EXPOSICIÓN DE MOTIVOS

No podemos hablar de Seguridad Integral en el Ecuador, porque no existe, vemos crimen en las calles, centros de rehabilitación ensangrentados, muertes a diario, el dolor de las victimas y de sus familias, además en la red nos colapsan servicios y nos roban nuestros datos. No obstante, con ello se ha dejado a un lado la regulación de nuevos sistemas de seguridad que permitan actuar a las instituciones de seguridad en el ciberespacio y con ello poder prevenir los ilícitos que se dan en las calles y en la red.

Vivimos en una era digital, usamos diariamente la tecnología, nos comunicamos mediante la red, estamos interrelacionados con procesos digitales en casi todos los ámbitos, económicos, sociales, políticos, de seguridad, entre otros y ocasiona un flujo de la información en los diferentes servicios tanto públicos como privados, que deben estar asegurados bajo normas y leyes que puedan enfrentar las nuevas amenazas digitales y evitar la delincuencia.

En la región países como Colombia, Brasil, Chile, Argentina, Perú han desarrollado normas, estrategias, ratificación de instrumentos internacionales, como el Convenio de Budapest, políticas nacionales de ciberseguridad, ciberdefensa, ciberinteligencia, con el objetivo fundamental de garantizar la seguridad del ciberespacio como parte de la seguridad nacional, con cooperación internacional.

Constituye una urgencia para el Ecuador, el que se elabore textos normativos que creen normas que permitan actuar y mitigar los delitos que se pretenden ejecutar desde la red.

Es necesario que nuestro país cuente con subsistemas, mecanismos, estrategias de detección, prevención y reacción de los incidentes en el sistema digital, articulando a las instituciones de seguridad, defensa, inteligencia, para poder manejar las diferentes crisis de ciberseguridad, ciberdefensa y ciberinteligencia de manera ágil, oportuna, efectiva, eficiente y coordinada, con la finalidad de proteger las infraestructuras tecnológicas del

Estado y de sus ciudadanos, y así también prevenir el cometimiento de ilícitos ante amenazas, riesgos y ataques en el ciberespacio.

Es indispensable que nuestro país resguarde la seguridad ciudadana, la soberanía del Estado, en el ciberespacio y se pueda prevenir, investigar, mitigar, actuar efectivamente ante el cometimiento, riesgo, ataque de delitos cibernéticos. Sin dejar a un lado el factor que actualmente muchos delitos se articulan, planean y ejecutan con y desde sistemas operativos, y dispositivos tecnológicos.

De la misma manera es momento que incentivemos y promovamos una cultura de ciberseguridad en el uso responsable del ciberespacio en el país y se conozcan los riesgos que se pueden dar en la red.

En nuestro ordenamiento jurídico existen varias disposiciones jurídicas enfocadas en la protección de los datos e información en sentido general de la seguridad digital. Estas disposiciones legales pretenden proteger las operaciones que tienen lugar en el ciberespacio. Sin embargo, esta dispersión normativa no resulta favorable en el contexto actual, en el que tienen lugar ataques y amenazas en dicho entorno. Existe la necesidad de que se expida un Sistema de Seguridad Digital que englobe todos los aspectos que intervienen en las operaciones que se realizan empleando la tecnología para evitar cualquier vulneración de derechos y asegurar una adecuada protección.

Resulta evidente que Ecuador, que a pesar de tener varias normas jurídicas enfocadas en la protección de las operaciones que tienen lugar en la red, requiere de un sistema adecuado de Seguridad Digital con sus respectivos subsistemas, su aprobación debe ser priorizada, ya que nos coloca en una situación de vulnerabilidad con respecto a otros países de la región que si cuentan con normas adecuadas que previenen el cometimiento de ilícitos.

Estamos obligados armonizar normas comunes con la región, realizando un análisis de derecho comparado que definan procedimientos, mecanismos de cooperación, acciones conjuntas en función de garantizar la ciberseguridad, ciberdefensa, ciberinteligencia y que no sigamos teniendo incidentes y delitos como se han dado últimamente con los ataques a diferentes instituciones como CNT, ANT y los sistemas financieros.

Es importante resaltar que el presente Proyecto de Ley, no incrementa el presupuesto económico del Estado, no crea institucionalidad, ni imposibilita el cumplimiento de las funciones de los organismos del Estados, otorga seguridad jurídica para poder actuar bajo amenazas, ataques en la red, siempre respetando los principios y garantías constitucionales.

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 66, numeral 19, de la Constitución de la República reconoce y garantizará a las personas: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente Protección. La recolección, archivo,

procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" y en su numeral 21 garantiza a las personas "el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; está no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación".

Que el artículo 83 de la Norma Constitucional, 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 el artículo 85 de la Constitución de la República dispone: "La formulación, ejecución, evaluación y control de las políticas públicas y servicios públicos que garanticen los derechos reconocidos por la Constitución, se regularán de acuerdo con las siguientes disposiciones: 1. Las políticas públicas y la prestación de bienes y servicios públicos se orientarán a hacer efectivos el buen vivir y todos los derechos, y se formularán a partir del principio de solidaridad (...) En la formulación, ejecución, evaluación y control de las políticas públicas y servicios públicos se garantizará la participación de las personas, comunidades, pueblos y nacionalidades";

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 Carta Magna 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 227 de la Constitución de la República dispone: "La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación";

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 numeral 10 del artículos 261 de la Constitución de la República determina que el Estado central tendrá competencias exclusivas: "(...) 10. El espectro radioeléctrico y el régimen general de comunicaciones y telecomunicaciones; puertos y aeropuertos";

Que el artículo 277 de la Constitución de la República del Ecuador, señala 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 artículo 313 de la Constitución de la República dispone: "El Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia. Los sectores estratégicos, de decisión y control exclusivo del Estado, son aquellos que por su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, y deberán orientarse al pleno desarrollo de los derechos y al interés social. Se consideran sectores estratégicos la energía en todas sus formas, las telecomunicaciones, los recursos naturales no renovables, el transporte y la refinación de hidrocarburos, la biodiversidad y el patrimonio genético, el espectro radioeléctrico, el agua, y los demás que determine la ley";

Que la Ley Orgánica de Transparencia y Acceso a la Información Pública, y su Reglamento, enfatizan en el derecho de las personas al acceso a la información pública, conforme a las garantías consagradas en la Constitución de la República;

Que el artículo 6 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos señala: "Accesibilidad y confidencialidad.- Son confidenciales los datos de

carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso publico atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales. (...) La autoridad o funcionario que por naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos (...)";

Que el artículo 3 numeral 1 de la Ley Orgánica de Telecomunicaciones establece como uno de los objetivos de la ley: "Promover el desarrollo y fortalecimiento del sector de las telecomunicaciones";

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

LEY ORGÁNICA DE SEGURIDAD DIGITAL, CIBERSEGURIDAD, CIBERDEFENSA Y CIBERINTELIGENCIA

CAPÍTULO I
OBJETO Y ÁMBITO

Artículo 1.- Objeto.- El objeto de la presente Ley es establecer un Sistema de Seguridad Digital, con los componentes o subsistemas de ciberseguridad, ciberdefensa que permita prevenir, combatir, reaccionar, neutralizar, manejar la o las crisis y recuperar información en caso de amenazas, riegos y/o ataques informáticos con la participación de los diferentes organismos públicos y privados para coordinar las acciones del Estado y

promover la seguridad digital en los distintos niveles del gobierno y de la ciudadanía en el ciberespacio.

El Ecuador debe defender y proteger la soberanía, seguridad integral, las infraestructuras críticos públicas y privadas, la integridad política, la seguridad económica y la seguridad nacional; así también, salvaguardar los sistemas de información digital de los organismos estratégicos, operacionales y tácticos ante ataques, riesgos o amenazas en el ciberespacio.

Artículo 2.- Ámbito.- El ámbito de aplicación de la ley esta encaminada a la facultad de ejecución de políticas públicas, operaciones de ciberseguridad, ciberdefensa, ciberinteligencia dentro del territorio nacional y en el exterior con la colaboración internacional respectiva, teniendo como finalidad la de prevenir y mitigar toda actividad cibernética maliciosa que ponga en riesgo la seguridad integral del estado ecuatoriano, la soberanía y la protección de los derechos de la ciudadanía en general.

CAPÍTULO II
DEFINICIONES Y PRINCIPIOS DE LA SEGURIDAD DIGITAL

Artículo 3.- Definiciones.- Para los fines de esta Ley se entenderá por:

a) Amenaza cibernética.- Toda acción que, aprovechando la vulnerabilidad de los sistemas de información, buscan atentar contra la seguridad de un sistema de información con finalidades contrarias a Ley.
b) Ataque cibernéticos o ciberataque.- Son actos maliciosos que buscan causar daño accediendo a un sistema informático desde y en el ciberespacio.
c) Ciberdefensa.- Es una herramienta para asegurar la defensa nacional en el contexto digital y cuenta con mecanismos propios para la defensa, prevención y enfrentamiento al ciberterrorismo y protección de la soberanía del Estado.

d) Ciberespacio.- Espacio sin limites físicos en el cual personas interactúan mediante sistemas informáticos través de internet, redes, dispositivos tecnológicos.
e) Ciberdelincuencia.- Es la actividad criminal donde los servicios o aplicaciones en el ciberespacio se utilizan o son el blanco para perpetuar un delito.
f) Ciberseguridad.- Es el conjunto de herramientas, políticas, conceptos de seguridad digital, directrices, métodos de Gestión y prevención de riesgos, acciones, practicas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos, información y bienes que se encuentran en el ciberespacio.
g) Ciberinteligencia. – Mecanismo que busca detectar y neutralización de amenazas y riesgos para la seguridad interna y defensa del Estado de los incidentes que se puedan dar en el ciberespacio o la red.

Artículo 4.- Principios.- En el desarrollo de las actividades de la seguridad digital, ciberseguridad, ciberinteligencia y ciberdefensa se deberán garantizar y aplicar los principios y los derechos fundamentales de las y los ciudadanos establecidos en la Constitución de la Republica.

CAPÍTULO III
SISTEMA NACIONAL DE SEGURIDAD DIGITAL

Artículo 5.- Sistema Nacional de Seguridad Digital.- Es el conjunto de subsistemas, instituciones, políticas, estrategias, normativas, planes, programas, con el fin de efectuar la conducción estratégica de la seguridad digital del Estado en la prevención y respuesta, para enfrentar los desafíos, riesgos y amenazas que afectan al ejercicio de los derechos y libertades de sus ciudadanos en el ciberespacio, sistemas informáticos y la red.

Artículo 6.- Funciones de las instituciones del Sistema de Seguridad Digital.- Les corresponde evaluar los factores y situaciones que puedan afectar a la Seguridad Digital

del Estado, con la finalidad de prevenir, contrarrestar y mitigar las amenazas, riesgos y ataques que se puedan dar en el ciberespacio.

Los órganos e instituciones del Sistema de Seguridad Digital deberán recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis; detectar las necesidades y dictar y emitir las medidas sobre planificación y coordinación en todas las entidades del sector público con la finalidad de garantizar la disponibilidad y el correcto funcionamiento de los recursos de este sistema.

Artículo 7.- Conformación del Sistema Nacional de Seguridad Digital.- El Sistema de Seguridad Digital estará conformado por subsistemas que se encargarán de acuerdo al ámbito de sus competencias en precautelar la ciberseguridad, ciberdefensa y ciberinteligencia.
La rectoría de la Sistema Nacional de Seguridad Digital la tendrá el Consejo de Seguridad Pública y del Estado, a través de su Secretario.

La Fiscalía General del Estado y el Consejo de la Judicatura serás instituciones auxiliares al Sistema de Seguridad Digital.

De manera eventual podrá formar parte cualquier otro organismo o institución involucrado que se requiera para los fines de ciberseguridad, ciberdefensa y ciberinteligencia.

Artículo 8.- Funciones y atribuciones del Secretario del Consejo de Seguridad Pública y del Estado.- Además de las que la le establece la Ley deberá cumplir:

1) Elaborar el Plan de Seguridad Digital de acuerdo al Plan Nacional de Desarrollo.

2) Definir la política pública de las institucionales en materia de ciberseguridad, ciberdefensa y ciberinteligencia, controlar, fiscalizar su cumplimiento.
3) Realizar los diagnósticos necesarios con las instituciones del Sistema Nacional de Seguridad Digital y presentarlos a la Presidenta o Presidente de la Republica y al Consejo de Seguridad Pública y del Estado.
4) Supervisar y monitorear los riegos y las medidas de ciberseguridad, ciberdefensa y ciberinteligencia, para la protección de infraestructuras críticas.
5) Presentar las estrategias preventivas y de mitigación al Presidente de la República y al Consejo de Seguridad Publica y del Estado en materia de seguridad digital.
6) Asegurar la actuación coordinada de los subsistemas para prevenir, gestionar y eliminar cualquier acto que atente contra la ciberseguridad, ciberdefensa y ciberinteligencia del país.
7) Dar seguimiento y presentar informes a la o el Presidente de la República y al Consejo de Seguridad Pública y del Estado sobre los hechos delictivos que han tenido lugar en el ciberespacio, ciberdefensa y ciberinteligencia.
8) Controlar el cumplimiento de las funciones por parte de las instituciones del Sistema Nacional de Seguridad.
9) Aprobar o improbar los planes, informes o evaluaciones que presenten los diferentes subsistemas.
10) Recomendar la suscripción de acuerdos y convenios internacionales en materia de ciberseguridad, ciberdefensa y ciberinteligencia a la Función Ejecutiva.

CAPÍTULO IV
SUBSISTEMAS DE SEGURIDAD DIGITAL

Artículo 9.- Subsistema de Ciberseguridad.- El Subsistema de Ciberseguridad estará conformado por: Policía Nacional, Ministerio de Gobierno a través de la Subsecretaria de Seguridad Ciudadana o quien haga sus veces, y el Ministerio de Telecomunicaciones y de la Sociedad de la Información y tendrá coordinación directa con el subsistema de ciberinteligencia, quien entregará la información necesaria para correcto cumplimiento de las funciones del subsistema de ciberseguridad.

En relación a las funciones del subsistema será ciberseguridad además de las actuar de manera inmediata ante las amenazas, riegos, ataques, y manejo de crisis serán las que señalen en el reglamento de esta Ley.

Artículo 10.- Funciones del Ministerio de Gobierno del Subsistema de Ciberseguridad.- El Ministerio de Gobierno a través, de la Subsecretaria de Seguridad Ciudadana o quien haga sus veces, en coordinación con la Policía Nacional deberá;

1. Cumplir y hacer cumplir con las políticas públicas, estrategias, planes emitidos por el ente rector de la materia.
2. Identificar los componentes de infraestructura informática que poseen un alto riesgo.
3. Realizar la evaluación de las vulnerabilidades en ciberseguridad de las instituciones del Estado con la finalidad de plantear al ente rector un informe para su aprobación, deberá contar con las acciones y medidas y recomendaciones para controlar los posibles riesgos.
4. Proponer acciones eficaces y validas para la protección de datos de los organismos del Estado que utilizan sistemas informáticos.

5. Coordinar y apoyar la implementación de la solución a los casos presentados por delitos informáticos, ciberataques y otros incidentes que puedan afectar a las instituciones públicas y privadas.
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 los sistemas informáticos.
7. Se deberá contar los agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones, respetando los principios y garantías constitucionales, que pertenecerán al Ministerio de Gobierno y Policía Nacional.
8. Generar política pública de cooperación internacional, con la finalidad de para apoyar y resolver cualquier incidente que tenga lugar dentro del país y pueda ser ocasionado desde el exterior.
9. Deberá elaborar un registro de investigaciones ejecutadas y se presentará semestralmente al ente rector.
10. Presentar proyectos de investigación y transferencia tecnológica con la finalidad de prevenir incidentes, delitos informáticos en el ciberespacio.
11. Coordinar y cooperar con organizaciones tanto públicas como privadas, para de manera conjunta cumplir la reglamentación correspondiente a los fines de garantizar la ciberseguridad.
12. Las demás atribuciones que las establezca el presente reglamento.

Estas funciones serán adicionales a las que les otorga las leyes, reglamentos, normativa interna de acuerdo al ámbito de sus competencias.

Artículo 11.- Funciones del Ministerio de Telecomunicaciones y de la Sociedad de la Información dentro de los Subsistemas de Ciberseguridad, Ciberdefensa y Ciberinteligencia.- Las funciones del Ministerio de Telecomunicaciones y de la Sociedad de la Información de acuerdo a las funciones y características propias de la

institución deberá coordinar y trabajar con los diferentes subsistemas de ciberseguridad, ciberdefensa y ciberinteligencia por lo que cumplirá:

1) Cumplir con las actividades y funciones determinadas por el ente rector.
2) Se emitirá protocolos, estrategias, planes de seguridad informática y de la información con la finalidad proteger las diferentes infraestructuras cibernéticas de las instrucciones del Estado.
3) Recomendar la priorización en la obtención de equipamiento tecnológico y humano para fortalecer las infraestructuras digitales del Estado.
4) Alertar y denunciar a las autoridades competentes por los incidentes, delitos que puedan darse en el ciberespacio y afecte a la seguridad ciudadana y soberanía del estado.
5) Las demás que establezca el reglamento de esta Ley.

Estas funciones serán adicionales a las que les otorga las leyes, reglamentos, normativa interna de acuerdo al ámbito de sus competencias.

Artículo 12.- Subsistema de Ciberdefensa.- El subsistema de ciberdefensa estará conformado por: Misterio de Defensa, Comando Conjunto de las Fuerzas Armadas, y el Ministerio de Telecomunicaciones y de la Sociedad de la Información y tendrá coordinación directa con el subsistema de ciberinteligencia, quien entregará la información necesaria para correcto cumplimiento de las funciones del subsistema de ciberdefensa para el resguardo y protección de ilícitos en relación a la soberanía del Estado.

En relación a las funciones del subsistema será ciberdefensa además de las actuar de manera inmediata ante las amenazas, riegos, ataques, y manejo de crisis serán las que señalen en el reglamento de esta Ley.

Artículo 13.- Funciones del Ministerio de Defensa y Comando Conjunto de las Fuerzas Armadas dentro del Subsistema de Ciberdefensa.- Las funciones del Ministerio de Defensa se ejecutarán de manera coordinada con el Comando Conjunto de las Fuerzas Armadas, quienes deberán;

1. Cumplir y hacer cumplir con las políticas públicas, estrategias, planes emitidos por el ente rector de la materia.
2. Identificar los componentes de infraestructura informática que poseen un alto riesgo en relación a soberanía del Estado.
3. Realizar la evaluación de las vulnerabilidades en ciberdefensa de las instituciones del Estado con la finalidad de plantear al ente rector un informe para su aprobación, deberá contar con las acciones y medidas y recomendaciones para controlar los posibles riesgos.
4. Coordinar y apoyar la implementación de la solución a los casos presentados por delitos informáticos, ciberataques y otros incidentes que puedan afectar a las instituciones públicas y privadas, que pongan en riesgo la defensa y soberanía del Estado.
5. Responder a los incidentes Informáticos mediante su investigación técnica, recopilación de pruebas o evidencias de cualquier acción que represente un indicio de fraude en los sistemas informáticos, que pongan en riesgo la defensa y soberanía del Estado.
6. Se deberá contar los agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones, respetando los principios y garantías constitucionales, que pertenecerán a las Fuerzas Armadas.
7. Generar política pública de cooperación internacional, con la finalidad de para apoyar y resolver cualquier incidente que pongan en riesgo la defensa y soberanía del Estado.

8. Deberá elaborar un registro de investigaciones ejecutadas y se presentará semestralmente al ente rector.
9. Presentar proyectos de investigación y transferencia tecnológica con la finalidad de prevenir incidentes, ataques a la soberanía del Estado en el ciberespacio.
10. Coordinar y cooperar con organizaciones tanto públicas como privadas, para de manera conjunta cumplir la reglamentación correspondiente a los fines de garantizar la ciberdefensa.
11. Las demás atribuciones que las establezca el presente reglamento.

Estas funciones serán adicionales a las que les otorga las leyes, reglamentos, normativa interna de acuerdo al ámbito de sus competencias.

Artículo 14.- Subsistema de Ciberinteligencia.- El subsistema de ciberinteligencia, será liderado por el Centro de Inteligencia Estratégico y se articulará con los subsistemas de ciberseguridad, ciberdefensa para la detección y neutralización de amenazas de la seguridad ciudadana y defensa del Estado en el ciberespacio, y cumplirá con las funciones que determina el reglamento de esta Ley.

Estas funciones serán adicionales a las que les otorga las leyes, reglamentos, normativa interna de acuerdo al ámbito de sus competencias.

CAPÍTULO V
ORGANISMOS AUXILIARES DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL

Artículo 15.- Funciones de la Fiscalía General del Estado como organismo auxiliar del Sistema Nacional de Seguridad Digital.- La Fiscalía General del Estado deberá

brindar asistencia técnica jurídica en la aplicación de las leyes a través de su organización institucional, además de las siguientes;

1. Asesorar al Sistema Nacional del Seguridad Digital, en relación a las problemáticas e índices criminológicos de acuerdo a las denuncias presentadas por delitos informáticos.
2. Registrar las denuncias a escala nacional por delitos informáticos y presentar semestralmente al ente rector.
3. Levantar la información de carácter criminológica y proponer políticas y estrategias de prevención del delito en el ciberespacio.
4. Elaborar estadísticas a nivel nacional relacionado con los delitos ocurridos en el ciberespacio nacional.
5. Las demás que determine el reglamento de esta Ley.

Estas funciones serán adicionales a las que les otorga las leyes, reglamentos, normativa interna de acuerdo al ámbito de sus competencias.

Artículo 16.- Funciones del Consejo de la Judicatura como organismo auxiliar del Sistema Nacional de Seguridad Digital.- El Consejo de la Judicatura como órgano auxiliar del Sistema Nacional del Seguridad Digital, deberá:

1) Registrar e informar semestralmente los procesos judiciales a escala nacional por delitos informáticos al ente rector.
2) Presentar un informe semestral con los resultados de los procesos judiciales que se lleven a cabo en el sistema de justicia y Función Judicial.
3) Ejecutar, planes, acciones y capacitación a jueces, fiscales, peritos y demás funcionarios públicos de la Función Judicial en seguridad digital.
4) Las demás que determine el reglamento de esta Ley.

Estas funciones serán adicionales a las que les otorga las leyes, reglamentos, normativa interna de acuerdo al ámbito de sus competencias.

DISPOSICIONES REFORMATORIAS

PRIMERO.- Agréguese en el Código Orgánico Monetario y Financiero en su artículo 14.1 Funciones. Para el desempeño de sus funciones, la Junta de Política y Regulación Financiera tiene que cumplir los siguientes deberes y ejercer las siguientes facultades: (…)

15. Establecer, en el marco de sus competencias, cualquier medida que coadyuve a: (…)

e. Prevenir y erradicar delitos informáticos en la operación y funcionamiento de las entidades financieras, de valores, seguros y servicios de atención integral de salud prepagada, mediante la implementación de buenas prácticas de ciberseguridad, considerando los estándares internacionales y el avance tecnológico.

SEGUNDO.- Agréguese en el Código Orgánico Monetario y Financiero en su artículo 62 Funciones. La Superintendencia de Bancos tiene las siguientes funciones:

9. Exigir que las entidades controladas presenten y adopten las correspondientes medidas correctivas y de saneamiento, en especial en delitos informáticos y tecnológicos e imponer sanciones por incumplimiento en políticas de ciberseguridad;

TERCERO.- Agréguese en la Ley Orgánica de Economía Popular y Solidaria, en el artículo 147 Atribuciones. La Superintendencia tendrá las siguientes atribuciones:

e. Exigir que las entidades controladas presenten y adopten las correspondientes medidas correctivas y de saneamiento, en especial en delitos e incidentes

informáticos y tecnológicos e imponer sanciones por incumplimiento en políticas de ciberseguridad (…)

i. Las demás previstas en la Ley y su Reglamento.

CUARTO.- Agréguese en la Ley Orgánica de Datos Personales, en su artículo Art. 76.- Funciones atribuciones y facultades. La Autoridad de Protección de Datos Personales es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la Protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y en su reglamento de aplicación, para lo cual le corresponde las siguientes funciones, atribuciones y facultades;

18) Entregar un informe trimestral de riesgos, ataques informáticos registrados en relación a la protección de datos, al ente rector del Sistema Nacional de Seguridad Digital, para su análisis y decisión en la generación de políticas públicas.

19)Las demás atribuciones establecidas en la. normativa vigente.

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.

SEGUNDA.- En un plazo de 180 días contados desde la aprobación de esta Ley, la Asamblea Nacional deberá adecuar los tipos penales que establece el Convenio de Budapest, en el Código Orgánico Integral Penal, entre los cuales deberá considerarse los relativos al ataque a la integridad de un sistema informático, interceptación ilícita, ataque a la integridad de los datos informáticos, acceso ilícito al sistema informático,

falsificación informática, fraude informático y abuso de dispositivos y los demás que se crean necesarios de acuerdo a la realidad del Estado y cooperación internacional.

TERCERO.- En un plazo de 180 días contados desde la aprobación de esta Ley, la Asamblea Nacional y la Función Ejecutiva deberán adecuar la normativa para que se permita el uso de técnicas especiales de investigación en la red, como los agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones, respetando los principios y garantías establecidos en la Constitución de la República y los tratados internacionales de derechos humanos ratificados por el Ecuador.

DISPOSICIÓN GENERAL.- En un plazo de 180 días, la Asamblea Nacional y la Función Ejecutiva deberán reformar las leyes, estrategias, políticas públicas vigentes en materia de seguridad, para que permitan articular el trabajo del Sistema Nacional de Seguridad Digital y se pueda armonizar de manera valida y eficaz en su cumplimiento.

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