seguridad Integral del Estado; las disposiciones de esta ley serán de carácter obligatorio para todas las Instituciones públicas, privadas, personas naturales y jurídicas.

TÍTULO II

DEFINICIONES Y PRINCIPIOS

DEL SISTEMA DE SEGURIDAD DIGITAL

Capítulo 1

Articulo 3.- Definiciones.- Para los fines consiguientes se entenderá por:

a) **Ciberdefensa.-** Es la capacidad del Estado para defender la soberanía de las infraestructuras críticas tecnológicas y áreas estratégicas de la nación.
b) **Ciberseguridad.-** Es el conjunto de herramientas, políticas, técnicas de seguridad, directrices, métodos de gestión de riesgos y tecnologías que puedan utilizarse para prevenir, reducir, investigar y neutralizar los riegos, amenazas y delitos de naturaleza cibernética a los que están expuestas todas las instituciones públicas, privadas, personas naturales y jurídicas en territorio ecuatoriano.
c) **Ciberespacio.-** Es un escenario que involucra activos tangibles (redes de comunicaciones, sistemas de información y equipos) y activos intangibles

(información digital, propiedad intelectual, marca y reputación), desapareciendo la concepción de un área física, extendiéndose en tiempo y espacio.

d) **Ciberespionaje.-** Conjunto de actividades originadas o patrocinadas por Estados, organizaciones o individuos conocidos o desconocidos, con la intención de apropiarse de información sensible o valiosa que afecte la Seguridad Integral del Estado.
e) **Ciberataque.-** Conjunto de actividades no autorizadas ejecutadas mediante el uso de las Tecnologías de la Información y Comunicación, que vulneren los activos de información y que afecte la Seguridad Integral del Estado.
f) **Tecnologías de la Información y Comunicaciones (TIC).-** agrupan al conjunto de sistemas y herramientas digitales, concebidos y utilizados para: producir, tratar, intercambiar, clasificar, recuperar y presentar información digital.

Capítulo 2

Articulo 4.- Principios.- En el desarrollo de las actividades y/u operaciones de seguridad digital se deberán observar los siguientes principios:

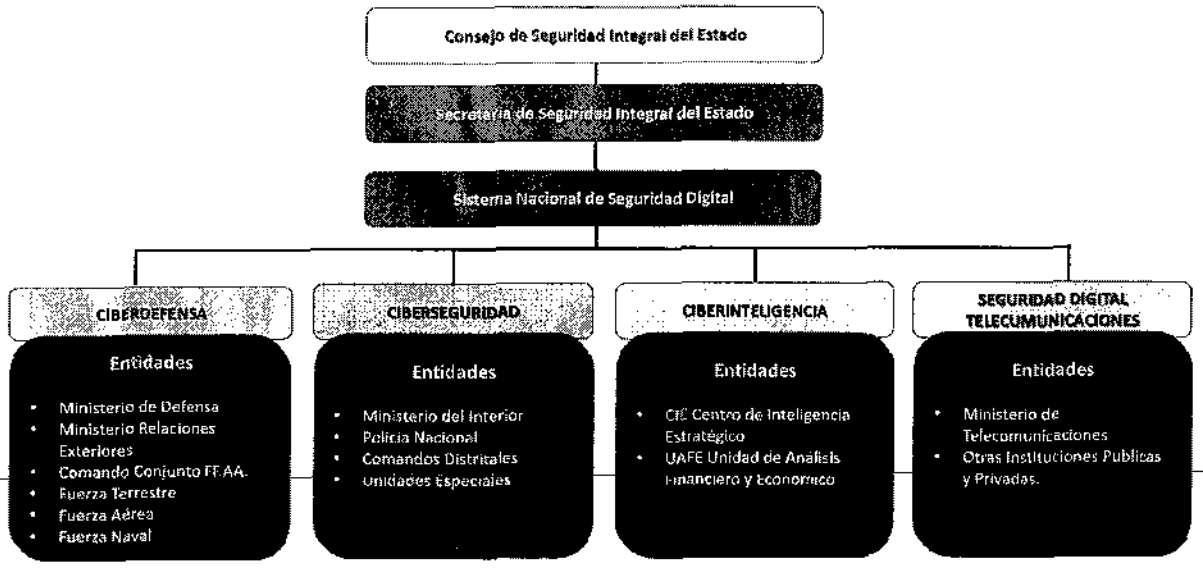
a) **Oportunidad.-** Conjunto de acciones inmediatas enmarcadas en un espacio y tiempo apropiados para poder alertar y/o neutralizar una amenaza en el ciberespacio.
b) **Confidencialidad.-** Se deberá mantener la compartimentación de las operaciones en los ámbitos de seguridad y defensa de los activos de información digital así como la reserva en las estrategias y acciones desarrolladas.
c) **Necesidad.-** Conjunto de informaciones que permitan al Estado la toma de decisiones inmediatas ante amenazas o riesgos a la seguridad integral del país.
d) **Prevención.-** Medidas oportunas sobre las amenazas y gestión de riesgos en el ciberespacio, que utilicen los organismos del sistema de seguridad digital en base a análisis estratégicos y prospectivos.
e) **Proporcionalidad.-** Las herramientas, políticas, técnicas de seguridad, directrices, métodos de gestión de riesgos y tecnologías, deberán prevalecer al interés público sobre el personal con la finalidad de salvaguardar la Seguridad Integral del Estado.
f) **Legalidad.-** El Estado y los organismos de ciberseguridad y ciberdefensa, en cuanto a las infracciones que se cometan en el ciberespacio procederán conforme al derecho del debido proceso y la normativa que corresponda.
g) **Integridad.-** Es la precisión, consistencia y confiabilidad de los datos durante su ciclo de vida. Los datos deben permanecer inalterados durante la transferencia y no deben ser modificados por entidades no autorizadas.

h) **Disponibilidad.-** Se deberá propender a la disponibilidad de la red y los datos a los usuarios del ciberespacio.

TÍTULO III

DE LA ORGANIZACIÓN DELSISTEMA NACIONAL DE SEGURIDAD DIGITAL.

ORGANIZACIÓN DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL



Artículo 5.- Sistema Nacional de Seguridad Digital.- Será un Sistema transversal a la Ley de Seguridad Integral y del Estado, sus componentes de Ciberdefensa y Ciberseguridad, deberán trabajar en forma conjunta, coordinada y articulada con la finalidad de prevenir, reducir, investigar y neutralizar los riesgos, amenazas y delitos de naturaleza digital que afecten a la Seguridad Integral del Estado.

Proporcionaran Ciberinteligencia de forma oportuna para la toma de decisiones por parte de las máximas autoridades del Estado.

Artículo 6.- Organismos que conforman el Sistema Nacional de Seguridad Digital.- Este sistema está estructurado por los siguientes componentes:

a. Ciberdefensa del Ministerio de Defensa.
b. Ciberseguridad del Ministerio del Interior.
c. Seguridad Digital del Ministerio de Sectores Estratégicos
d. Seguridad Digital de la Secretaria de inteligencia.

e. Seguridad Digital del Ministerio de Telecomunicaciones y de la Sociedad de la Información.
f. Seguridad Digital de la Unidad de Análisis Financiero y Económico.
g. Seguridad Digital de otras instituciones públicas y privadas con infraestructura crítica que lo requieran.

Artículo 7.- Atribuciones del Sistema Nacional de Seguridad Digital

a. Asesorar al Presidente de la República y al Consejo de Seguridad Integral del Estado en el análisis y definición de la política nacional de seguridad digital, la misma que contendrá las estrategias, reglamentos, planes y programas que se aplicaran para la ejecución y cumplimiento de las acciones de ciberseguridad y ciberdefensa.
b. Integrar el funcionamiento y articular las actividades de los diferentes componentes del Sistema Nacional de Seguridad Digital.
c. Analizar y proponer las alternativas de estructura orgánica para la conformación del Sistema Nacional de Seguridad Digital.
d. Elaborar el Plan Nacional de Seguridad Cibernética para la aprobación por parte del Secretario Nacional de Seguridad Integral.
e. Elaborar propuestas de legislación aplicable en materia de ciberespacio, para su análisis y aprobación respectiva.

Artículo 8.- Del Sistema Nacional de Seguridad Digital.- Es el responsable de la elaboración de la Apreciación Nacional de Seguridad Digital y del Plan Nacional de Seguridad Digital, así como de la planificación, coordinación y ejecución de los planes y operaciones de los integrantes del Sistema Nacional de Seguridad Digital.

El Sistema Nacional de Seguridad Digital estará dirigido por un Director (a) quien será nombrado por el Consejo de Seguridad Integral del Estado previa selección de una terna presentada por la Secretaría Nacional de Seguridad Integral y cumplirá funciones por un periodo de cuatro años.

El Director de Seguridad Digital será sujeto de control político cada tres meses por parte de la Asamblea Nacional y rendirá cuentas de su gestión ante el Contralor General del Estado.

Articulo 9.- Funciones del Sistema Nacional de Seguridad Digital.-

Cumpliera las siguientes funciones:

a) Preparar la Apreciación Nacional de Seguridad Digital y del Plan Nacional de Seguridad Digital los cuales deberán ser aprobados por el Secretario Nacional de Seguridad Integral.

b) Supervisará la planificación y ejecución de las operaciones de Ciberseguridad y Ciberdefensa.
c) Coordinará el empleo de los medios humanos y tecnológicos de los componentes del Sistema Nacional de Seguridad Digital.
d) Propenderá al reclutamiento, la capacitación integral, de los servidores y funcionarios públicos en el área de Ciberdefensa y Ciberseguridad.
e) Coordinar y asesorar a los entes gubernamentales y privados en la aplicación de políticas de Ciberdefensa y Ciberseguridad.
f) Planificar y evaluar el uso de los gastos reservados asignados por el presupuesto del Estado para las actividades de Seguridad Digital.
g) Identificar las amenazas actuales y potenciales en el ámbito del ciberespacio, proponiendo las acciones tendientes a prevenir, reducir, investigar y neutralizar los riesgos, amenazas y delitos en el ciberespacio que afecten a la soberanía territorial y seguridad ciudadana.
h) Se implementará los Centros de Respuesta a Incidentes de Seguridad Digital (CSIRT), para el manejo de la ciberseguridad (Policía Nacional) y ciberdefensa (Fuerzas Armadas) que funcionarán de manera integrada y otros dependiendo de su naturaleza particular de infraestructura crítica nacional (Salud, finanzas, energía, entre otros).
i) ~~Coordinar y determinar las infraestructuras críticas digitales.~~
j) Coordinación y establecimiento de alianzas, acuerdos y demás instrumentos que permitan mantener la cooperación nacional e internacional en el campo de la ciberdefensa y ciberseguridad.
k) Elaborar proyectos de leyes basados en legislación internacional que sustenten la ejecución de actividades de los organismos responsables de la Ciberdefensa y Ciberseguridad.

Capítulo 1

DEL DIRECTOR NACIONAL DE SEGURIDAD DIGITAL

Articulo 10.- Del Director.- La o el Director, constituyen la máxima autoridad del Sistema Nacional de Seguridad Digital, quien será nombrado por el Consejo de Seguridad Integral del Estado previa selección de una terna presentada por la Secretaría Nacional de Seguridad Integral.

Articulo 11.- Requisitos.- Además de lo establecido en la Ley Orgánica de Servicio Público LOSEP, la o el Director deberá cumplir con los siguientes requisitos:

a) Ser ecuatoriano o ecuatoriana de nacimiento.

b) Acreditar título de cuarto nivel en carreras afines a Ciberdefensa y/o Ciberseguridad.
c) Acreditar una experiencia laboral de 4 años probada en áreas de Ciberdefensa y/o Ciberseguridad.

Artículo 12.- Atribuciones.- Son atribuciones de la o el Director Nacional de Seguridad Digital las siguientes:

a) Presentar y ejecutar la Apreciación Nacional de Seguridad Digital y el Plan Nacional de Seguridad Digital previa la aprobación del Secretario Nacional de Seguridad Integral.
b) Establecer escenarios prospectivos en base a las matrices de riesgo y amenazas en el ciberespacio y recomendar los cursos de acción a tomar.
c) Asesorar al Presidente de la República, al Consejo de Seguridad Integral del Estado, organismos gubernamentales y privados sobre políticas de ciberseguridad y ciberdefensa que deben ejecutarse.
d) Proporcionar Ciberinteligencia oportuna para la toma de decisiones al Presidente de la República y al Consejo de Seguridad Integral del Estado.
e) Supervisar la planificación y ejecución de las operaciones de ciberseguridad y Ciberdefensa de los componentes del sistema.
f) Identificar amenazas y vulnerabilidades en la infraestructura critica nacional en el ámbito de ciberseguridad y ciberdefensa.
g) Levantar un mapa de la infraestructura crítica nacional y áreas estratégicas que pueden ser afectadas por ciberataques.
h) Aprobar y supervisar el uso de los gastos especiales asignados al Sistema Nacional de Seguridad Digital.
i) Los demás que determine la presente ley.

Capitulo 2
De los Organismos que conforman el Sistema de Seguridad Digital

Articulo 13.- Ciberdefensa.- El Comando de Ciberdefensa de las Fuerzas Armadas será parte del Sistema Nacional de seguridad Digital y cumplirá las siguientes funciones:

a) Tendrá como misión fundamental la detección, prevención, contención y respuesta ante ciberataques a la infraestructura critica del estado.
b) Preparara y ejecutara la planificación para la detección, prevención, contención y respuesta, ante las nuevas amenazas cibernéticas que traten de afectar las áreas críticas o estratégicas nacionales.
c) Presentará para su aprobación el plan de ciberdefensa al Director Nacional de Seguridad Digital.

d) Levantará escenarios prospectivos en base a las matrices de riesgo y amenazas en el ciberespacio y recomendar los cursos de acción a tomar.
e) Levantará un mapa de la infraestructura crítica nacional y áreas estratégicas que pueden ser afectadas por ciberataques.
f) Coordinara con los otros componentes del Sistema Nacional de Seguridad Digital las acciones conjuntas para repeler o contrarrestar los ciberataques provenientes del ciberespacio.
g) Previa autorización del Director Nacional de Seguridad Digital podrá firman convenios bilaterales y multilaterales con otras naciones en el ámbito de la Ciberdefensa para mejorar los canales de información, detección y/o respuesta coordinada ante incidentes cibernéticos.

El Comando de Ciberdefensa dispondrá de los recursos y tecnología acordes con su misión y amenazas existentes.

Artículo 14.- Ciberseguridad.- las Unidades de ciberseguridad de la Policía Nacional, serán parte del Sistema Nacional de seguridad Digital y cumplirá las siguientes funciones:

a) Tendrá como misión fundamental la detección, prevención, contención y respuesta ante ciberataques orientados hacia la seguridad ciudadana o delitos digitales que ~~pongan en riesgo la infraestructura critica del estado.~~
b) Preparara y ejecutara la planificación para la detección, prevención, contención y respuesta, ante los nuevos delitos cibernéticos.
c) Presentará para su aprobación el plan de ciberseguridad al Director Nacional de Seguridad Digital.
d) Levantará escenarios prospectivos en base a las matrices de riesgo y amenazas en el ciberespacio y recomendar los cursos de acción.
e) Levantará un mapa de la infraestructura crítica nacional y áreas estratégicas que pueden ser afectadas por ciberataques.
f) Coordinara con los otros componentes del Sistema Nacional de Seguridad Digital las acciones conjuntas para repeler o contrarrestar los ciberataques provenientes del ciberespacio.
g) Previa autorización del Director Nacional de Seguridad Digital podrá firman convenios bilaterales y multilaterales con otras naciones en el ámbito de la ciberseguridad para mejorar los canales de información, detección y/o respuesta coordinada ante incidentes cibernéticos.

La Ciberseguridad dispondrá de los recursos y tecnología acordes con su misión y amenazas existentes.

Artículo 15.- Ciberinteligencia.- las Unidades de Ciberinteligencia del Centro de Inteligencia Estratégico y la Unidad de Análisis Financiero y Económico, serán parte del Sistema Nacional de seguridad Digital y cumplirá las siguientes funciones:

a) Tendrá como misión fundamental proporcionar inteligencia oportuna y útil sobre el accionar de las amenazas cibernéticas a fin de permitir a los diferentes organismos del Sistema Nacional de Seguridad Digital estar preparados para la detección, prevención, contención y respuesta ante ciberataques.
b) Preparara y ejecutara la búsqueda colección, interpretación y difusión de la inteligencia sobre amenazas cibernéticas a las autoridades para la toma de decisiones.
c) Presentará para su aprobación el Plan de Búsqueda de las amenazas cibernéticas ciberseguridad al Director Nacional de Seguridad Digital.
d) Levantará escenarios prospectivos en base a las matrices de riesgo y amenazas en el ciberespacio y recomendar los cursos de acción.
e) Coordinara con los otros componentes del Sistema Nacional de Seguridad Digital los productos de inteligencia o los requerimientos sobre las amenazas del ciberespacio a la seguridad del Estado.
f) Previa autorización del Director Nacional de Seguridad Digital podrá firman convenios bilaterales y multilaterales con otras naciones en el ámbito de la Ciberinteligencia para mejorar los canales de información, detección y/o respuesta coordinada ante incidentes cibernéticos.

La Ciberinteligencia dispondrá de los recursos y tecnología acordes con su misión y amenazas existentes.

Artículo 16.- Seguridad Digital de Telecomunicaciones.- Las entidades de Telecomunicaciones y las empresas públicas y/o privadas que tengan información o instalaciones digitales que puedan ser afectados por ataques cibernéticos formaran parte del Sistema Nacional de seguridad Digital y cumplirá las siguientes funciones:

a) Prestaran las facilidades a los organismos de Seguridad Digital y colaboraran con los mismos a fin de reducir las amenazas existentes.

DISPOSICIÓN FINAL. La **LEY DE SEGURIDAD DIGITAL** entrará en vigencia el día … publicado en el Registro Oficial ….. Dado y suscrito en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de Quito, provincia de Pichincha a los …..