ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR
Leyes para la gente

Memorando Nro. AN-PR-2021-0156-M

Quito, D.M., 13 de mayo de 2021

PARA: Sr. Dr. Javier Aníbal Rubio Duque
Secretario General

ASUNTO: DIFUNDIR EL PROYECTO DE LA LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA

De mi consideración:

Según lo dispuesto en el artículo 55 de la Ley Orgánica de la Función Legislativa, envío el ***"PROYECTO DE LA LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA"*** remitido el 10 de mayo de 2021 y suscrito por el asambleísta José Ricardo Serrano Salgado, a través del memorando Nro. AN-SSJR-2021-0055-M, a fin de que sea difundido a las/los asambleístas y a la ciudadanía por medio del portal Web y se remita al Consejo de Administración Legislativa (CAL), para el trámite correspondiente.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Mg. César Ernesto Litardo Caicedo
PRESIDENTE DE LA ASAMBLEA NACIONAL

Anexos:
- Memorando Nro. AN-SSJR-2021-0055-M, en 28 fojas.

Copia:
Sr. Dr. Paco Gustavo Ricaurte Ortiz
Prosecretario General

OC/JR

Firmado electrónicamente por:
CESAR ERNESTO LITARDO CAICEDO

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR
Leyes para la gente

Memorando Nro. AN-SSJR-2021-0055-M

Quito, D.M., 10 de mayo de 2021

PARA: Sr. Mg. César Ernesto Litardo Caicedo
Presidente de la Asamblea Nacional

ASUNTO: PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA

De mi consideración:

De conformidad con lo dispuesto en los artículos 134 numeral 1 y 136 de la Constitución de la República del Eccuador, en concordancia con lo dispuesto en los artículos 54 numeral 1 y 55 de la Ley Orgánica de la Función Legislativa, me permito presentar ante usted el "PROYECTO DE LA LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA", para lo cual sírvase disponer a quien corresponda proceda con el trámite pertinente.

Adjunto firmas de respaldo y ficha de verificación de cumplimiento de las ODS.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Dr. José Ricardo Serrano Salgado
ASAMBLEÍSTA

Anexos:
- an-cmgp-2021-0031-m_jose_serrano.pdf
- cyber_jose_serrano.pdf
- oficio_de_apoyo_proyecto_seguridad_ciberneiÌtica_(1)-signed.pdf
- oficio_de_apoyo_proyecto_seguridad_cibernetica-1-signed.pdf
- an-amkc-2021-0023-m.pdf
- an-gcfh-2021-0031-m.pdf
- apoyo_al_proyecto_de_ley_organica_de_seguridad_cibernetica.pdf
- memo_apoyo_ley_seguridad_cibernetica_-0052-m.pdf
- ficha_de_verificacioÌn_de_cumplimiento_ods_seguridad_cibernetica.pdf
- proyecto_de_seguridad_cibernetica.pdf

Copia:
Sr. Dr. Javier Aníbal Rubio Duque
Secretario General

Firmado electrónicamente por:
JOSE RICARDO SERRANO SALGADO

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR
2017-2021

PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA

EXPOSICIÓN DE MOTIVOS

La Constitución de la República consagra en el artículo 16 el derecho a la información y comunicación. De igual forma, en el artículo 66 numeral 19, se refiere al acceso, tratamiento de la información y datos personales. En consonancia con la norma constitucional, existen varias disposiciones infraconstitucionales como la Ley de Seguridad Pública y del Estado que en el artículo 2 reconoce como parte de esta seguridad la salvaguarda, supervisión y control de los riesgos que puedan estar presentes en el contexto tanto tecnológico como científico, entre otros.

En el Ecuador, no existe normativa en ciberseguridad, ciberfensa y ciberinteligencia, no obstante, cuenta con varias disposiciones jurídicas enfocadas a la protección y reconocimiento de dicho importante asunto entre las que se encuentran: la Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley Orgánica y de la Contraloría General del Estado, Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva.

El Ecuador cuenta con una Agenda Política de Defensa “Libro Blanco” que define en su alcance nacional que las Fuerzas Armadas realizan operaciones de carácter militar para dar cumplimiento a su misión de defender la soberanía, la integridad del territorio tanto continental, insular, aéreo, marítimo y también el ciberespacio sin articular con otros organismos, por lo que se requiere un sistema fuerte de ciberseguridad, ciberdefensa y ciberinteligencia, así como se determinan los riesgos y amenazas a la seguridad del país al identificarlo como uno de los más significativos.

Actualmente, según el Ministerio de Telecomunicaciones y de la Sociedad de la Información se está trabajando en la elaboración de una Estrategia de Seguridad

con el objetivo de fortalecer y asegurar el entorno digital en el país para lo que está recibiendo asesoría especializada por parte del Banco Interamericano de Desarrollo (BID) y la consultora NRD Cyber Security.

El Gobierno ecuatoriano mediante el (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019) realizará acciones conjuntas entre el sector público y privado para ir perfeccionando sus sistemas de seguridad, fundamentalmente para proteger la información y datos públicos tanto de las entidades como de los ciudadanos.

Como se aprecia la ciberseguridad en Ecuador presenta dificultades, puesto que su marco jurídico es realmente pobre y aun no cuenta con una Estrategia Nacional colocándose ante ello, en una situación de alta vulnerabilidad en este orden.

El panorama en Ecuador en cuanto a los ataques a la ciberseguridad es el siguiente, el Viceministro de Telecomunicaciones (Real, 2019), expone que, a raíz del retiro de asilo a Julián Assange, fundador de WikiLeaks, ha generado la aparición de 40 millones de ataques. Estos manifestaron incluso un crecimiento en un solo día, lo que trajo como consecuencia que el país pasó del lugar 51 al 31 a nivel internacional en cuanto al volumen de ataques de esta clase. Ello obligó al Estado a la implementación de un Protocolo que se activó de forma indefinida para enfrentar estos actos.

Se debe destacar que entre las instituciones con mayor cantidad de intentos de ataques se encuentran: el Banco Central del Ecuador; Presidencia de la República; la Corporación Nacional de Telecomunicaciones (CNT); el Servicio de Rentas Internas; el Ministerio del Interior; el Consejo de la Judicatura, algunos Gobiernos Autónomos Descentralizados, universidades y el Ministerio de Ambiente.

Cabe destacar que se han realizado ataques directos hacia los datos personales. Al respecto, el Telégrafo (2019) explica que se realizó la venta de datos personales,

ya que se filtró una base de datos con información de 20,8 millones de registros (cerca de 18 gigabits) que afectaría a la mayoría de la población del país.

En ese sentido, se analiza que en Ecuador la actividad que más se emplea es el phishing como modalidad que está dirigida fundamentalmente a actos fraudulentos que se ha manifestado en el tráfico de empresarial. También acciones de intrusión interna de información.

En informe elaborado por (Microsoft, 2019) se asevera que Ecuador tiene un alto riesgo de seguridad, ya que es mayor que los promedios a nivel mundial ante las amenazas recibidas como malware y malware de minería de criptomoneda, que se han detectado 6.5 millones de billones de señales de amenazas que atraviesan la nube de esta compañía. Ello obliga a preparase en materia de ciberseguridad y coloca en un alto de grado de vulnerabilidad tanto al país como a su economía.

Como se aprecia Ecuador tiene una situación compleja en materia de ciberseguridad, ciberdefensa y ciberinteligencia no solo dentro de su territorio, sino también a escala regional e internacional; lo que implica que debe trabajar en normas jurídicas adecuadas y en una estrategia integral de ciberseguridad para enfrentar esta clase de actos.

En el Ecuador existe un marco jurídico enfocado a la protección y reconocimiento de la ciberseguridad entre las que se encuentran: la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley Orgánica del Sistema Nacional de Registro de Datos Públicos y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el Código Orgánico Integral Penal. Además, existe un Proyecto de Ley Orgánica de protección de datos personales presentado en septiembre de 2019, aun no aprobado. A pesar de lo expuesto, aun es insuficiente teniendo en cuenta que las disposiciones jurídicas están dispersas y muchas de ellas están incompletas y rezagadas ante el desarrollo tecnológico actual.

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR
2017-2021

ASAMBLEA NACIONAL

EL PLENO

CONSIDERANDO

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 154 numeral 1 de la Constitución de la República del Ecuador, dispone que, a las Ministras y Ministros de Estado, además de las atribuciones establecidas

en la ley, les corresponde ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativos que requiera su gestión;

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 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.

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR
2017-2021

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

LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA

TÍTULO I

OBJETIVO Y AMBITO DE APLICACIÓN

Articulo 1.- Objetivo.- Se tiene como objetivo el salvaguardar la seguridad de las personas naturales y jurídicas en el ciberespacio, proteger la seguridad nacional, promover la coordinación y articulación institucional, y gestionar, prevenir y enfrentar los delitos que tengan lugar en el ciberespacio, con un sistema de articulación para el combate de los mismos, mejorando las capacidades de protección, y respuesta ante una serie de posibles brechas, como la seguridad de las personas en el ciberespacio contribuyendo a la Seguridad Integral del Estado, previniendo las amenazas y reduciendo los riesgos cibernéticos que puedan afectar la seguridad, soberanía del país y la paz ciudadana. No se limita únicamente a la información ya que también puede estar enfocado a proteger la disponibilidad de servicios industriales entre otros.

Se propende a alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesarias para sustentar todos los objetivos de ciberseguridad, ciberdefensa y ciberinteligencia, con una adecuada colaboración internacional.

Artículo 2.- Ámbito de aplicación.- Se establecerá planes, programas y políticas que permitan garantizar el desarrollo de las actividades de seguridad cibernéticas, las disposiciones de esta ley serán de carácter obligatorio para todas las instituciones públicas o privadas.

TÍTULO II

DEFINICIONES Y PRINCIPIOS DE LA SEGURIDAD CIBERNETICA.

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

a) **Amenaza.-** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información, puede tener un potencial efecto negativo sobre algún elemento de los sistemas. Las amenazas pueden proceder de ataques como, fraude, robo, virus, de sucesos físicos, como incendios, inundaciones o negligencia y decisiones institucionales, como el mal manejo de contraseñas, no usar cifrado. Pueden ser internas y externas.

b) **Auditoría de seguridad cibernética.-** Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones

c) **Ciberseguridad.**- Es la materia que se encarga de minimizar el nivel de riesgo al que está expuesta la información ante amenazas o incidentes de

naturaleza cibernética. La ciberseguridad tiene como foco la protección de la información digital.

d) **Ciberdefensa.-** Es el conjunto de acciones estrategias legales, operaciones activas o pasivas desarrolladas en el ámbito de redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticas de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueron concebidos a la vez que se impide que fuerzas enemigas las utilicen para cumplir sus objetivos estratégicos.

e) **Ciberesfera**: es un sistema formado por el conjunto de elementos digitales, personales y relacionales que conforman la envoltura o hábitat cibernético de la humanidad.

f) **Ciberactivismo:** es un conjunto de técnicas de comunicación mediadas por el ciberespacio y su tecnología, que permiten la dedicación intensa a una determinada línea de acción en la vida pública, en el área social, política o religiosa, mediante el logro de una comunicación más rápida y difusión de gran audiencia.

g) **Ciberarma:** Acción cibernética destinada a realizar funciones ofensivas o defensivas que se materialicen en un ataque y tengan por finalidad un daño intencional, con resultado de destrucción de las cosas, violencia en las personas, disfuncionalidad o disrupción, temporal o permanente, de redes, sistemas, equipos, funciones, servicios o instalaciones, o atente contra intereses, derechos o libertades.

h) **Ciberespacio.-** Es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipo y personal relacionados con

los sistemas informáticos cualquieras sean estos y las telecomunicaciones que los vinculan.

i) **Ciberespionaje.-** Es el entorno complejo resultante de la interacción entre las personas, el software y los servicios de Internet por medio de dispositivos tecnológicos conectados a redes, las cuales no existen en ningún tipo de forma física.

j) **Ciberdelincuencia.-** Es la actividad criminal donde los servicios o aplicaciones en el Ciberespacio se utilizan o son el blanco de un crimen, o donde el Ciberespacio es la fuente, herramienta, destino o el lugar de un crimen

k) **Seguridad de la información.-** son las medidas preventivas para proteger la información, garantizando, confidencialidad, disponibilidad e integridad. Esta información puede estar en cualquier tipo de medio donde se almacene y es lo que intentaremos proteger.

l) **Seguridad informática.-** Son todas aquellas medidas tomadas para proteger la integridad y la privacidad de la información almacenada en un sistema informático y signifique un riesgo si llega a manos de otras personas. Se puede referir a Software, base de datos y archivos entre otros.

Articulo 4.- Principios.- En el desarrollo de las actividades de la seguridad cibernéticas, seguridad informática, seguridad de la información se deberán observar los principios de accesibilidad, cooperación, colaboración, confidencialidad, disponibilidad, igualdad, integridad, interés Público,

interoperabilidad, legalidad, proporcionalidad, responsabilidad, seguridad.

TÍTULO III

DE LA ORGANIZACIÓN.

Articulo 5.- Sistema Nacional de Seguridad Cibernética.- El sistema de Seguridad Cibernética, será autónomo e independiente, debe coordinar acciones de cooperación e intercambio de información entre instituciones públicas, privadas y organismos regionales e internacionales enfocadas a la capacitación, concientización y capacidad de respuesta ante ciberamenazas a través de un protocolo de información y seguimiento de incidentes rectorado por el Consejo Nacional de Seguridad Cibernética, que permita al estado contar con una auditoria de seguridad cibernética, para prevenir, reaccionar y capacitar en materia de seguridad digital.

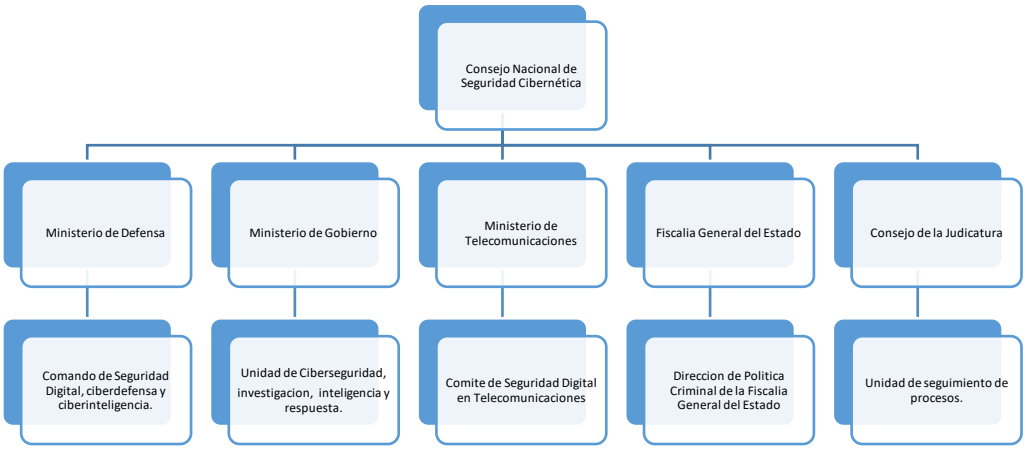
Artículo 6.- Organismos que conforman el Sistema Nacional de Seguridad Cibernético.- Este sistema está estructurado por los siguientes componentes.

a. Ministerio de Defensa.
b. Ministerio de Gobierno.
c. Ministerio de Telecomunicaciones y de la Sociedad de la Información.
d. Fiscalía General del Estado
e. Consejo de la Judicatura.

Artículo 7.- Consejo Nacional de Seguridad Cibernética. Es un organismo de consejo, análisis y estrategia para el Presidente de la Republica, y al Consejo de Seguridad Pública y del Estado, quienes alertarán sobre las amenazas que se desarrollen en el sistema de seguridad cibernético. Pertenecerá a la Función Ejecutiva.

El Consejo Nacional de Seguridad Cibernética será presidido por el Presidente de la República y conformado de forma permanente por: las Fuerzas Armadas del Ecuador, Ministerio de Telecomunicaciones y de la Sociedad de la Información, el Ministerio de Gobierno, la Fiscalía General del Estado y el Consejo dela Judicatura. Es la máxima autoridad en materia de ciberseguridad en el país.

De manera eventual puede formar parte de este Consejo, cualquier otro organismo o institución involucrada con cierta actividad o acción, en función de la necesidad en determinado momento.



Artículo 8.- Funciones y Atribuciones del Consejo Nacional de Seguridad Cibernética.

1) Definir la política y las normas institucionales en materia de ciberseguridad, ciberdefensa y ciberinteligencia, comprobar su aplicación y gestión a nivel de los organismos del Estado y empresas privadas.
2) Evaluar los requerimientos estratégicos y los recursos necesarios relacionados con la ciberseguridad.
3) Monitorear los riesgos existentes en el país en materia de ciberseguridad, ciberdefensa y ciberinteligencia.
4) Supervisar las medidas de ciberseguridad, ciberdefensa y ciberinteligencia. para la protección de infraestructuras críticas.
5) Supervisar la investigación y monitoreo de los incidentes relativos a la ciberseguridad, ciberdefensa y ciberinteligencia.
6) Supervisar el cumplimiento de las normativas de ciberseguridad en el país.
7) Asegurar la actuación coordinada de los integrantes del Consejo para prevenir, gestionar y eliminar cualquier acto que atente contra la ciberseguridad en el país.
8) Aprobar las principales iniciativas para incrementar la seguridad en el ciberespacio nacional.
9) Aprobar las metodologías y procesos a nivel nacional para garantizar la ciberseguridad, ciberdefensa y ciberinteligencia.
10) Evaluar y coordinar la implementación de controles a nivel nacional en materia de ciberseguridad, ciberdefensa y ciberinteligencia.
11) Dar seguimiento a los hechos delictivos que han tenido lugar en el ciberespacio, ciberdefensa y ciberinteligencia.
12) Dar seguimiento a los procesos judiciales ante actos delictivos en materia de ciberseguridad, ciberdefensa y ciberinteligencia.
13) Controlar el cumplimiento de las funciones por parte de los organismos miembros de este Consejo Nacional de Seguridad Cibernética.

14) Suscribir Acuerdos y Convenios internacionales y regionales en materia de ciberseguridad, ciberdefensa y ciberinteligencia.

Artículo 9.- Funciones de las Fuerzas Armadas dentro Consejo Nacional de Seguridad Cibernética.

Las funciones del Ministerio de Defensa se ejecutarán a través de un Comando de Seguridad Digital, ciberdefensa y ciberinteligencia, quien deberá;

1) Cumplir con las actividades y funciones determinadas por el Consejo Nacional de Seguridad Cibernética.
2) Coordinar con los niveles estratégicos de la defensa y el Estado, los requerimientos estratégicos relacionados con la ciberseguridad para presentar al Consejo Nacional de Cibernética.
3) Asumir la dirección para actualizar la información y estrategias acerca de la infraestructura critica a proteger a escala nacional, previa autorización del Consejo Nacional de Cibernética.
4) Analizar y definir el mejoramiento de las capacidades de ciberdefensa y proponerlo al Consejo Nacional de Cibernética para su aprobación.
5) Coordinar la elaboración de la planificación de gestión de acuerdo con la Estrategia de ciberseguridad y ciberdefensa para ejecutar actividades relacionadas con la defensa en el ciberespacio.
6) Dirigir y supervisar dentro de las Fuerzas Armadas la ejecución constante de las capacidades de ciberdefensa, en beneficio de alcanzar los objetivos estratégicos y cumplimiento de las misiones en ese orden.
7) Gestionar que los recursos humanos y técnicos tanto militares como los servidores públicos estén debidamente capacitados en materia de ciberdefensa de acuerdo con el desarrollo científico técnico en esta área.

8) Asumir cualquier misión que se asigne sobre ciberdefensa por el orden jerárquico superior.

Artículo 10.- Funciones del Ministerio de Telecomunicaciones y de la Sociedad de la Información dentro Consejo Nacional de Seguridad Cibernética.

Las funciones del Ministerio de Telecomunicaciones y de la Sociedad de la Información en función de la ciberseguridad se ejecutarán a través de la Comité de Seguridad Digital en Telecomunicaciones, quien deberá;

1) Cumplir con las actividades y funciones determinadas por el Consejo Nacional de Seguridad Cibernética.
2) Establecer líneas de seguridad informática, protección de infraestructura computacional y todo lo vinculado a ella, comprende también la información existente en las instituciones públicas del país, previamente aprobado por Consejo Nacional de Seguridad Cibernética.
3) Formular protocolos de seguridad informática a aplicar para todas las instituciones públicas y empresas privadas, previa aprobación por el Consejo Nacional de Seguridad Cibernética.
4) Revisar el estado de los medios y herramientas informáticas y de tecnologías de la información y comunicación en los organismos del sector público.
5) Realizar recomendaciones sobre el manejo de herramientas informáticas y tecnológicas de la información y comunicación en las entidades públicas.

Artículo 11.- Funciones del Ministerio de Gobierno dentro Consejo Nacional de Seguridad Cibernética.

Las funciones del Ministerio de Gobierno en función de la ciberseguridad se ejecutarán a través del Unidad de Ciberseguridad, investigación, inteligencia y respuesta, quien deberá;

1. Cumplir con las actividades y funciones determinadas por el Consejo Nacional de Seguridad Cibernética.
2. Diseñar y ejecutar los procedimientos para identificar los componentes de infraestructura informática que poseen un alto riesgo, realizar la evaluación de las vulnerabilidades con la finalidad de plantear al Consejo Nacional para su aprobación, las acciones para controlarlos.
3. Estudiar y proponer al Consejero Nacional actividades para coadyuvar a la protección de la integridad y confidencialidad de los datos de los organismos del Estado que utilizan TIC's.
4. Determinar la influencia, el alcance y características de los incidentes informáticos con el objetivo de realizar recomendaciones al Consejo Nacional
5. Coordinar y apoyar la implementación de la solución a los casos presentados por Ciberdelito.
6. Responder a los incidentes Informáticos mediante su investigación técnica, recopilación de pruebas o evidencias de cualquier acción que represente un indicio de fraude en las TIC's,
7. Mantener un vínculo sustentado en la operación con los CSIRT (Grupo de Respuesta a Incidentes de Seguridad Informática) de otros países para apoyar y resolver cualquier incidente que tenga lugar dentro del país.
8. Elaborar y mantener actualizado el registro de investigaciones ejecutadas para contar con los antecedentes y referencias de cada uno de los casos
9. Proponer al Consejo Nacional de Ciberseguridad proyectos de investigación y transferencia tecnológica vinculados con el asunto de responder a los a incidentes informáticos, prevención y control de delitos en el ciberespacio.
10. Coordinar y cooperar con organizaciones tanto públicas como privadas, entre ellos con: proveedores de servicio de internet (ISP), proveedoras de seguridad, Grupos de Respuesta a Incidentes de Seguridad Informática

(CSIRT) de otros países, Fiscalía General del Estado y otras entidades que cuentan con áreas de seguridad informática para de manera conjunta cumplir la reglamentación correspondiente a los fines de garantizar la ciberseguridad.

Artículo 12.- Funciones de la Fiscalía General del Estado dentro Consejo Nacional de Seguridad Cibernética.

La Fiscalía General del Estado, cuenta con a función fundamental en el orden jurídico en materia de Ciberseguridad y Ciberdefensa dentro del Consejo Nacional de Seguridad Cibernética, puesto que debe brindar asistencia a los efectos de revisar la normativa vigente y su aplicación en el país. Esta ejecuta las acciones a través de la Dirección de Política Criminal, quien deberá;

1) Cumplir con las actividades y funciones determinadas por el Consejo Nacional de Seguridad Cibernética.
2) Registrar las denuncias a escala nacional por delitos informáticos.
3) Generar y estudiar información de carácter criminológica, con la finalidad proponer políticas y estrategias de prevención del delito en el ciberespacio.
4) Organizar y actualizar los datos estadísticos a nivel nacional relacionado con los delitos ocurridos en el ciberespacio nacional.
5) Realizar estudios criminológicos y formular propuestas para disminuir el índice delictivo en el ciberespacio nacional.
6) Implementar y desarrollar estudios e investigaciones técnicas partiendo de la estadística sobre la seguridad en el ciberespacio.
7) Proponer al Consejo Nacional de Ciberseguridad políticas institucionales enfocados en la prevención y enfrentamiento de los delitos en el ciberespacio.
8) Ejercer otras funciones y responsabilidades en el ámbito de su competencia, que le asigne el Consejo Nacional de Ciberseguridad.

Artículo 13.- Funciones del Consejo de la Judicatura dentro Consejo Nacional de Seguridad Cibernética.

El Consejo de la Judicatura tiene un rol importante en el orden jurídico nacional en materia de Ciberseguridad y dentro del Consejo Nacional, ya que de forma articulada con la Fiscalía General del Estado debe brindar asistencia legal sobre la normativa vigente y su aplicación en el país, quien deberá;

1) Cumplir con las actividades y funciones determinadas por el Consejo Nacional de Ciberseguridad.
2) Registrar los procesos judiciales a escala nacional por delitos informáticos.
3) Dar a conocer al Consejo Nacional de Ciberseguridad los resultados de los procesos judiciales por la comisión de actos delictivos en el ciberespacio.
4) Fomentar la preparación de peritos en materia de ciberseguridad
5) Ejecutar acciones de capacitación a jueces y servidores públicos en materia de ciberseguridad
6) Ejecutar una revisión de la normativa vigente en materia penal sobre los delitos informáticos a los efectos, de ser necesario, proponer las reformas que resulten convenientes al CAL para su evaluación y propuesta a la Asamblea Nacional.
7) Ejercer otras funciones y responsabilidades en el ámbito de su competencia, que le asigne el Consejo nacional de Ciberseguridad.

Artículo 14.- Dirección y Secretaria técnica del Consejo Nacional de Seguridad Cibernética. El Consejo estará presidido por una o un Director, nombrado por el Pleno de la Asamblea Nacional, quien será designada o designado de una terna enviada por el Presidente de la República, con una duración en su cargo por cinco años, quien estará sujeto a control político y

administrativo. Sus funciones y atribuciones serán determinadas por el reglamento respectivo.

DISPOSICIONES TRANSITORIAS

PRIMERA.- El Reglamento de la presente Ley, lo elaborará el Presidente de la República del Ecuador, en un plazo de 180 días, a partir de la publicación.

DISPOSICIÓN GENERAL.- En un plazo de 180 días, la Asamblea Nacional, deberá reformar las Leyes vigentes en materia de Seguridad, para que permitan articular el trabajo de la Seguridad Cibernética y se pueda armonizar su cumplimiento en atribuciones en el ciberespacio.

DISPOSICION FINAL.- Esta Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Memorando Nro. AN-AMKC-2021-0023-M

Quito, D.M., 10 de mayo de 2021

PARA: Sr. Dr. José Ricardo Serrano Salgado
Asambleísta

ASUNTO: Apoyo Proyecto de Ley

De mi consideración:

En ejercicio de mis atribuciones previstas en la Constitución y en la Ley Orgánica de la Función Legislativa, en mi calidad de Asambleísta por medio de la presente manifiesto mi voluntad de apoyar el "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA" de su iniciativa.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Master. Karina Cecilia Arteaga Muñoz
ASAMBLEÍSTA

Firmado electrónicamente por:
KARINA CECILIA ARTEAGA MUNOZ

Memorando Nro. AN-CMGP-2021-0031-M

Quito, D.M., 09 de mayo de 2021

PARA: Sr. Dr. José Ricardo Serrano Salgado
Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado

ASUNTO: voluntad de apoyar el "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA"

De mi consideración:

En ejercicio de mis atribuciones previstas en la Constitución y en la Ley Orgánica de la Función Legislativa, en mi calidad de Asambleísta por medio de la presente manifiesto mi voluntad de apoyar el "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA" de su iniciativa.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Sra. Gabriela Pamela Cerda Miranda
ASAMBLEÍSTA

Firmado electrónicamente por:
GABRIELA PAMELA CERDA MIRANDA

Memorando Nro. AN-GCFH-2021-0031-M

Quito, D.M., 10 de mayo de 2021

PARA: Sr. Dr. José Ricardo Serrano Salgado
Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado

ASUNTO: APOYO PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA

De mi consideración:

En ejercicio de mis atribuciones previstas en la Constitución y en la Ley Orgánica de la FuncioÌn Legislativa, en mi calidad de Asambleísta de la Provincia de Bolivar y por medio de la presente manifiesto mi voluntad de apoyar el "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA" de su iniciativa.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Ing. Fafo Holguin Gavilanez Camacho
ASAMBLEÍSTA

Anexos:
- proyecto_de_seguridad_cibernetica.docx

Copia:
Sr. Dr. Javier Aníbal Rubio Duque
Secretario General

Firmado electrónicamente por:
FAFO HOLGUIN GAVILANEZ CACMACHO

Fwd: APOYO AL PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA

1 mensaje

De: José Ricardo Serrano Salgado

Para: Nathalia Verónica Jaramillo del Pozo

10 de Mayo 2021 11:43

OFICIOS ENVIADO…CA.docx-signed.pdf (113 KB) Descargar | Eliminar

---

De: "Pinuccia Magaly Colamarco Vera" <pinuccia.colamarco@asambleanacional.gob.ec>
Para: "César Ernesto Litardo Caicedo" <cesar.litardo@asambleanacional.gob.ec>
CC: "José Ricardo Serrano Salgado" <jose.serrano@asambleanacional.gob.ec>
Enviados: Lunes, 10 de Mayo 2021 9:08:34
Asunto: APOYO AL PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA

Estimado Señor Ingeniero
César Litardo Caicedo

Por medio del presente hago envío adjunto del oficio con mi firma de respaldo a la solicitud de APOYO AL **"PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA",** iniciativa del Asambleísta José Serrano Salgado.

Saludos cordiales,

Mg. Pinuccia Colamarco Vera
Asambleísta por Manabí

Memorando Nro. AN-OMMA-2021-0009-M

Quito, D.M., 10 de mayo de 2021

PARA: Sr. Dr. José Ricardo Serrano Salgado
Asambleísta

ASUNTO: APOYO AL PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA

De mi consideración:

En ejercicio de mis atribuciones previstas en la Constitución y en la Ley Orgánica de la FuncioÌn Legislativa, en mi calidad de Asambleísta por medio de la presente manifiesto mi voluntad de apoyar el "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA" de su iniciativa.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Sr. Manuel Alfredo Ochoa Morante
ASAMBLEÍSTA

Firmado electrónicamente por:
MANUEL ALFREDO OCHOA MORANTE

Memorando Nro. AN-OACU-2021-0052-M

Quito, D.M., 10 de mayo de 2021

PARA: Sr. Dr. José Ricardo Serrano Salgado
Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado

ASUNTO: Apoyo "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA"

De mi consideración:

En ejercicio de mis atribuciones previstas en la Constitución y en la Ley Orgánica de la Función Legislativa, en mi calidad de Asambleísta por medio de la presente manifiesto mi voluntad de apoyar el "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA" de su iniciativa.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Sr. Carlos Urel Ortega Alvarez
ASAMBLEÍSTA

Anexos:
- proyecto_de_seguridad_cibernetica_0805457001620667646.ocx

Firmado electrónicamente por:
CARLOS UREL ORTEGA ALVAREZ

D.M. de Quito, 09 de mayo de 2021
Oficio No AS-ORO-2021-32

Doctor
José Serrano Salgado
Asambleísta Nacional
Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado
ASAMBLEA NACIONAL DEL ECUADOR
En su despacho. –

De mi consideración:

En ejercicio de mis atribuciones previstas en la Constitución y en la Ley Orgánica de la Función Legislativa, en mi calidad de Asambleísta por medio de la presente manifiesto mi voluntad de apoyar el "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA" de su iniciativa.

Con sentimientos de distinguida consideración.

Atentamente,

Firmado electrónicamente por:
ROSA GINA ORELLANA

Rosa Orellana Román

Asambleísta por la provincia de El Oro

D.M. de Quito, 10 de mayo de 2021
Oficio Nro. 1011 – LRDQ – AN – 2021

Doctor
José Serrano Salgado
Asambleísta Nacional
Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado
ASAMBLEA NACIONAL DEL ECUADOR
En su despacho. –

De mi consideración:

En ejercicio de mis atribuciones previstas en la Constitución y en la Ley Orgánica de la Función Legislativa, en mi calidad de Asambleísta por medio de la presente manifiesto mi voluntad de apoyar el "PROYECTO DE LEY ORGÁNICA DE SEGURIDAD CIBERNÉTICA" de su iniciativa.

Con sentimientos de distinguida consideración.

Atentamente,

Firmado electrónicamente por:
LUIS RAFAEL QUIJIJE DELGADO

Lcdo. Rafael Quijije Delgado

ASAMBLEÍSTA POR LA PROVINCIA DE MANABÍ

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

FICHA DE VERIFICACIÓN DEL CUMPLIMIENTO DE LOS OBJETIVOS DE DESARROLLO SOSTENIBLE EN INICIATIVAS LEGISLATIVAS

Nombre del Proyecto de Ley y/o reforma: Proyecto de Ley Orgánica de Seguridad Cibernética

Proponente de la iniciativa legislativa: José Serrano Salgado

I. NECESIDAD DEL PROYECTO O INICIATIVA LEGISLATIVA

1. ¿Responde este proyecto de Ley y/o reforma a una necesidad jurídica?

- El proyecto de ley responde a una necesidad jurídica de tipificar nuevas infracciones penales cometidas en el ciberespacio.

2. ¿Responde este proyecto de Ley y/o reforma a una necesidad programática y/o derecho?

- Responde a la protección de derechos encaminados a una cultura de paz y convivencia pacífica garantizando seguridad nacional y ciudadana.

3. ¿Qué normas legales vigentes se verían afectadas o deberían derogarse o reformarse con la aprobación de la norma propuesta?

Ley de Seguridad Pública y del Estado

II. ALINEACIÓN PROGRAMÁTICA

4. ¿El ámbito de la propuesta de Ley y/o reforma y sus principios están previstos dentro de los objetivos del Plan Nacional de Desarrollo?
¿A qué objetivo del PND se alinea más su contenido?

- Eje 1: Derechos para Todos Durante Toda la Vida
- Objetivo 1, Garantizar una vida digna con iguales oportunidades para todas las personas.
- Objetivo 3, Garantizar los derechos de la naturaleza para las actuales y futuras generaciones.
- Eje 3: Más Sociedad Más Estado
- Objetivo 9, Garantizar la soberanía y la paz, y posicionar estratégicamente el país en la región y el mundo.

5. ¿La propuesta de Ley y/o reforma viabiliza, apoya o complementa de alguna manera los Objetivos de Desarrollo Sostenible (Agenda 2030)?
¿A qué objetivo del Agenda 2030 se alinea más su contenido?

- Objetivo 16, Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y crear instituciones eficaces, responsables e inclusivas a todos los niveles.

III. REPERCUSIONES ECONÓMICAS Y PRESUPUESTARIAS

6. ¿La propuesta de Ley y/o reforma da lugar a alguna carga y/o impacto económico en:

- _Ninguno

IV. REPERCUSIONES SOCIALES

7. ¿Qué población se vería beneficiada?

- Población nacional

V. EFECTOS Y/O REPERCUSIONES POLÍTICAS

8. ¿Qué función/es y/o entidad/es se encargarán de implementar la propuesta de Ley y/o reforma?

- Función Ejecutiva
- Función Legislativa
- Función Judicial

9. ¿Es posible identificar posibles efectos secundarios negativos, conflictividad o consecuencias no deseadas de su propuesta?

NO