QUINTO SUPLEMENTO

REGISTRO OFICIAL

ÓRGANO DE LA REPÚBLICA DEL ECUADOR

SUMARIO:

Págs.

Año II - Nº 479 - 82 páginas
Quito, miércoles 23 de junio de 2021

ACUERDO MINISTERIAL 006-2021

EL MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (S)

CONSIDERANDO:

Que, el artículo 3 de la Constitución de la República determina como deber primordial del Estado garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales; el artículo 16 ibídem dispone que todas las personas, en forma individual o colectiva, tienen derecho a la comunicación e información;

Que, el artículo 66, numeral 19, ibídem 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; ésta 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 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, el numeral 1 del artículo 154 de la Constitución de la República confiere a las ministras y ministros de Estado, además de las atribuciones establecidas en la ley, la rectoría de las políticas públicas del área a su cargo; así como la facultad de expedir los acuerdos y resoluciones administrativas que requiera su gestión;

Que, el artículo 226 de la Constitución de la República indica 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 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 ibídem 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 numeral 10 del artículo 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 280 de la norma constitucional señala: *"El Plan Nacional de Desarrollo es el instrumento al que se sujetarán las políticas, programas y proyectos públicos; la programación y ejecución del presupuesto del Estado; y la inversión y la asignación de los recursos públicos; y coordinar las competencias exclusivas entre el Estado central y los gobiernos autónomos descentralizados. Su observancia será de carácter obligatorio para el sector público e indicativo para los demás sectores.";*

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, el inciso segundo del artículo 314 de la Constitución de la República dispone que el Estado garantizará que los servicios públicos, prestados bajo su control y regulación, respondan a principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad;

Que, en el artículo 1 de la Ley Orgánica de Telecomunicaciones señala: *"La presente ley tiene por objeto desarrollar, el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos";*

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";*

Que, el artículo 88 de la Ley Orgánica de Telecomunicaciones respecto de la promoción de la sociedad de la información establece que la actuación del Ministerio de Telecomunicaciones y de la Sociedad de la Información estará encaminada a la formulación de políticas, planes, programas y proyectos destinados entre otros, a: *"1. Garantizar el derecho a la comunicación y acceso a la Información. 2. Promover el acceso universal a los servicios de telecomunicaciones; en especial, en zonas urbano marginal o rural, afín de asegurar una adecuada cobertura de los servicios en beneficio de las y los ciudadanos ecuatorianos. 3. Promover el establecimiento eficiente de infraestructura de telecomunicaciones, especialmente en zonas urbano marginales y rurales. 4. Procurar el Servicio Universal. 5. Promover el desarrollo y masificación del uso de las tecnologías de información y comunicación en todo el territorio nacional (...)";*

Que, el artículo 140 de la Ley Orgánica de Telecomunicaciones dispone: "*Rectoría del sector. El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento*

General y los planes de desarrollo que se establezcan a nivel nacional. Los planes y políticas que dicte dicho Ministerio deberán enmarcarse dentro de los objetivos del Plan Nacional de Desarrollo y serán de cumplimiento obligatorio tanto para el sector público como privado";

Que, el numeral 2 del artículo 141 de la Ley Orgánica de Telecomunicaciones dispone que es competencia del órgano rector del sector de las Telecomunicaciones y de la Sociedad de la Información*: "2. Formular, dirigir, orientar y coordinar las políticas, planes y proyectos para la promoción de las tecnologías de la información y la comunicación y el desarrollo de las telecomunicaciones, así como supervisar y evaluar su cumplimiento";*

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 público 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, mediante Decreto Ejecutivo No. 8, de 13 de agosto de 2009, publicado en el Registro Oficial No. 10, de 24 de agosto de 2009, el Presidente de la República creó el Ministerio de Telecomunicaciones y de la Sociedad de la Información como órgano rector del desarrollo de las Tecnologías de la Información y Comunicación, que incluye las telecomunicaciones y el espectro radioeléctrico;

Que, mediante Acuerdo Ministerial No. 011-2018, de 08 de agosto de 2018, se expide el Plan Nacional de Gobierno Electrónico 2018-2021. Este instrumento muestra la situación actual del país en materia de gobierno electrónico, las acciones que serán ejecutadas en tres programas; Gobierno Abierto, Gobierno Cercano y Gobierno Eficaz y Eficiente. En el Capítulo 1. Fundamentos Generales, literal 5. Diagnóstico se enfatiza que: *"Dentro de las iniciativas relevantes que ha implementado el gobierno entorno a la ciberseguridad se encuentra la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) (…)";*

Que, mediante Acuerdo Ministerial No. 15-2019, del 18 de julio del 2019, se expide la Política Ecuador Digital cuyo objeto es transformar al país hacia una economía basada en tecnologías digitales, mediante la disminución de la brecha digital, el desarrollo de la Sociedad de la Información y del Conocimiento, el Gobierno Digital, la eficiencia de la administración pública y la adopción digital en los sectores sociales y económicos;

Que, la Política Ecuador Digital está compuesto por tres programas: Ecuador conectado, Ecuador eficiente y ciberseguro; y, Ecuador innovador y competitivo. El programa Ecuador eficiente y ciberseguro tiene como objetivo proteger a la sociedad frente a las amenazas cibernéticas, generar confianza en el uso del internet y fomentar el desarrollo económico y social basado en el uso de las Tecnologías de la Información y de la Comunicación (TIC);

Que, el Gabinete Sectorial de Seguridad en Sesión Ordinaria de 8 de mayo de 2019, resolvió entre otros puntos: *"PRESENTACIÓN POLÍTICA DE CIBERSEGURIDAD. El Ministerio de Telecomunicaciones y de la Sociedad de la Información deberá presentar en el próximo Gabinete Sectorial de Seguridad, la Política de Ciberseguridad integrada";*

Que, mediante Acuerdo Nro. 052, de 10 de mayo de 2021, el Secretario General de la Presidencia de la República acordó la subrogación del señor Econ. Julio César Muñoz Bravo, Viceministro de Tecnologías de la Información y Comunicación, al cargo de Ministro de Telecomunicaciones y de la Sociedad de la Información;

Que, la Vigésima Sesión Ordinaria del Gabinete Sectorial de Seguridad tuvo lugar en la ciudad de El Coca el 1 de abril de 2021. En ella se aprobó la Política Nacional de Ciberseguridad y se designó al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) como el encargado de publicarla mediante Acuerdo Ministerial.

Que, mediante Memorando Nro. MINTEL-SGERC-2021-0134-M, de 27 abril de 2021, el Subsecretario de Gobierno Electrónico y Registro Civil remitió el informe técnico de motivación para la publicación de la Política Nacional de Ciberseguridad, en el que se recomienda: *"(...) la publicación del instrumento legal correspondiente para la publicación de la Política Nacional de Ciberseguridad".*

Que con sumilla inserta en el memorando Nro. MINTEL-SGERC-2021-0134-M, el Viceministro de Tecnologías de la Información y Comunicación aprobó el informe y dispuso la emisión de este Acuerdo

En ejercicio de las atribuciones que le confiere el numeral 1 del artículo 154 de la Constitución de la República, el numeral 2 del artículo 141 de la Ley Orgánica de Telecomunicaciones; y, artículo 17 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva.

Acuerda:

Art. 1.- Publicar la Política de Ciberseguridad, que se encuentra anexa y que forma parte integral del presente Acuerdo Ministerial.

Art. 2.- El objetivo de la presente política es construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio.

La política establece directrices que buscan afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país, así como a la creación de una confianza digital que favorece el intercambio de información y, en consecuencia, de bienes y servicios en línea.

La política tiene un enfoque multisectorial y multidimensional que se debe al carácter transversal de la ciberseguridad. Por tanto, la política alcanza a varios sectores y actores, públicos y privados, del país, y de manera vertical y horizontal. En esta medida, la política establece directrices para encaminar las acciones de las entidades de la Administración Pública Institucional y que dependen de la Función Ejecutiva, en coordinación con los otros poderes del Estado, sociedad civil y ciudadanía en general.

Art. 3.- De la ejecución del presente Acuerdo Ministerial, encárguese a la Subsecretaria Gobierno Electrónico y Registro Civil, que ejecutará las acciones necesarias para la implementación de la Política de Ciberseguridad.

Disposición Final.- El presente Acuerdo Ministerial entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dado en Quito, D.M., a los 17 días del mes de mayo del año 2021.

Firmado electrónicamente por:
JULIO CESAR MUNOZ BRAVO

Econ. Julio César Muñoz Bravo
MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (S)


MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN
POLÍTICA NACIONAL
DE CIBERSEGURIDAD
sembramos
Futuro
Lenín

PRESENTACIÓN

Andrés Michelena Ayala
Ministerio de Telecomunicaciones
y de la Sociedad de la Información

La seguridad de toda la población ecuatoriana en el ciberespacio – en el "quinto dominio[1]"-, es prioridad estratégica del Gobierno Nacional. En ese contexto, entidades del sector público y privado, así como de la sociedad civil y la academia, trabajan arduamente en el proceso de construcción de nuestra Política Nacional de Ciberseguridad (PNC).

El Gobierno del presidente Moreno, en uso de sus atribuciones constitucionales, ha trazado y ha definido esta política, enriquecida por actores relacionados, para establecer lineamientos y acciones, sin descuidar el análisis de riesgos y amenazas -potenciales y reales- que enfrenta nuestro país. De esta forma podemos generar más capacidades para: identificar, monitorear, evaluar, gestionar, prevenir, mitigar; en suma, para enfrentar con éxito los riesgos y amenazas.

Para alcanzar un Ecuador Digital Ciberseguro que garantice el Estado de Derecho, proteja los servicios e infraestructuras críticas del Estado y de seguridad a la población en el ciberespacio, el Gobierno trazó su línea de acción asentada en 7 pilares: 1) Gobernanza de ciberseguridad; 2) Sistemas de información y gestión de incidentes; 3) Protección de servicios e infraestructuras críticas digitales; 4) Soberanía y defensa; 5) Seguridad pública y ciudadana; 6) Diplomacia en el ciberespacio y cooperación internacional; 7) Cultura y educación de ciberseguridad.

Estas acciones priorizan el fortalecimiento institucional y la articulación efectiva por parte del Gobierno, de forma ordenada, con un enfoque integral y la activa presencia de múltiples actores. Por ello, las entidades gubernamentales y las entidades privadas del país deben cooperar con responsabilidad. Sólo de esa forma se tendrá un Ecuador Digital Ciberseguro.

Esta política está en línea con la Agenda 2030 para el Desarrollo Sostenible de la ONU, el plan global de acción a favor de las personas, el planeta y la prosperidad, que busca

[1] La seguridad tiene 5 dominios: aire, tierra, mar, espacio y ciberespacio considerado como el quinto dominio, en el cual los estados ahora luchan contra los ataques cibernéticos.

fortalecer la paz universal y el acceso a la justicia. Los Objetivos de Desarrollo Sostenible de la ONU están contenidos en nuestro Plan Nacional de Desarrollo (PND) 2017-2021: acceso seguro a las TIC, internet de las cosas (IoT) y tecnología de la operación (TO). Estos elementos son clave para el desarrollo futuro de las actividades políticas, sociales, culturales y económicas de nuestro país.

En razón de que el dominio del ciberespacio trasciende las fronteras del país, el enfoque de nuestra política se orienta al ámbito internacional; por eso, Ecuador deberá articular acciones para fortalecer la ciberseguridad a nivel regional y multilateral, al tiempo que promueva el uso de tecnologías para el desarrollo socioeconómico del país, en áreas de la economía digital.

Una vez emitida la Política Nacional de Ciberseguridad, el siguiente desafío inmediato será su implementación, el constante monitoreo y la evaluación. Pero el primer paso está dado, gracias a la voluntad política del Presidente Moreno. La puesta en marcha de esta política es un avance muy importante, es un resultado tangible que resalta el compromiso del Gobierno Nacional en materia de ciberseguridad, puesta al servicio de nuestra población. Además, tiene el mérito de posicionar al país en el marco de la Agenda Global Digital, en tiempos tan duros y difíciles como los que afectan al país, a la región y al planeta en general.

ÍNDICE

Índice de Figuras

Índice de Gráficos

Índice de Tablas

LISTADO DE ACRÓNIMOS

APCID	Administración Pública Central, Institucional y Dependiente
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
CERT	Critical Emergency Response Team - Centro de Respuesta Rápida Ante Incidentes Informáticos
CICTE	Comité Interamericano contra el Terrorismo
CIES	Centro de Inteligencia Estratégica
CIRT	Critical Incident Response Team– Centro de respuesta a incidentes informáticos
CSIRT	Critical Security Incident Response Team - Centros de Respuesta Incidentes de Seguridad Informática
E-government Survey	Encuesta de Gobierno Electrónico
EcuCERT	Centro de respuesta a incidentes informáticos del Ecuador
EGDI	Índice de Desarrollo de Gobierno Electrónico
EGSI	Esquema Gubernamental de Seguridad de la Información
ESR	ESET Security Report
FIRST	Forum of Incident Response and Security Teams)
GCI	Índice Global de Ciberseguridad
IC	Infraestructura crítica
ICD	Infraestructura crítica digital
INEC	Instituto Ecuatoriano de Estadísticas y Censos
INEN	Servicio Ecuatoriano de Normalización
IoT	Internet de las cosas
UIT	Unión Internacional de Telecomunicaciones
MDN	Ministerio de Defensa
MDG	Ministerio de Gobierno
MREMH	Ministerio de Relaciones Exteriores y Movilidad Humana
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información
NTE	Norma Técnica Ecuatoriana
OEA	Organización de Estados Americanos

PNC	Política Nacional de Ciberseguridad (PNC)
SDH	Secretaría de Derechos Humanos
SIETEL	Sistema de Información y Estadística de los Servicios de
SOC	Centro de Operaciones de Seguridad
SINARDAP	Sistema Nacional de Registro de Datos Públicos
TIC	Tecnologías de la información y de la comunicación
TO	Tecnologías de la operación
UNCRC	The United Nations Convention on the Rights of the Child - Convención de las Naciones Unidas Sobre los Derechos del Niño

INTRODUCCIÓN

La agenda digital ha tomado mayor relevancia en el contexto actual –crisis por COVID-19- durante el cual se han evidenciado los beneficios y oportunidades que brinda el uso de las tecnologías de la información y comunicación, pero también el incremento de los delitos en línea y por tanto la necesidad de garantizar la seguridad de los ciudadanos en el ciberespacio.

El Ecuador trabaja activamente en el ámbito nacional para garantizar un internet libre, abierto y seguro, a fin de continuar aprovechando los beneficios económicos y sociales que ofrece y que se enmarcan en la agenda de desarrollo sostenible.

En este sentido, la ciberseguridad y la creación de confianza en el ciberespacio se tornan fundamental. Con ello, al igual que en foros internacionales, el Ecuador reconoce que el uso de las TIC ha sido ventajoso para su desarrollo socioeconómico, y que a la vez representa un desafío para la comunidad internacional, por los riesgos y amenazas del ciberespacio.

En el mundo más de 4.100 millones de usuarios tienen acceso a internet (UIT - Unión Internacional de Telecomunicaciones, 2019), que representan más de la mitad de la población mundial[2]. En el caso de las nuevas tecnologías de la información y comunicación, su creciente democratización ha traído consigo cambios y retos permanentes, al constituirse como uno de los pilares del mundo globalizado[3]. El avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivos de violencia y destrucción alrededor del mundo[4]. Es así que un número creciente de personas y grupos obtienen ventajas de la rapidez, conveniencia y anonimato que brinda el Internet para perpetrar una serie de actividades delictivas de sabotaje y terrorismo, que no conocen fronteras físicas, representando amenazas reales para las víctimas a nivel global[5].

[2] Uno de cada tres de estos usuarios es menor de 18 años y accede al internet en su mayoría a través del teléfono celular. Niños niñas y adolescentes en el mundo están en línea alrededor de dos horas al día entre semana y aproximadamente el doble de tiempo el fin de semana

[3] Las Tecnologías de la información y de la comunicación (TIC) son fundamentales para la democratización del conocimiento. Es decir, las TIC constituyen un elemento indispensable de cara a las proyecciones de desarrollo social de los países, de los grupos sociales y de los individuos (Lugo, 2010, IIPE, 2014).

[4] El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado, e incluyendo a la sociedad civil. Según Naciones Unidas, en el mundo los cibercrímenes (o ciberdelitos) llegaría a representar un costo de 600 mil millones USD (ONUDC, 2016).

[5] Un impacto primario del delito cibernético es financiero, considerando que puede incluir muchos tipos diferentes de actividades delictivas con fines de lucro, incluidos ataques de ransomware, fraude por correo electrónico e internet y fraude de identidad, así como intentos de robo de cuentas financieras, tarjetas de crédito u otra información de tarjetas de pago. No obstante, también se ven afectadas las personas y los Estados.

Si en el pasado el delito cibernético era perpetrado principalmente por individuos o por pequeños grupos, en la actualidad se estarían configurando patrones novedosos bajo los cuales operan concertadamente redes delictivas muy complejas en el ciberespacio, que reúnen a individuos en distintos países en tiempo real, para cometer delitos y ataques cibernéticos a una escala sin precedentes. (INTERPOL, 2017).

Entre los principales delitos cibernéticos, se destacan la piratería, que afecta a la propiedad intelectual, los ataques con códigos maliciosos, como por ejemplo ataques de denegación de servicios, que constituyen amenazas a la seguridad de los gobiernos, negocios e individuos y que suponen un desafío para los organismos de seguridad y agencias encargadas de la aplicación de la ley, entre otros. Estos delitos se producen, en parte, debido a que varios países no han desarrollado las capacidades necesarias para prevenir, investigar y combatir este tipo de fenómenos.

En este sentido es importante el "Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan" (CCN-CERT Centro Criptológico Nacional, 2015). El Ecuador entiende a la ciberseguridad como la capacidad del Estado para proteger a las personas, sus bienes activos de información y servicios esenciales ante riesgos y amenazas que se identifican en el ciberespacio. De forma complementaria el país se adhiere al concepto de la Unión Internacional de Telecomunicaciones -UIT- que la concibe como ¨el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y a los usuarios en el ciberentorno¨ (UIT2010, 20).

La ciberseguridad en el Ecuador se enmarca dentro de los deberes constitucionales del Estado, especialmente el desarrollo y el establecimiento de una cultura de paz. Dado el principio integral de la ciberseguridad y asuntos digitales, la presente Política Nacional de Ciberseguridad incluye aspectos que se enmarcan en competencias como la ciberdefensa, la ciberinteligencia y la ciberdiplomacia. Asimismo, se reconoce el alcance nacional, multisectorial y con un enfoque de múltiples actores, en el diseño, implementación y monitoreo de la PNC.

Los principios que rigen esta política son la promoción y el respeto de los derechos humanos y libertades fundamentales, el fomento de la confianza, la resiliencia, la responsabilidad compartida, el f1omento del desarrollo de actividades en el entorno digital y el mercado nacional de TIC. En el marco de un Internet libre, abierto y seguro, prima la comunicación de las personas, la protección de datos, el derecho a la privacidad, y el marco de los objetivos de desarrollo sostenible. Esta política se basa en siete pilares que contemplan diversas temáticas de intervención del Estado, en coordinación con el sector privado, la academia y

sociedad civil, que permitirán la ciberseguridad del Ecuador. Estos pilares se enfocan en el trabajo en la gobernanza de la ciberseguridad, en sistemas de información y gestión de incidentes, en la protección de los servicios e infraestructuras críticas, la soberanía y defensa, la seguridad pública y ciudadana, la diplomacia en el ciberespacio junto con la cooperación internacional y la promoción de la cultura y educación para la ciberseguridad.

El objetivo general de esta política, articulado con sus objetivos específicos, es construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población, así como la protección de los bienes jurídicos del Estado en este dominio; encaminando acciones para garantizar un ciberespacio seguro.

El objetivo contribuirá de manera directa al desarrollo social, económico y humano del país, así como a la creación de una confianza digital fundamental para favorecer el intercambio de información y, en consecuencia, de bienes y servicios en línea, fortaleciendo el compromiso del estado con la ciberseguridad.

Su implementación conlleva un proceso de seguimiento, medición y evaluación continuo y flexible, que permitirá ajustarla efectivamente ante los rápidos cambios en el entorno digital e identificar el impacto de las acciones de esta política en el fortalecimiento de la ciberseguridad nacional. Para que esta política sea efectiva, el estado ecuatoriano deberá asignar los recursos financieros necesarios que aseguren la implementación de las líneas de acción enunciadas en ella.

Esta política tiene un alcance nacional, alineada a la normativa y demás instrumentos de política pública. Debido al carácter ubicuo de la ciberseguridad, la política también se aplica al espectro radioeléctrico y en las infraestructuras digitales, donde se incluyen: los dominios, plataformas y programas donde se maneje información de carácter pública y privada de la población; asimismo, se consideran las infraestructuras con servicios automatizados y los servicios esenciales del Estado como parte de los bienes jurídicos a proteger.

La ciberseguridad se convertirá, progresivamente, en un tema de vital importancia dentro de la agenda de seguridad, desarrollo y derechos humanos en el Ecuador, por lo que se requiere desarrollar y potenciar las capacidades nacionales, políticas, estrategias, planes, programas y proyectos intersectoriales para la seguridad cibernética.

Es esencial la concientización en la sociedad ecuatoriana sobre las potenciales vulnerabilidades que enfrenta en el entorno cibernético, lo que permitirá propender a la garantía de derechos y libertades, como de la seguridad integral en el ciberespacio.

PROCESO DE ELABORACIÓN DE LA POLÍTICA

La elaboración de la presente política parte de un proceso técnico, con la conformación de una mesa interinstitucional, denominado "Grupo interinstitucional de Ciberseguridad", conformada por las siguientes instituciones: Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), quién preside el grupo, el Ministerio de Gobierno (MDG), el Ministerio de Defensa (MDN), el Centro de Inteligencia Estratégica (CIES) y el Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH), que mediante un trabajo interdisciplinario ha contribuido desde los enfoques de cada una de las instituciones participantes, con el fin de garantizar la adaptabilidad de la misma al contexto aplicativo. Este instrumento toma en consideración los intereses nacionales y, a la vez, considera a los temas de ciberseguridad desde una visión holística, común, compartida y de largo plazo.

La determinación de la metodología requirió la revisión de herramientas internacionales existentes para el desarrollo de políticas en este ámbito y un análisis de los avances de otros países en la materia. Asimismo, el desarrollo de este documento incluye la revisión de los marcos normativos vigentes nacionales e internacionales y los instrumentos de planificación nacional de los sectores involucrados. Además, contempla el levantamiento de un diagnóstico nacional que identifica las brechas existentes en cuanto a la ciberseguridad en el país. Una vez priorizadas, estas fundamentaron el diseño de acciones nacionales que permitirán solventar las problemáticas de la ciberseguridad en el Ecuador.

En la construcción de esta política participaron actores de la Función Ejecutiva, al igual que otras funciones del Estado. Se contó con insumos de las Empresas Públicas, de los operadores de infraestructuras críticas, representantes de la academia, centros de respuesta a incidentes, actores del sector privado y de la sociedad civil.

La política propone un horizonte definido al 2023, en el cual se implementarán las líneas de acción definidas en la política y a partir del proceso de seguimiento y monitoreo, se podrán observar los resultados de la misma a corto y mediano plazo.

Figura 1: Aprobación de la Hoja de Ruta para la elaboración de la Política Nacional de Ciberseguridad.

Elaborado por: Grupo Interinstitucional de Ciberseguridad.

ANTECEDENTES

El compromiso del Ecuador con la ciberseguridad ha progresado recientemente con la adopción de varias políticas y estrategias sectoriales que definen el enfoque del gobierno con respecto a la ciberseguridad. Dichas estrategias precisan de coordinación general.

Cabe resaltar que más allá de la ausencia de marcos reglamentarios a nivel nacional para la protección de infraestructura crítica, los sectores financieros y de telecomunicaciones han establecido y adoptado procesos de gestión de riesgos de ciberseguridad y las mejores prácticas en medidas de seguridad.

En tal virtud, esta política se alinea a la normativa nacional vigente y al Plan Nacional de Desarrollo 2017-2021 "Toda una Vida".

Ecuador ha tomado en consideración el avance de las regulaciones internacionales, que se han desarrollado debido al aparecimiento de acciones susceptibles de causar afectaciones negativas, por lo que se emiten normas internas y se aúnan esfuerzos, para ir construyendo una primera generación de normativa nacional.

A continuación, se lista el marco normativo relacionado.

A. Marco normativo

a. Nacional

CONSTITUCIÓN DE LA REPÚBLICA
La Constitución de 2008 se establece como la norma jurídica de mayor jerarquía dentro del ordenamiento jurídico ecuatoriano, primando inclusive sobre los convenios y tratados internacionales salvo excepciones en casos de derechos humanos más beneficiosos, leyes orgánicas y ordinarias, así como las demás normas. Art. 3, 16, 66 (Núm. 19 y 21), 158, 313 y 393
CÓDIGO ORGÁNICO INTEGRAL PENAL
El Código Orgánico Integral Penal, a menudo referido por sus siglas COIP, es un conjunto sistematizado y organizado de normas jurídicas de carácter punitivo, es decir un compendio legislativo que establece delitos y penas conforme al sistema penal ecuatoriano.

Art. 103, 104, 170, 178, 188, 190, 194, 202.1, 202.2, 229 al 234, 262, 353.1, 415.1, 415.2, 472, 476, 526, 553.2,
LEY ORGÁNICA DE LA IDENTIDAD Y DATOS CIVILES
La presente Ley tiene por objeto garantizar el derecho a la identidad de las personas y normar y regular la gestión y el registro de los hechos y actos relativos al estado civil de las personas y su identificación. Art. 1 y 3 (Núm. 4 y 6)
LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO
La presente ley tiene por objeto regular la seguridad integral del Estado democrático de derechos y justicia y todos los habitantes del Ecuador, garantizando el orden público, la convivencia, la paz y el buen vivir, en el marco de sus derechos y deberes como personas naturales y jurídicas, comunidades, pueblos, nacionalidades y colectivos, asegurando la defensa nacional, previniendo los riesgos y amenazas de todo orden, a través del Sistema de Seguridad Pública y del Estado. Art. 2, 3, 10, 11, 38, 41 y 43
LEY ORGÁNICA DE TELECOMUNICACIONES
Esta Ley tiene por objeto desarrollar, el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos. Art. 76, 77, 78, 79, 80, 81, 82, 83, 84, 85 y 140
LEY ORGÁNICA PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES
Esta Ley prevé de manera particular, enfocar la acción del Estado en la sensibilización y prevención de la violencia y con la participación de la ciudadanía, bajo el principio de corresponsabilidad. Estos dos actores deben garantizar a través de políticas, planes y programas, la transformación de los patrones socioculturales y la erradicación de prácticas que naturalizan la violencia contra las mujeres. Esta Ley establece además tres componentes para la erradicación de la violencia: atención, protección y reparación de las mujeres víctimas de violencia para garantizar su seguridad e integridad y para retomar su proyecto de vida. Art 12

LEY ORGÁNICA DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS
Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. Art. 5, 7,8, 9,10, 29, 51, 54, 58, 62, 63, 64
CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN
Protección a los derechos intelectuales y a asumir la defensa de los mismos, como un aspecto imprescindible para el desarrollo tecnológico del país. La ley, incluye en su codificación la protección de bases de datos que se encuentren en forma impresa u otra forma, así como también los programas de ordenador (software).
NORMAS TÉCNICAS
● Familia de NTE INEN-ISO/IEC 27000, principalmente; ✓ NTE INEN-ISO/IEC 27000, Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – Descripción general de vocabulario ✓ NTE INEN-ISO/IEC 27002:2013, Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información. ✓ NTE INEN-ISO/IEC 27005, Tecnología de la Información - Técnicas de Seguridad - Gestión del Riesgo en la Seguridad de la información. ✓ NTE INEN-ISO/IEC 27032, Tecnologías de la Información – Técnicas de seguridad Directrices para Ciberseguridad ● Resolución ARCOTEL-2018-0652, Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de las redes y servicios de telecomunicaciones, publicada en el Registro Oficial No. 331, del 20 de septiembre de 2018. ● Resolución No. SB-2018-771 de la Superintendencia de Bancos, que reforma la Norma de Control para la Gestión del Riesgo Operativo, publicada en el Suplemento del Registro Oficial No. 325, del 12 de septiembre de 2018.

b. Internacional

INSTRUMENTOS INTERNACIONALES
• Carta de las Naciones Unidas. • Convenio de Ginebra y sus Protocolos adicionales. • Resolución AG/RES 2004 (XXXIV-O / 04) de la Organización de Estados Americanos (OEA): Adopción de una Estrategia de Seguridad Cibernética • Resoluciones UNGA 55/63 y 56/121 de las Naciones Unidas sobre la lucha contra el uso de la tecnología de la información con fines delictivos. • Resoluciones UNGA 57/239, 58/199 y 64/211 de las Naciones Unidas sobre la creación de una cultura mundial de seguridad cibernética y la protección de infraestructuras críticas de la información. • Resolución UNGA 73/266 sobre Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. • Declaración para la protección de infraestructura crítica ante las amenazas emergentes – Comité Interamericano contra el Terrorismo de la OEA (20 de marzo de 2015). • Resolución CICTE/RES. 1/19 del 24 de mayo de 2019 sobre Medidas Regionales de Fomento y Confianza en el Ciberespacio (MFCS) del Comité Interamericano contra el Terrorismo.

B. Vinculación de la Ciberseguridad con la Planificación Nacional

Plan Nacional de Desarrollo 2017-2021 "Toda una Vida"
Objetivo 1.- Garantizar una vida digna con iguales oportunidades para todas las personas. Objetivo 7.- Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía. Objetivo 9.- Garantizar la soberanía y la paz, y posicionar estratégicamente al país en la región y el mundo.
Plan Nacional de Seguridad Integral 2019 – 2030
Desde una visión holística de las problemáticas de seguridad para el Estado, evidencia la aparición de amenazas como los ciberataques que identifica como una problemática transversal por el creciente uso de la tecnología.
Agenda de Coordinación Intersectorial de Seguridad
Política PND 9.1 Promover la paz sostenible y garantizar servicios eficientes de seguridad integral. Estrategia 3: Automatización de la obtención y administración de la información para inteligencia estratégicas. Estrategia 4: Coordinación de la cooperación interinstitucional e internacional para fortalecer la gestión de inteligencia.
Política de Defensa Nacional 2018
Reconoce que los ciberataques y las vulneraciones a la infraestructura crítica tienen la capacidad de afectar al Estado. Determina que el ciberterrorismo, ciberespionaje e infiltraciones a los sistemas informáticos son instrumentos de agresión. La política propone el desarrollo de la industria de la defensa con miras a proveer productos y servicios estratégicos especializados para aportar las capacidades de la ciberdefensa.
Plan Específico de Defensa Nacional 2019-2030
Reconoce al ciberespacio como un componente más del territorio ecuatoriano. Las implicaciones se vinculan al desarrollo de operaciones en este dominio para la defensa de la soberanía; con el fin de aportar a la ciberseguridad nacional.

Plan Específico de Seguridad Pública y Ciudadana 2019-2030
Se establecen políticas articuladas y coordinadas de prevención y control respecto de las distintas expresiones del delito y en sus diferentes ámbitos, lo que lleva a prevenir, anticipar y combatir amenazas locales, nacionales e internacionales. La división entre seguridad pública y seguridad ciudadana permite un marco de acción diferenciado sobre la suscitación de delitos, por un lado, una competencia Estatal encaminada al resguardo del orden público y la protección interna, por otro lado, una seguridad ciudadana enfocada en las acciones institucionales dedicadas a reducir los factores de vulnerabilidad hacia el cometimiento de delitos.
Plan Específico de Inteligencia 2019-2030
Este plan entiende como amenaza para el Estado ecuatoriano a todo fenómeno o condición en la que uno o más actores con capacidad y fines específicos generen un daño, pérdida o consecuencia negativa directa contra los ejes de protección de la seguridad integral del Estado, entendiendo a estos como ser humano, Estado y naturaleza. En este contexto, se establece como una de las amenazas para el Ecuador las acciones contra el Estado en el ciberespacio.
Plan Específico de Relaciones Exteriores y Movilidad Humana 2019-2030
Objetivo Estratégico 3: Fomentar la cooperación internacional para la lucha contra la delincuencia organizada transnacional y las amenazas a la seguridad nacional".
Plan Nacional de Sociedad de la Información y del Conocimiento 2018-2021
Es un instrumento de planificación orientado a propiciar el desarrollo nacional en torno al área de la Sociedad de la Información, contiene los programas y proyectos que permitirán alcanzar objetivos trazados en la Política Nacional de Telecomunicaciones y de la Sociedad de la Información. Dentro del Programa 1: Seguridad de la Información y uso responsable de las TIC, se busca de manera primordial fortalecer el marco regulatorio, normativo y estratégico para incrementar la seguridad de la información en el país por lo que promueve la elaboración la Estrategia Nacional de Ciberseguridad que permita determinar los lineamientos generales de la Ciberseguridad en el Ecuador.
Plan Nacional de Gobierno Electrónico 2018-2021
Este Plan plantea catorce estrategias, una de ellas enfocada en la ciberseguridad mencionando como principales beneficiarios a las personas naturales y jurídicas. Además, propone emitir un modelo estandarizado de ciberseguridad para la Administración Pública Central, Institucional y Dependiente (APCID), fortalecer el CERT, capacitar a los funcionarios de la APCID y difundir los beneficios de contar con

este modelo a la ciudadanía.
Política Ecuador Digital
Instrumento cuyo objetivo es transformar y dirigir al país, hacia una economía basada en tecnologías digitales mediante la disminución de la brecha digital, el desarrollo de la Sociedad de la Información y del Conocimiento, el Gobierno Digital, la eficiencia de la administración pública, y la adopción digital en los sectores sociales y económicos, esta política se compone de 3 ejes: Ecuador Conectado, Ecuador Eficiente y Ciberseguro y Ecuador Innovador y Competitivo. Cada uno incluye un conjunto de proyectos para incrementar los índices de accesibilidad a las tecnologías de la información y comunicación, el fortalecimiento de las capacidades de talento humano, la potenciación de los sectores de la economía y el impulso del emprendimiento e innovación; es así que el eje de acción Ecuador Eficiente y Ciberseguro garantiza la participación ciudadana, la democratización de los servicios públicos, la simplificación de trámites, la gestión de la seguridad de la información y la protección de datos personales.
Política Pública por una Internet segura para niños, niñas y adolescentes
Instrumento cuyo objetivo es proteger la dignidad e integridad física, psicológica, emocional y sexual de la niñez y adolescencia; y potenciar las oportunidades y habilidades que ofrecen las tecnologías digitales en su vida y desarrollo integral.
Plan Nacional de Seguridad Ciudadana y Convivencia Social Pacífica 2019 – 2030
Este plan propone crear una estrategia que permita prepararnos con anticipación, ante los riesgos, establece en su Objetivo 7: Implementar anticipación estratégica en las acciones públicas para enfrentar riesgos y amenazas, fundamentalmente los relacionados al crimen organizado, lavado de activos, delincuencia transnacional, terrorismo y cibercriminalidad.

SITUACIÓN ACTUAL

A. Panorama Nacional de la Ciberseguridad

Desde el año 2011, con la "Estrategia Ecuador Digital 2.0" emitida por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), se inició el desarrollo de Políticas Públicas Sectoriales que permitirían que las tecnologías de la información y comunicación se usen efectivamente en el proceso de desarrollo productivo, social y solidario del Ecuador, para el bienestar de todos los ciudadanos. Con el objeto de implementar dicha Estrategia, se impulsaron cuatro planes estratégicos:

- Plan Nacional de Alistamiento Digital.
- Plan Nacional de Gobierno en Línea.
- Plan Nacional de Banda Ancha
- Plan Nacional de Gobierno Electrónico.

El MINTEL, mediante Acuerdo Ministerial Nro. 015-2019, publicado en el Registro Oficial Nro. 69 del 28 de octubre de 2019, emite la "Política Ecuador Digital", cuyo objetivo es transformar y dirigir al país, hacia una economía basada en tecnologías digitales mediante la disminución de la brecha digital, el desarrollo de la Sociedad de la Información y del Conocimiento, el Gobierno Digital, la eficiencia de la administración pública, y la adopción digital en los sectores sociales y económicos, esta política se compone de 3 ejes: Ecuador Conectado, Ecuador Eficiente y Ciberseguro y Ecuador Innovador y Competitivo. Cada uno incluye un conjunto de proyectos para incrementar los índices de accesibilidad a las tecnologías de la información y comunicación, el fortalecimiento de las capacidades de talento humano, la potenciación de los sectores de la economía y el impulso del emprendimiento e innovación; es así que el eje de acción Ecuador Eficiente y Ciberseguro garantiza la participación ciudadana, la democratización de los servicios públicos, la simplificación de trámites, la gestión de la seguridad de la información y la protección de datos personales.

Esta política está enmarcada en los diferentes ejes establecidos en el Acuerdo Nacional 2030 y contribuye a la transformación digital de las instituciones públicas y los diferentes sectores de la economía, permitiendo el incremento de la productividad y competitividad de las empresas.

En el año 2013 el gobierno central desarrolló e implementó el Esquema Gubernamental de Seguridad de la Información (EGSI), lo que permitió ampliar la accesibilidad de sus servicios a los ciudadanos. Esto, a su vez, generó desafíos para la protección de la información de los mismos. El EGSI se implementó en las instituciones de la Administración Pública Central con el fin de que las Instituciones públicas cuenten con un marco de referencia para la gestión de la seguridad de la información.

Los resultados obtenidos del proceso de evaluación fueron la base para la actualización de este esquema gubernamental de seguridad de la información en el año 2020, denominado EGSI V2.0, cuyo objetivo es preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados. Cabe mencionar que según revela el informe "E-government Survey" (E-government Survey 2020, 2020), el Ecuador subió 10 escalones respecto al 2018 en su posición en el Índice de Desarrollo de Gobierno Electrónico (EGDI) de Naciones Unidas. Actualmente, el país ocupa el puesto 74 de 193 países, ubicándolo por encima de la media mundial y regional.

A partir del año 2016, el Plan Nacional de Telecomunicaciones y TI 2016-2021, delinea el futuro del sector de las telecomunicaciones, impulsando la mejora de estos servicios y la reducción de la brecha digital. Además, se actualizó el Plan Nacional de Gobierno Electrónico 2018-2021, que en sus tres ejes de acción y catorce estrategias, vincula a la ciberseguridad con las personas naturales y jurídicas mediante la implementación de la emisión de un modelo estandarizado de ciberseguridad para la Administración Pública Central, Institucional y Dependiente (APCID), el fortalecimiento del Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT) actualmente gestionado por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), y la capacitación de los funcionarios de la APCID en la implementación del modelo de ciberseguridad.

Se ha desarrollado la propuesta de normativa de protección de datos personales a través de la Dirección Nacional de Registro de Datos Públicos (DINARDAP), entidad adscrita al MINTEL y que lidera este esfuerzo, apoyada por sectores claves que ayudan en el desarrollo de dicha normativa, Este proyecto de ley se encuentra en fase de análisis por parte de la Asamblea Nacional. Asimismo, la Ley Orgánica de Telecomunicaciones determina la obligación de los prestadores de servicios de telecomunicaciones de garantizar en el ejercicio de su actividad la protección de datos de carácter personal, al igual que la Ley Orgánica del Sistema Nacional de Registros de Datos Públicos, garantiza la protección de los datos contenidos en todos los registros públicos.

La legislación de protección al consumidor de Ecuador no protege del todo a los consumidores contra el fraude en línea y otras formas de delito cibernético o negligencia comercial y la Defensoría del Pueblo, entidad responsable de la protección del consumidor no tiene capacidades suficientes para abordar la protección del consumidor en línea.

Se ha adoptado una legislación integral sobre propiedad intelectual de productos y servicios en línea y el Servicio Nacional de Derechos Intelectuales (SENADI) está designado como la entidad encargada de velar por su cumplimiento.

En 2020 se emitió la Política de Datos Abiertos, de aplicación para las Instituciones de la Administración Pública, cuyo objetivo es consolidar los procesos de organización y publicación de los datos que generan estas instituciones. La finalidad de esta política es fortalecer la participación ciudadana, la transparencia gubernamental, mejorar la eficiencia en la gestión pública, promover la investigación, el emprendimiento y la innovación en lo que se refiere a tecnologías de la información. Como complemento de esta política el 15 de enero de 2021, se publicó en el Registro Oficial Suplemento Nro. 371 la Guía de Datos Abiertos que permite la implementación de las directrices de la política, y cuyo objetivo es proporcionar criterios técnicos y metodológicos para planificar, abrir, publicar y promover la utilización de los datos abiertos gubernamentales.

Estas acciones estatales junto al aporte del sector privado, han permitido, hasta el 2020, tener los siguientes avances según el reporte de Sistema de Información y Estadística de los servicios de Telecomunicaciones (SIETEL) de la ARCOTEL:

- La masificación del uso de las TIC alcanzó a un 60,7% de la población.
- El uso del internet llegó a un 64,19% de la población.
- La cantidad de abonados que usan teléfonos inteligentes (Smartphones) es de 65,3%.
- Las líneas activas 4G existentes equivalen al 54,79% de la población y el total de líneas activas móviles del 85,75% de la población.
- El número de cuentas de internet de banda ancha alcanzó 1'990.489.

De la misma manera, el MINTEL a través del Proyecto emblemático de "Infocentros Comunitarios", implementó y administra a nivel nacional 886 infocentros y megainfocentros, que dotan a 735 parroquias rurales y urbano marginales de lugares de desarrollo comunitarios apoyados en herramientas TIC, y desde donde se han capacitado a 1'262.960 personas como una de las estrategias para contribuir con su desarrollo personal y profesional.

El incremento en la conectividad de la sociedad en su conjunto, acarrea vulnerabilidades que requieren de la atención de parte de los distintos actores involucrados. En el Ecuador, conscientes de la necesidad de protección en el ciberespacio, en julio del año 2014 se creó el EcuCERT, reconocido como un CIRT (Critical Incident Response Team) nacional oficial de acuerdo al índice mundial de ciberseguridad y perfiles de ciberbienestar (ITU, 2015) y miembro certificado FIRST (Forum of Incident Response and Security Teams).

La Comunidad Objetivo del EcuCERT de ARCOTEL está conformada por: el sector de las telecomunicaciones nacionales y las instituciones públicas, así como aquellas del sector privado que demanden los servicios que EcuCERT ofrece. Si bien EcuCERT está reconocido

como un punto de contacto nacional e internacional para la gestión de vulnerabilidades e incidentes, sus atribuciones se enmarcan en el sector de telecomunicaciones, conforme la Ley Orgánica de Telecomunicaciones que lo rige.

En agosto de 2018, la ARCOTEL expidió la "Norma Técnica para Coordinar la Gestión de Incidentes y Vulnerabilidades que Afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones". En esta norma se establece: la definición de un catálogo de vulnerabilidades e incidentes, tiempos de respuesta, protocolo para la clasificación de la información, mecanismo para el intercambio de información sobre un evento de seguridad y auditorías de seguridad para identificar vulnerabilidades en la infraestructura de los Prestadores de Servicios de Telecomunicaciones.

La falta de regulación en materia de ciberseguridad hace que la aplicación de la normativa excluya a otros sectores por lo que el accionar del EcuCERT es limitado fuera del ámbito de las telecomunicaciones; no obstante, se emiten reportes sobre vulnerabilidades e incidentes a varias instituciones del Estado; así como, consejos y recomendaciones técnicas.

A nivel nacional existen Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT) en las siguientes áreas: académica, defensa, sector privado y sector financiero. Es fundamental articular una estructura o sistema para coordinar sus acciones, y de ese modo, trabajar de manera integrada, en base a protocolos normativa y lineamientos nacionales. El EcuCERT debe fomentar la generación de más CSIRT coordinadores sectoriales, a fin de gestionar los incidentes de manera nacional e intersectorial.

Actualmente, existen trece CSIRT en Ecuador, a través de los cuales; y, enmarcados en un trabajo colaborativo con EcuCERT, se han ejecutado varias acciones técnicas frente a incidentes a nivel nacional. Así mismo, el Ministerio de Gobierno y la Policía Nacional del Ecuador han proyectado la creación de un CSIRT específico que permita la gestión de incidentes informáticos en materia de seguridad pública y ciudadana. Para ello se establecerán los mecanismos formales de colaboración, coordinación, intercambio de información, responsabilidades y respuesta a incidentes, a través de un protocolo nacional de gestión de incidentes nacionales.

Debido a la emergencia sanitaria que se atraviesa a nivel mundial producto de la pandemia por el COVID-19, los gobiernos se han visto obligados a tomar medidas emergentes como el teletrabajo, la teleducación y la telemedicina. En este sentido, organismos e instituciones públicos y privados, así como la población en general, han optado por dichas modalidades. A raíz de esta situación se evidencia un incremento exponencial de incidentes en el ciberespacio en lo que va de este año. En Ecuador, la mayoría de organismos, instituciones y ciudadanía, no están preparados adecuadamente para enfrentar los riesgos asociados a la

seguridad de la información debido a la falta de regulación, políticas, conciencia y herramientas que permitan contar con un ciberentorno seguro.

La cultura de la ciberseguridad en Ecuador no se ha consolidado en su totalidad por cuanto no existe una conciencia generalizada de los riesgos asociados al uso de la Tecnología de la Información y la Comunicación, en especial la Internet. Es decir, no se reconoce a la seguridad en el ciberespacio como un tema prioritario y esto implica que no se toman medidas proactivas para mejorarla. De igual manera, la baja implementación de buenas prácticas de ciberseguridad aumenta las susceptibilidades a diversas amenazas cibernéticas y delitos informáticos.

El país no cuenta con una política nacional que impulse la inversión de recursos para la educación en ciberseguridad. Las mallas escolares no abordan la temática y las universidades no ofrecen carreras enfocadas a la misma. Sin embargo, las discusiones sobre la necesidad de incluir programas de ciberseguridad a nivel universitario han comenzado y existen pocas propuestas de maestrías en temas de ciberseguridad. Se espera que esta política impulse estos programas para que a futuro se pueda cubrir la demanda nacional de profesionales especializados.

En Ecuador están disponibles certificaciones profesionales en ciberseguridad, la mayoría de estas por parte de entidades internacionales. Esto quiere decir que existe una dependencia internacional en lo que respecta a certificaciones tanto para personas como para instituciones. Además, existe un desconocimiento sobre las mismas y algunas son demasiado costosas para el público en general, razón por la cual en muchos casos no se adquieren estas certificaciones.

A nivel gubernamental, una problemática constante es la obsolescencia de los equipos (hardware) y las restricciones presupuestarias para adquirir bienes de larga duración, así como, licencias de software, lo que se configura como un reto para la protección de la información y la labor de las entidades de control.

Un mayor uso de la Internet implica un aumento en la vulnerabilidad de la ciudadanía que hace uso de esta herramienta, tanto en lo profesional como en lo cotidiano. El aprovechamiento de estas vulnerabilidades en el ciberespacio por parte de actores delictuales se ha convertido en una nueva forma de atentar contra los derechos de las personas.

Los delitos informáticos son desterritorializados, es decir que no necesariamente se anclan a las naciones, teniendo capacidades transfronterizas que limitan el actuar policial basado en la circunscripción territorial. Este tipo de delito pasa completamente desapercibido para la víctima quien, por lo general, no es consciente de haber sido perjudicada. Lo que conlleva

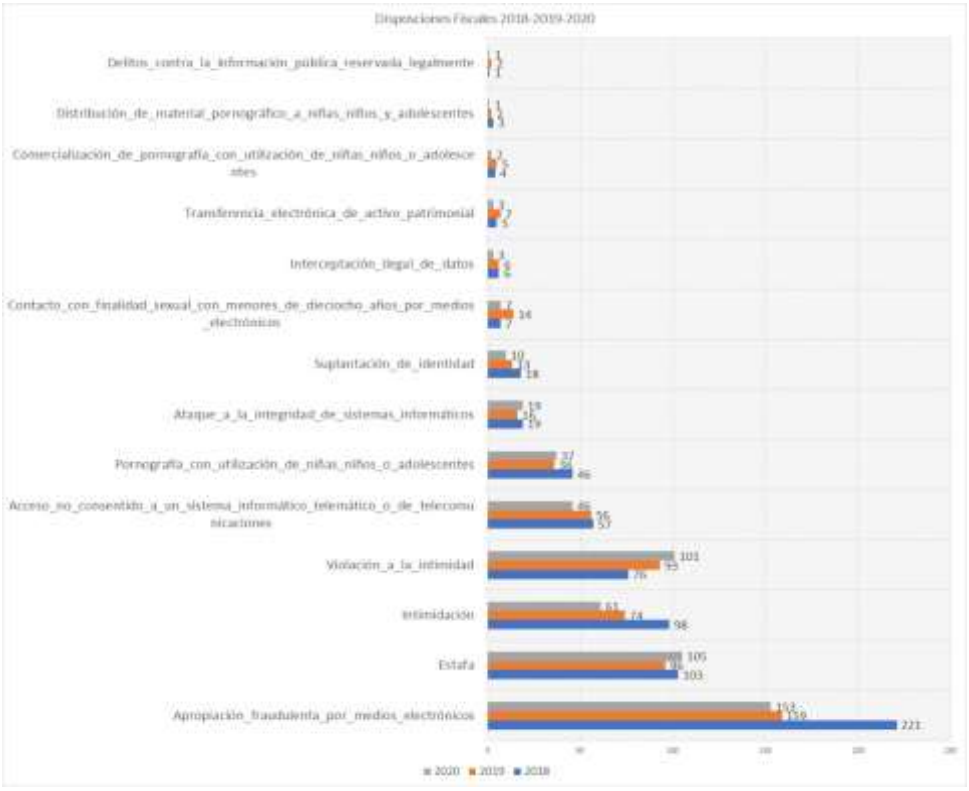
que la mayoría de veces quienes han sido afectados, no presenten la debida denuncia ante las autoridades.

A esto se suma la ausencia de un marco regulatorio que permita conocer los procedimientos policiales y judiciales para identificar y judicializar delitos informáticos, así como la no adhesión a convenios internacionales existentes, que faciliten acciones de cooperación en el ámbito de delitos transnacionales en el ciberespacio.

Las unidades dedicadas al seguimiento e investigación de delitos informáticos requieren incrementar el talento humano especializado en áreas tecnológicas y el número de personal existente para atender oportunamente los requerimientos de la ciudadanía. En este ámbito se requiere que el personal involucrado cuente con capacitación y especialización a nivel de educación superior con el objetivo de tener un dominio de las herramientas existentes y aprovechar al máximo la tecnología, en la lucha contra los delitos informáticos.

La información que mantiene el Ministerio de Gobierno evidencia que el principal delito informático que afecta a la población es la apropiación fraudulenta por medios electrónicos. La siguiente tabla muestra el listado de delitos informáticos registrados en los años 2018, 2019 y 2020

Gráfico 1: Principales delitos informáticos en Ecuador 2018-2019-2020



Fuente: UIDT-DNPJ

En base al riesgo que representan estos delitos y el mal uso del ciberespacio y de las TIC para la ciudadanía y el bienestar de un país, surge la necesidad de estructurar unidades especializadas de las distintas carteras de Estado para identificar, diagnosticar, prevenir y contrarrestar incidentes cibernéticos y demás acciones ilegales que puedan presentarse en el ciberespacio.

Cabe mencionar que las innovaciones en las plataformas de delito cibernético tienen una mayor facilidad de uso y la popularidad de estos servicios conlleva a ataques más eficientes, inclusive siendo empleados por todos los demás grupos de actores de amenaza.

En el marco de la prevención de incidentes cibernéticos se ha priorizado la protección de infraestructuras críticas digitales y servicios esenciales. Salvaguardar estas infraestructuras y servicios no es una tarea nueva, por cuanto desde la óptica de soberanía y seguridad del Estado ya se identificaban áreas estratégicas a defender. Los nuevos enfoques de la seguridad implican un cambio en la óptica de estos espacios vitales para el Estado, los cuales, en torno a consideraciones de desarrollo, económicas, ambientales y de seguridad, amplían el alcance y la concepción de estas infraestructuras.

A nivel regional, el Comité Interamericano contra el Terrorismo (CICTE), de la Organización de los Estados Americanos (OEA), define a las infraestructuras críticas digitales y servicios esenciales como aquellas instalaciones, sistemas y redes, así como servicios y equipos físicos y de tecnología de la información, cuya inhabilitación o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad, la actividad económica, el medio ambiente, servicios de gobierno, o el eficaz funcionamiento de un Estado (…) y que cualquier interrupción de estos (…) tendría graves consecuencias para los flujos de servicios esenciales y el funcionamiento de las cadenas de suministros (OEA/Ser.L/X.2.15; CICTE/doc.1/15).

En lo nacional es imperante desarrollar una concepción de sectores estratégicos que contemple el concepto de protección de la infraestructura crítica digital y servicios esenciales planteado por la OEA. En este sentido, el Ecuador tiene la necesidad de actualizar o desarrollar normativas y regulaciones nacionales que permitan fortalecer la protección de estas infraestructuras y sus servicios.

El Estado ecuatoriano reconoce como una prioridad la protección de las infraestructuras críticas y servicios esenciales, por cuanto las mismas se ven amenazadas por hechos de origen antrópico y también natural. En el país, la mayoría de estas infraestructuras y servicios, tanto públicos como privados, dependen de las TIC y TO para su normal funcionamiento. La vulneración de estos sistemas, ocasionaría la falla e interrupción de servicios esenciales para la sociedad, con graves consecuencias para la población.

Determinar las vulnerabilidades de estas infraestructuras requiere, en principio, su identificación y definición a nivel nacional; su protección es responsabilidad del Estado, de los operadores y de la sociedad civil en general, siendo entonces fundamental la coordinación y cooperación entre sectores públicos y privados.

B. *Análisis de Riesgos y Amenazas*

La identificación de las tendencias emergentes sobre las amenazas cibernéticas y la comprensión de la evolución de los delitos cibernéticos son importantes para la ciberseguridad nacional. El panorama de amenazas cibernéticas proporciona información sobre los desarrollos internacionales relacionados con las amenazas en este aspecto; sin embargo, cada país tiene sus propias peculiaridades. Es vital entender el panorama nacional de amenazas cibernéticas para desarrollar las capacidades de ciberseguridad necesarias y mitigar efectivamente los riesgos en el ciberespacio.

Los ciberataques y ciberdelitos tienen como característica fundamental el ser difíciles de rastrear. Al ser ataques y delitos que se realizan remotamente, su persecución no puede valerse de procedimientos ordinarios, requiriéndose necesariamente de análisis o peritajes informáticos. Además de su carácter remoto, este tipo de ataques y/o delitos se valen de técnicas para ocultar la locación desde la cual se originan. Los ataques informáticos por ejemplo pueden utilizar filtros como proxy chains o virtual private networks (VPN) que evitan los enlaces directos entre las máquinas que realizan los ataques y los servidores de internet, esto hace que los protocolos de internet (IP por sus siglas en inglés) cambien cuando se navega por internet, dificultando a las instituciones del orden conocer la locación, incluso el país de donde se producen estos ataques.

La deep web es un ejemplo de cómo los ciberdelincuentes anonimizan su conexión por internet, navegando por páginas web no indexadas a los motores de búsqueda y evitando los registros o memoria de los buscadores convencionales como Yahoo, Bing, Google, entre otros. Lo anterior, les permite realizar transacciones y demás actividades no autorizadas por ley en el ámbito cibernético. A esto se suma la dark web que consiste en las páginas web que no pueden ser indexadas por motores de búsqueda y para acceder a ellas se necesita software y configuraciones específicas, manteniendo enlaces encriptados entre el usuario y los servidores de internet.

El ciberespacio además de permitir el surgimiento de nuevos tipos de delitos, han perfeccionado delitos de tipificaciones no tan actuales, como es el caso de la pornografía infantil, la cual implica la representación, por cualquier medio, de un niño involucrado en actividades sexuales explícitas reales o simuladas o de sus partes íntimas con fines sexuales

(UNCRC La Convención de las Naciones Unidas sobre los Derechos del Niño, 2002). Las páginas web del deep web y dark web han permitido la consolidación de comercialización de material pornográfico, de armas, de drogas, trata de personas y tráfico de personas. Se han creado verdaderos mercados ilícitos virtuales y anónimos dentro del internet, los cuales se han convertido en maneras de delinquir.

En definitiva, prácticamente todos los delitos comunes se han potenciado con el uso de internet, de las tecnologías comunicacionales y las técnicas de anonimato. Delitos como la extorsión, anteriormente se lo consideraba ligado al secuestro de las personas o al robo de sus bienes tangibles, pero al momento se dan extorsiones en línea, ejerciendo presión a la víctima sobre su información personal y digital, amenazándola con difundir o eliminar su información, obteniendo réditos económicos a cambio de no publicarla. El Ecuador es vulnerable ante las amenazas cibernéticas, esto de acuerdo al Índice Global de Ciberseguridad (GCI), emitido por la ITU, publicado el 09 de julio de 2019, que ubica al país en el puesto 98 de 193, siendo 193 el país con mayores vulnerabilidades a nivel mundial. El número de ataques cibernéticos dirigidos para Ecuador, detectados por la firma de antivirus Kaspersky Lab (2020), refleja que el Ecuador se encuentra en el puesto número 89 de países más atacados en el mundo.

Figura 2: Índice Global de Ciberseguridad (GCI por sus siglas en inglés)

Fuente: Índice Global de Ciberseguridad (GCI)

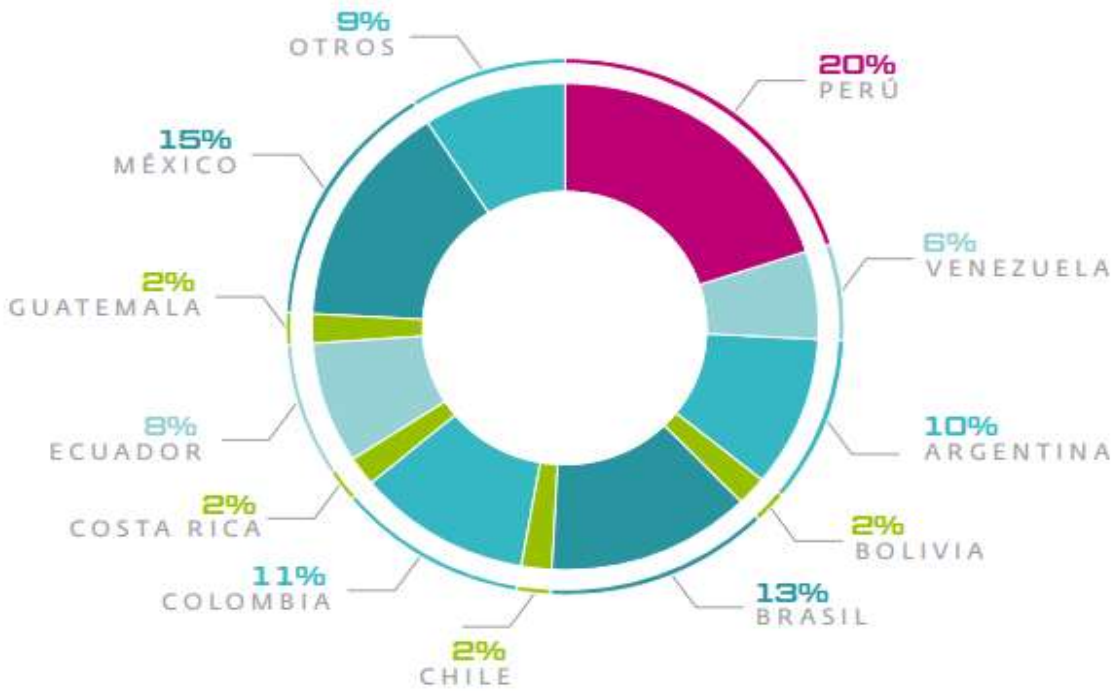
La encuesta multipropósito TIC 2019, realizada por el Instituto Nacional de Estadísticas y Censos (INEC), refleja que el porcentaje de hogares con acceso a la Internet se ha incrementado en los últimos años; en 2019 el 45.5% de hogares a nivel nacional tuvieron acceso a internet. Esta misma encuesta indica que los niños, niñas y adolescentes entre 5 y 17 años, utilizan el internet principalmente desde su hogar (64.5%), desde centros de acceso público (15%) y desde su institución educativa (13.1%). En menor medida lo usan en el trabajo o en otros lugares.

En cuanto al uso de teléfono celular inteligente, en 2019 el 12.2% de personas que tienen teléfono celular inteligente, son niños, niñas y adolescentes entre 5 y 15 años de edad, frente a 1,2% de niños, niñas y adolescentes entre 5 y 15 años de edad que tenían teléfono celular inteligente en el año 2012.

Sin duda, la tecnología y la experiencia digital tienen muchos aspectos positivos, sin embargo, la exposición al mundo digital sin un entorno seguro, implica muchos riesgos, en particular, para niños, niñas y adolescentes: desde trastornos relacionados con el juego, riesgos financieros, recopilación y monetización de datos personales, ciberacoso, ciberbulling, discursos de odio, racismo, violación a la intimidad y/o datos personales y exposición a conductas o contenidos inapropiados, entre otros.

Según la firma ESET, el Ecuador se encuentra entre los 10 países de América Latina más afectados por software malicioso (malware).

Gráfico 2: Detecciones de Ransomware por país

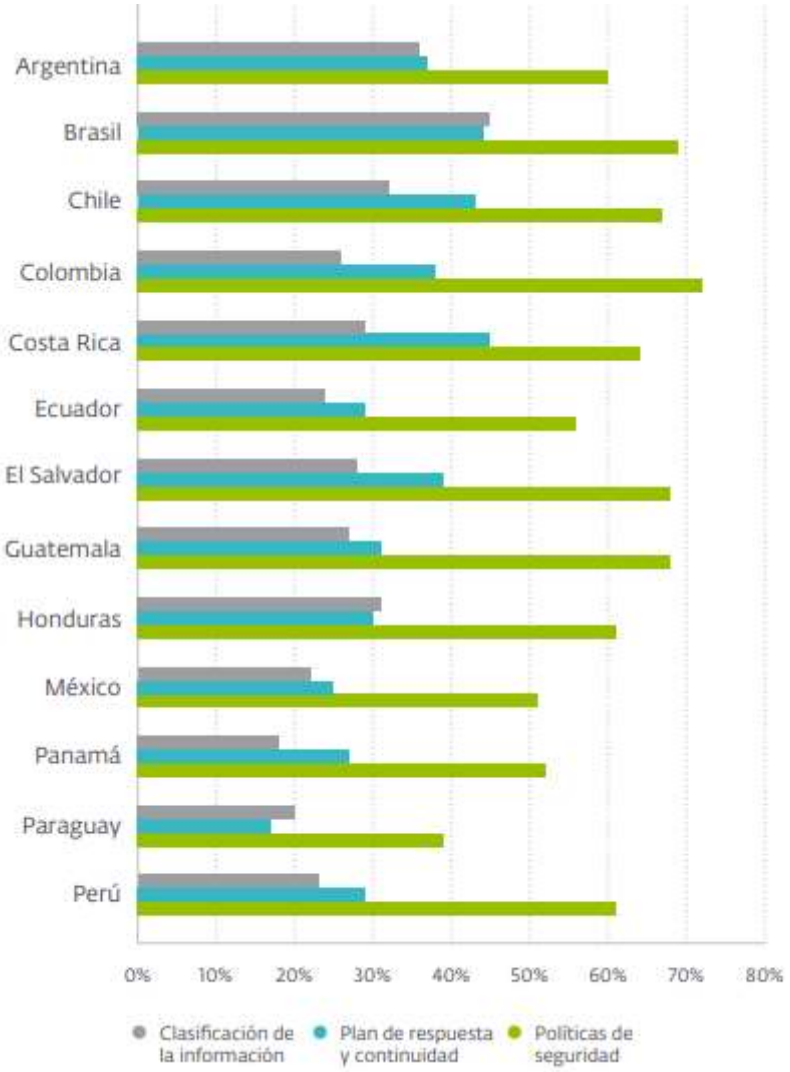


Fuente: ESET Security Report Latinoamerica 2020

En el Informe anual de esta firma; Security Report Latinoamerica 2020 se menciona que la seguridad no solo aborda al área tecnológica, también es necesario complementarla con políticas, planes que permitan gestionar adecuadamente la seguridad de la información.

Esto último se ve reflejado precisamente en que casi el 98% de las empresas en la región cuenta con algún control basado en tecnología. Sin embargo, aún el 39% de las empresas no cuenta con políticas de seguridad y apenas un 28% clasifica su información.

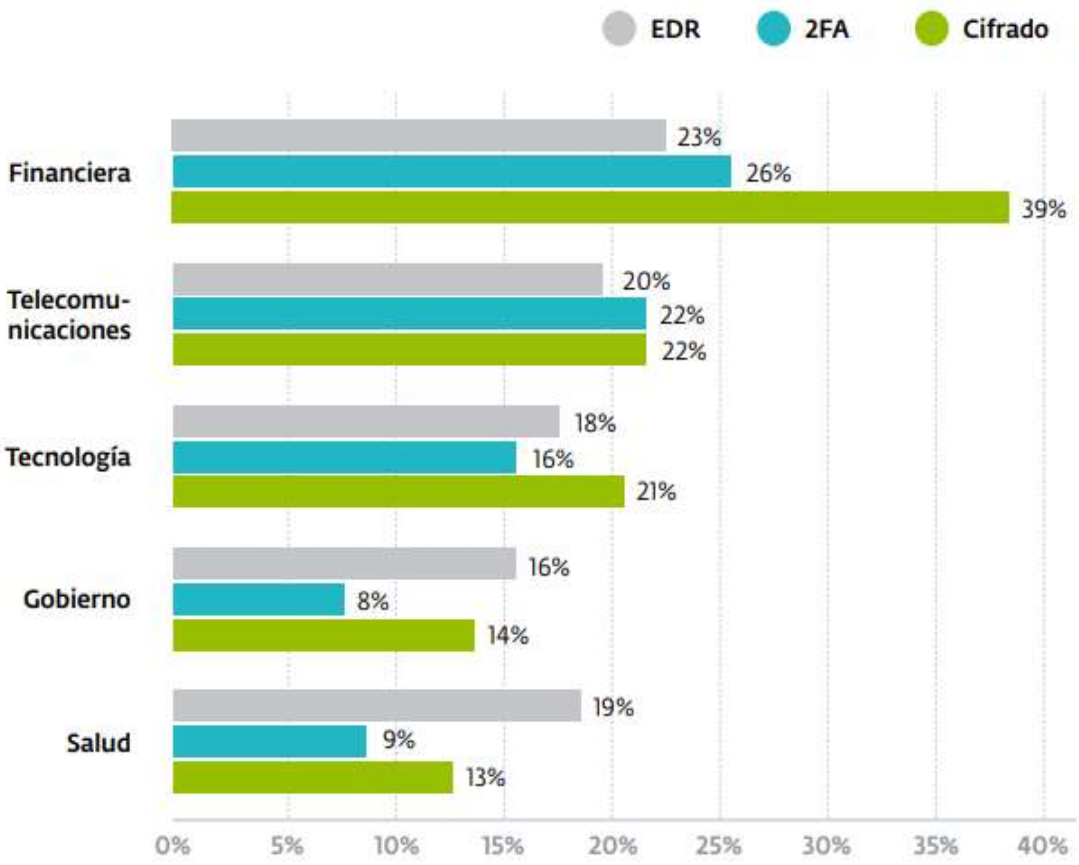
Gráfico 3: Niveles de implementación de prácticas de gestión para la seguridad por país



Fuente: ESET Security Report (ESR) 2020

En el informe anual Security Report (ESR) del 2019, ofrece un panorama sobre el estado de la seguridad digital en los sectores gubernamental, financiero, telecomunicaciones, tecnología y salud en la región. El informe evidencia que la adopción de las medidas y tecnologías de protección es mayor en el sector financiero, ubicándose en los dos últimos puestos los sectores de salud y de gobierno.

Gráfico 4: Implementación de medidas de protección de seguridad por sector en Latinoamérica, 2019.



Fuente: ESET Security Report 2019.

EDR: Endpoint Detection and Response, 2AF: Segundo factor de Autenticidad; Cifrado:

En el año 2019, según el informe realizado por la firma consultora NRD Cyber Security, "Panorama de Amenaza Cibernética y Revisión de la Capacidad de la Ciberseguridad en Ecuador, se identificó que las 10 principales ciberamenazas que afectan al país son: suplantación de identidad, correo no deseado, software malicioso, fuga de información, amenaza interna, manipulación física, robo de identidad, ataques de aplicaciones web, programa de secuestro de datos, denegación de servicio, ataques basados en la web, violaciones de datos, redes de bots, minería de criptomonedas maliciosa y espionaje cibernético[6]. Entre estas amenazas se mencionan tanto vectores de ataque como acciones maliciosas, los cuales son empleados por una variedad de actores.

Los vectores de ataque permiten ejecutar acciones contra los países, sus instituciones, empresas y ciudadanos. El ciberespionaje y/o ciber sabotaje facilita a los actores de amenaza

[6] Panorama de Amenazas y Riesgos (2019). NRD Cybersecurity con el apoyo del BID.

a mejorar su posición estratégica, geopolítica, económica o tecnológica, pudiendo inclusive para este fin llegar a interrumpir la normal prestación y el funcionamiento de la infraestructura crítica y servicios esenciales. Así mismo, algunos de estos actores están en condiciones de obtener, encriptar y eliminar información; impedir accesos y, de este modo, generar afectaciones a la sociedad en su conjunto.

Entre estos actores, uno de los más activos en el Ecuador son los delincuentes cibernéticos. Su principal motivo es la monetización, por lo tanto, dan lugar a amenazas como la suplantación de identidad, software malicioso, entre otros, con el objetivo de atacar a víctimas con un alto potencial de réditos.

Otro actor son los Estados naciones, que han desarrollado capacidades ofensivas cibernéticas muy complejas, las que emplean con fines militares y geopolíticos. La desinformación es otra amenaza, que puede originarse desde los Estados naciones o por parte de los actores internos (insiders), por cuanto el ciberespacio les permite aumentar la velocidad, la escala y la intensidad de estas campañas.

Las corporaciones también se consideran actores que utilizan diferentes vectores a fin de obtener conocimiento competitivo. Por otra parte, los hacktivistas constituyen un grupo de agentes de amenaza con diversas motivaciones y sus actividades se centran principalmente en la lucha por una causa en particular. Sus objetivos suelen ser el gobierno, las organizaciones del sector público y las empresas.

Los actores internos actúan maliciosa o inadvertidamente con diversas motivaciones, entre estas las ganancias financieras; pero, son las acciones no intencionales de los funcionarios y empleados las que están causando la mayor parte del daño a entidades y empresas. Algunos expertos en ciberseguridad ubican a este grupo de agentes de amenaza como una segunda fuente de riesgo después de los ciberdelincuentes.

Todas estas acciones y situaciones llevaron a la nominación, desarrollo y descripción de los pilares que conforman la política que nos ocupa.

PILARES

Los competidores estratégicos del Ecuador, conducen campañas cibernéticas para erosionar nuestro ciberespacio, amenazan nuestra infraestructura crítica y reducir nuestra prosperidad económica. El Gobierno del Ecuador debe perseguir, métodos innovadores para aprovechar nuestras capacidades y recursos existentes en el manejo estratégico de los riesgos en el ciberespacio.

Se han creado pilares que aseguran la existencia y disponibilidad de las funciones críticas de la nación, a la vez que promueven eficacia, innovación, comunicación confiable y prosperidad económica. Estos Pilares cibernéticos son consistentes con nuestros valores nacionales e intentan proteger las libertades de nuestros ciudadanos.

I) Gobernanza de la ciberseguridad

Los actores involucrados y sus interacciones en el sistema de ciberseguridad son la base para la organización en este ámbito. Es por esto que es necesario la conformación de un cuerpo colegiado con el propósito de articular los lineamientos y acciones que aportan al fortalecimiento de la ciberseguridad en el país, que será el "Comité Nacional de Ciberseguridad".

En la actualidad existe un Grupo Interinstitucional de Ciberseguridad para el desarrollo de la política compuesto por las siguientes instituciones: el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), quién preside el grupo, el Ministerio de Gobierno (MDG), el Ministerio de Defensa (MDN), el Centro de Inteligencia Estratégica (CIES) y el Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH).

El Gabinete Sectorial de Seguridad elaboró una propuesta para la creación de cuerpos colegiados con roles, funciones y responsabilidades determinadas. Uno de ellos es el Comité Nacional de Ciberseguridad, cuya estructura sería la misma que la que actualmente tiene el Grupo Interinstitucional de Ciberseguridad, presidida por MINTEL. La emisión de la política deberá incluir una disposición de creación del cuerpo colegiado.

II) Sistemas de información y gestión de incidentes

Este pilar se enfoca en la protección de los sistemas que permiten el procesamiento de datos en todo nivel, por cuanto son fundamentales para las actividades de entidades, empresas y ciudadanía. En este sentido, se considera fundamental la atención a incidentes informáticos

que afecten a estos sistemas impactando la confidencialidad, integridad y disponibilidad de los datos y la entrega y calidad de los servicios.

En este aspecto, el Ecuador mantiene una estructura para el manejo de incidentes de seguridad informática, siendo el EcuCERT la instancia de coordinación nacional. En consecuencia, se fortalecerá la normativa vigente a fin de que ECUCERT pueda establecer mecanismos de articulación y coordinación con los CERT existentes en el país. Este pilar enmarca acciones dirigidas a potenciar la capacidad del país en base a la articulación de los distintos actores, como, instituciones públicas, sector privado, academia, sociedad civil para la atención de eventos en el ciberespacio.

III) Protección de la infraestructura crítica digital y servicios esenciales

Las acciones que se generan en torno a este pilar están encaminadas a construir las condiciones necesarias de robustez y resiliencia para garantizar el normal funcionamiento de las infraestructuras críticas digitales y minimizar el impacto de incidentes en las mismas.

Estas infraestructuras pueden ser vulneradas por medios informáticos, tecnológicos y a través de redes de datos en el ciberespacio. Las repercusiones de estas vulneraciones no se limitan a la parte digital, sino que afectan la parte física en lo referente a su operatividad, la cual se entiende como vital para el desarrollo del país.

Este pilar considera la existencia de infraestructuras críticas digitales y servicios esenciales en diversos ámbitos, cuya afectación, denegación, interrupción o destrucción puede tener consecuencias importantes para los ecuatorianos. La economía, salud pública, sistemas electorales, seguridad, el funcionamiento del Estado y del sector privado, pueden verse vulnerados directamente, impactando el bienestar de la ciudadanía en general.

La protección de estas infraestructuras y servicios exige el trabajo coordinado de todos los actores privados y públicos involucrados, asegurando así su funcionamiento y la entrega de servicios esenciales para la ciudadanía. Por otro lado, su defensa es una parte primordial de la garantía de la integridad territorial y la soberanía nacional.

IV) Soberanía y defensa

Este pilar se fundamenta en el reconocimiento del ciberespacio como un dominio, donde las vulneraciones a los activos digitales y sus afectaciones en el entorno físico, pueden atentar contra la ciudadanía y el Estado en su totalidad.

La ciberdefensa es un complemento de la ciberseguridad, que provee la defensa contra las amenazas en el ciberespacio en beneficio de toda la población. Ésta se fundamenta en las

líneas de acción estratégica de la Política de Defensa 2018 y en el respeto al Derecho Internacional.

El Ecuador promueve una cultura de paz en este dominio, manteniendo como principios la transparencia y la cooperación en ciberdefensa. Este pilar propende el fortalecimiento de la seguridad internacional y el fomento de la confianza entre los Estados, impulsando el diálogo regional e internacional en este ámbito.

El ser humano constituye el eje central de esta política; y, en ese sentido, defender las infraestructuras críticas digitales, tanto en el Ecuador como en las sedes diplomáticas, agregadurías militares, oficinas consulares y oficinas comerciales, se consolida como uno de los objetivos de la ciberdefensa.

La Defensa Nacional contribuirá al desarrollo de la capacidad nacional de resiliencia, para hacer frente a las amenazas que se presenten en el ciberespacio, manteniendo la paz y protegiendo a la población y sus recursos.

V) Seguridad pública y ciudadana

Como parte de una competencia exclusiva del Estado, este pilar obedece a las acciones que se desarrollan para garantizar y proteger los derechos humanos y las libertades ciudadanas, así como la protección de las personas ante un amplio espectro de riesgos y amenazas en el ámbito de los delitos informáticos en el ciberespacio. Para ello se busca afianzar la convivencia social pacífica en todo ámbito, previniendo, avizorando y contrarrestando de acuerdo a las facultades legales, cualquier acción que atente o pretenda transgredir las normas establecidas, con especial énfasis en el dominio digital.

El ordenamiento jurídico penal ecuatoriano abordará concomitantemente el delito cibernético y garantizará la protección de los derechos fundamentales y el estado de derecho.

VI) Diplomacia en el ciberespacio y cooperación internacional

Las amenazas que enfrentamos en el ciberespacio son, en mayor medida, transnacionales y la única forma de abordarlas de manera efectiva es a través del diálogo, la cooperación internacional y la creación y fortalecimiento de la confianza.

En este sentido, el rol de la diplomacia se vuelve relevante, posicionando al Ecuador en la agenda digital global y regional, en varias esferas, tales como la seguridad internacional, los derechos humanos, el desarrollo sostenible, la cooperación internacional, el comercio mundial, entre otros.

Además, la diplomacia reviste de tal importancia debido a que en este tema están en juego cuestiones geopolíticas como la gobernanza del Internet, la seguridad e incluso el ciberconflicto.

Se debe garantizar la calidad de los procesos y seguridad de la información de los órganos del servicio exterior, agregadurías, procesos electorales, oficinas comerciales y, en general, servicios por delegación fuera del país. Para cumplir con este objetivo se deberá realizar el desarrollo normativo, tecnológico y la actualización pertinente de procesos y servicios.
Se reconocen los esfuerzos de la comunidad internacional para el desarrollo de medidas de fomento de la confianza, especialmente en el ámbito interamericano, con el objetivo de minimizar las situaciones de conflictos en el ciberespacio a través de la diplomacia.

VII) Cultura y educación de la ciberseguridad

Las acciones enmarcadas en este pilar promulgan el desarrollo educativo en el ámbito de seguridad en el ciberespacio y fomentan la construcción de una cultura de ciberseguridad que va desde la ciudadanía hasta las entidades públicas o privadas, con el objeto de construir una cultura y generar una conciencia compartida de los riesgos y amenazas en el ciberespacio.

Es fundamental que el país trabaje en el desarrollo de capacidades de los ciudadanos, en todos los niveles de educación, al incluir elementos específicos de la educación en cibernética. El fomento de habilidades en ese ámbito puede desarrollarse en todo momento de la vida educativa de una persona, lo que coadyuvará a contar con una fuerza laboral preparada. El Estado ecuatoriano debe formular políticas educativas al respecto e impulsar el aumento de la oferta académica de tercer y cuarto nivel relacionada directamente con la temática. Así también, es necesario que las universidades, centros de investigación y otras instituciones académicas incluyan a la educación en cibernética entre sus prioridades de investigación.

Este pilar se basa en la necesidad de establecer buenas prácticas y fortalecer el conocimiento de la población en ciberseguridad, por cuanto los usuarios son el principal objetivo por proteger. En este ámbito, las personas son consideradas la primera línea de protección ante los riesgos y amenazas en el ciberespacio.

OBJETIVOS Y LÍNEAS DE ACCIÓN

La política nacional de ciberseguridad establecerá lineamientos para la coordinación de actividades de todas las partes interesadas relevantes en seguridad cibernética, quienes tendrán funciones, responsabilidades claras respaldadas con capacidades operativas suficientes.

OBJETIVO GENERAL

Construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio, encaminando acciones para garantizar un ciberespacio seguro.

Este objetivo contribuirá de manera directa al desarrollo social, económico y humano del país, así como a la creación de una confianza digital fundamental para favorecer el intercambio de información y, en consecuencia, de bienes y servicios en línea, fortaleciendo el compromiso del estado con la ciberseguridad, la cual tiene un campo de aplicación que abarca todas las industrias y todos los sectores, tanto vertical como horizontalmente.

OBJETIVOS ESPECÍFICOS Y LÍNEAS DE ACCIÓN

1. Promover la cooperación entre el sector público y privado a nivel nacional fomentando la confianza y generando respuestas comunes a los riesgos y amenazas del ciberespacio.

   1.1. Establecer un marco normativo e institucional con funciones y responsabilidades de los actores gubernamentales para la ciberseguridad;
   1.2. Adoptar un marco de gestión del riesgo cibernético e integrarlo con un enfoque de resiliencia y seguridad nacional.
   1.3. Articular los diferentes planes, programas y proyectos con las instituciones del sector público y los demás actores involucrados en esta temática.
   1.4. Impulsar la formulación y promulgación de normativa y la adopción de buenas prácticas que viabilicen la interacción y trabajo colaborativo entre los diversos actores del ciberespacio.

2. Potenciar las capacidades de detección, previsión, prevención y gestión de los incidentes cibernéticos, al igual que el manejo de crisis de ciberseguridad de manera oportuna, efectiva, eficiente y coordinada.

2.1. Desarrollar e implementar procesos y herramientas comunes de gestión y atención a incidentes cibernéticos a nivel nacional sobre la base de protocolos de gestión, modelamiento de escenarios de posible ocurrencia e impacto.
2.2. Establecer mecanismos de coordinación interinstitucional que permitan el intercambio efectivo de información y el reporte de incidentes cibernéticos.
2.3. Definir e implementar procedimientos interinstitucionales que fortalezcan la resiliencia cibernética.
2.4. Impulsar el desarrollo y/o actualización de un marco normativo para el sistema nacional de gestión y atención de incidentes en el ciberespacio y definir competencias claras para cada uno de los actores involucrados.
2.5. Fortalecer la capacidad de los CSIRT como elementos clave del sistema nacional de gestión y atención de incidentes cibernéticos.
2.6. Fortalecer la capacidad de protección de datos, información, activos y servicios digitales en el sector público garantizando así la seguridad de los mismos y confianza en el ciberespacio.
2.7. Implementar sistemas de enlace prioritarios normalizados ante crisis cibernéticas

3. Proteger la infraestructura crítica digital del Estado ante amenazas y riesgos en el ciberespacio para garantizar su adecuado funcionamiento y la entrega de servicios esenciales.

3.1. Establecer una metodología compatible con estándares internacionales para la evaluación de riesgos y amenazas.
3.2. Establecer estrategias para evaluar el estado de la ciberseguridad a nivel estatal.
3.3. Identificar y definir la infraestructura crítica digital (ICD) a nivel nacional, teniendo en cuenta que engloba múltiples sectores, basándose en consideraciones políticas, sociales, económicas y ambientales.
3.4. Reducir el nivel de vulnerabilidades identificadas en la infraestructura crítica digital, fundamentado en la gestión de riesgos.
3.5. Establecer e implementar un modelo de coordinación entre las instituciones del Estado y los propietarios de las ICD, en base a la construcción de confianza.
3.6. Fortalecer la capacidad de resiliencia para asegurar la disponibilidad de las IC y servicios esenciales.
3.7. Fortalecer la capacidad de defensa de las áreas reservadas de seguridad e ICD en el ciberespacio en línea con la política exterior ecuatoriana.
3.8. Organizar ejercicios nacionales de ciberseguridad para evaluar la efectividad de los planes de contingencia establecidos.
3.9. Simular escenarios de crisis cibernética para la defensa y evaluar la respuesta de las mismas.
3.10. Impulsar un marco normativo y de buenas prácticas que fundamente la protección y defensa de las infraestructuras críticas digitales y servicios esenciales.

3.11. Monitorizar, analizar, mitigar y neutralizar las amenazas para reducir el nivel de riesgos en el ciberespacio con impacto en la soberanía del país.
3.12. Fortalecer las capacidades institucionales y operativas de defensa, exploración y respuesta ante la situación de ciberataques.

4. Resguardar la seguridad pública y ciudadana en el ciberespacio, previniendo y contribuyendo a la investigación de delitos cibernéticos, para el normal desarrollo de las actividades públicas y privadas, y el ejercicio de los derechos fundamentales de la ciudadanía, en un entorno de confianza.

4.1. Proteger los activos digitales tanto públicos como privados dentro del ámbito de delitos informáticos que atenten a la seguridad ciudadana en el ciberespacio.
4.2. Fortalecer las capacidades institucionales y operativas para la prevención, previsión y respuesta ante la suscitación de ciberdelitos.
4.3. Establecer y promover mecanismos de denuncia del delito cibernético.
4.4. Adaptar el ordenamiento penal interno relativo al cibercrimen con los estándares internacionales.

5. Potenciar la diplomacia ecuatoriana en el ámbito de la ciberseguridad por medio de los espacios de cooperación a nivel regional e internacional, en línea con el interés nacional y la política exterior del Ecuador.

5.1. Insertar al Ecuador en la agenda digital global y regional.
5.2. Representar al Ecuador en las negociaciones sobre la temática en foros internacionales y posicionar la agenda digital en las relaciones bilaterales, regionales y multilaterales.
5.3. Liderar el camino para la adhesión del Ecuador a la Convención de Budapest y otros instrumentos internacionales, que respondan al interés nacional.
5.4. Transversalizar los asuntos digitales nacionales en el marco de cumplimiento de la Agenda 2030 para el Desarrollo Sostenible.
5.5. Fortalecer la cooperación internacional en asuntos de ciberseguridad.
6. Generar una cultura de ciberseguridad y promover el uso responsable del ciberespacio en el Ecuador.

6.1. Fomentar la conciencia ciudadana, empleo responsable de las tecnologías y promoción de conocimiento en el ámbito de la ciberseguridad., así como también promover campañas de sensibilización sobre las distintas formas de violencia y delitos cibernéticos para su prevención.
6.2. Impulsar planes, proyectos e iniciativas de educación en ciberseguridad en todos los niveles, que contribuyan al fortalecimiento en la construcción de las capacidades nacionales.

RESPONSABILIDADES DE LAS ÁREAS DE OPERACIÓN.

Para cumplir con la ejecución de la Política Nacional de Ciberseguridad (PNC), se precisa establecer responsables directos y permanentes para cada uno de los pilares y objetivos establecidos. Además, es necesaria la coordinación estratégica de cada una de las instituciones responsables en materia de ciberseguridad, a fin de mejorar la eficiencia y eficacia en el ámbito de la Ciberseguridad.

Las responsabilidades acorde a las necesidades y en función de los roles y tareas que cada institución debe cumplir, quedan establecidas de la siguiente manera.

PILAR	OBJETIVO	INSTITUCIÓN RESPONSABLE
I. Gobernanza de la ciberseguridad	OBJETIVO 1	Ministerio de Telecomunicaciones (MINTEL)
II. Sistemas de información y gestión de incidentes	OBJETIVO 2	Ministerio de Telecomunicaciones (MINTEL)
III. Protección de la infraestructura crítica digital y servicios esenciales.	OBJETIVO 3	Ministerio de Defensa Nacional (MDN)
IV. Soberanía y defensa.		
V. Seguridad pública y ciudadana.	OBJETIVO 4	Ministerio de Gobierno (MDG)
VI. Diplomacia en el ciberespacio y cooperación internacional	OBJETIVO 5	Ministerio de relaciones Exteriores (MREMH)
VII. Cultura y educación de la ciberseguridad	OBJETIVO 6	Ministerio de Telecomunicaciones (MINTEL)

SEGUIMIENTO Y MONITOREO DE LAS LÍNEAS DE ACCIÓN

La definición de objetivos específicos, metas, indicadores y responsables descritos a continuación, corresponden a las líneas de acción definidas a corto y mediano plazo. Estas líneas se plantean hasta el año 2023 y que deben implementarse en las instituciones de la administración pública, a partir de la aprobación de la presente política.

En este sentido el indicador general de gestión de esta política se enmarca en el Índice de Ciberseguridad Global (GCI), el cual se lo define en base a 25 indicadores, los cuales están repartidos dentro de 5 pilares definidos en la Agenda Global de Ciberseguridad de la ITU.

La Agenda Global de Ciberseguridad de la ITU es un marco para la cooperación internacional orientada a mejorar la confianza y la seguridad en la sociedad de la información.

Se sugiere la revisión del presente instrumento y de la normativa relacionada directa o indirectamente con la política cada 3 años, o cuando se produzca un cambio de mandato institucional. Así se podrá verificar la eficacia y eficiencia de las líneas de acción establecidas, las cuales permitirán al país lograr una mejor resiliencia cibernética nacional y garantizar el bienestar de una nación.

OBJETVOS ESPECIFICOS Y LÍNEAS DE ACCIÓN	METAS	INDICADOR	RESPONSABLES
1. Promover la cooperación entre el sector público y privado a nivel nacional fomentando la confianza y generando respuestas comunes a los riesgos y amenazas del ciberespacio.			
1.2. Adoptar un marco de gestión del riesgo cibernético e integrarlo con un enfoque de resilencia y seguridad nacional.	Incrementar el número de instituciones que implementen un marco de gestión del riesgo cibernético.	Número de instituciones que implementan la gestión de riesgo aplicando el marco de referencia nacional de seguridad de gestión de riesgos más amplio.	MINTEL en consulta con el MDN, CIES, MINTEL, el ámbito académico y la Sociedad civil.
1.3. Articular diferentes planes, programas y proyectos con las instituciones del sector	Incrementar el número de proyectos definidos para la implementación de la política nacional de	Número de proyectos definidos para la implementación de la política nacional de	MINTEL en consulta con el MDN, CIES, MINTEL, el ámbito académico y la Sociedad civil.

público y los demás actores involucrados en esta temática.	ciberseguridad y de las estrategias que de esta se deriven.	ciberseguridad y las estrategias que de esta se deriven.	
	Incrementar el número de riesgos cibernéticos identificados.	Número de riesgos cibernéticos identificados.	ECUCERT EN CORDINACIÓN CON OTROS ACTORES.
	Monitoreo de riesgos cibernéticos registrados.	Porcentaje de Riesgos cibernéticos monitoreados.	MINTEL, ECUCERT.
1.4. Impulsar la formulación y promulgación de normativa y la adopción de buenas prácticas que viabilicen la interacción y trabajo colaborativo entre los diversos actores del ciberespacio.	Incrementar el número de propuestas normativas en ciberseguridad formuladas.	Número de propuestas normativas en ciberseguridad formuladas.	MINTEL, asignará responsables En coordinación con Fiscalía, Asamblea, instituciones públicas y privadas.
	Incrementar el número de Buenas prácticas en los ámbitos de seguridad de la información, seguridad de redes, seguridad de comunicaciones, seguridad de datos personales, etc.	Número de buenas prácticas en ciberseguridad adaptadas o adoptadas (implementadas).	MINTEL, INSTITUCIONES.
2. Potenciar las capacidades de detección, previsión, prevención y gestión de los incidentes cibernéticos, al igual que el manejo de crisis de ciberseguridad de manera oportuna, efectiva, eficiente y coordinada.			
2.1 Desarrollar e implementar procesos y herramientas comunes de gestión y atención a incidentes cibernéticos a nivel nacional sobre la base de protocolos, modelamiento de escenarios y posible ocurrencia e impacto.	Incrementar el número de instituciones que implementen procesos y herramientas para la gestión de incidentes cibernéticos.	Número de instituciones con procesos y herramientas comunes de gestión de incidentes cibernéticos implementados.	MINTEL
2.2 Establecer mecanismos de coordinación interinstitucional que permitan el intercambio efectivo de información y el reporte de incidentes cibernéticos.	Incrementar el número de Convenios institucionales con instituciones privadas para el intercambio de información.	Número de convenios firmados para el intercambio de información y reporte de incidentes cibernéticos.	MINTEL

2.3 Definir e implementar procedimientos interinstitucionales que fortalezcan la resiliencia cibernética.	Incrementar el número de Instituciones que implementen el procedimiento para gestión de incidentes ante una crisis cibernética.	Número de procedimientos implementados en las instituciones públicas para la gestión de incidentes ante una crisis cibernética.	MINTEL
2.4 Impulsar el desarrollo y/o actualización de un marco normativo para el sistema nacional de gestión y atención de incidentes en el ciberespacio y definir competencias claras para cada uno de los actores involucrados.	Incrementar el número de propuestas de instrumentos normativos que incluyan la gestión de riesgos cibernéticos.	Número de propuestas de creación o mejora de los instrumentos normativos que incluyen atribuciones para la gestión de incidentes cibernéticos.	MINTEL
2.5 Fortalecer la capacidad de los CSIRT como elementos clave del sistema nacional de gestión y atención de incidentes cibernéticos.	Incrementar el número de CSIRT.	Número de CSIRT creados o fortalecidos.	MINTEL (CSIRT NACIONAL-ECUCERT)
	Incrementar el número de CSIRT evaluados en nivel de madurez SIM 3.	Número de CSIRT evaluados en nivel de madurez (Security Incident Management Maturity Model - SIM3).	MINTEL (CSIRT NACIONAL-ECUCERT)
	Incrementar el porcentaje de servidores de los CSIRT y SOC gubernamentales capacitados.	Porcentaje de servidores de los CSIRT y SOC gubernamentales capacitados.	MINTEL (CSIRT NACIONAL-ECUCERT)
2.6 Fortalecer la capacidad de protección de la información, activos y servicios digitales en el sector público garantizando así la seguridad de los mismos y la confianza en el ciberespacio.	Crear el SOC gubernamental.	Creación de SOC gubernamental.	MINTEL (CSIRT NACIONAL-ECUCERT)
2.7 Implementar sistemas de enlace prioritarios normalizados ante crisis cibernéticas.	Incrementar el Número de ejercicios realizados de simulación de crisis entre CSIRT.	Número de ejercicios realizados de simulación de crisis entre CSIRT.	El CERT nacional ECUCERT, una vez establecido
3. Proteger la infraestructura crítica del estado ante amenazas y riesgos en el ciberespacio para garantizar su adecuado funcionamiento y la entrega de servicios esenciales.			

3.3. Identificar y definir la infraestructura crítica digital (ICD) a nivel nacional, teniendo en cuenta que engloba múltiples sectores, basándose en consideraciones sociales, económicas y ambientales.	Elaborar el 100% del catálogo de la infraestructura crítica digital a nivel nacional.	Porcentaje de avance del Catálogo de Infraestructuras Críticas Digital del Ecuador.	MDN Y MINTEL
3.4. Reducir el nivel de vulnerabilidades identificadas en la infraestructura crítica digital fundamentado en la gestión de riesgos.	Reducir el nivel de riesgo de las infraestructuras críticas digitales.	Número de operadores de infraestructura crítica digital que disponen de planes de contingencia.	MDN Y MINTEL
	Reducir el nivel de vulnerabilidad de la infraestructura crítica digital.	Número de vulnerabilidades divulgadas de la infraestructura crítica digital.	MDN Y MINTEL
3.5. Establecer e implementar un modelo de coordinación entre las instituciones del Estado y los propietarios de las ICD, en base a la construcción de confianza.	Realizar ejercicios de simulación a nivel de ICD	Número de ejercicios realizados (exitosos y fallidos).	MDN Y MINTEL
3.6. Fortalecer la capacidad de resiliencia para asegurar la disponibilidad de las ICD y servicios esenciales.	Capacidad de resiliencia de la ICD 75% al culminar los 3 años.	Porcentaje de redes con redundancia adecuada y conectividad múltiple.	MDN Y MINTEL
3.7. Fortalecer la capacidad de defensa de las áreas reservadas de seguridad e infraestructura crítica digital en el ciberespacio en línea con la política exterior ecuatoriana.	Actualizar el 100% de los instrumentos de planificación relacionados con la defensa de las áreas reservadas de seguridad y las ICD en el ciberespacio.	Porcentaje de instrumentos de planificación relacionados con la defensa de las áreas reservadas de seguridad y las infraestructuras críticas en el ciberespacio actualizados.	MIDENA
3.8. Organizar ejercicios nacionales de ciberseguridad para evaluar la efectividad de los planes de contingencia establecidos.	Ejercicio realizado por año.	Número de ejercicios realizados.	El SNGRE en cooperación con MINTEL, el MIDENA, el CIES, el ámbito académico, la sociedad civil y los propietarios de ICI.

3.9. Simular escenarios de crisis cibernética para la defensa y evaluar la respuesta de las mismas.	Ejercicio realizado por año.	El número de organizaciones con roles y responsabilidades claros en la respuesta de la ciberdefensa. El número de ejercicios realizados en el año, resultados de cada ejercicio y su evaluación de acuerdo a un checklist.	MIDENA y COCIBER
3.10. Impulsar un marco normativo y de buenas prácticas que fundamente la protección y defensa de las infraestructuras críticas y servicios esenciales.	Establecer un protocolo entre las instituciones del Estado y los propietarios de las ICD.	Protocolo de atención ante ciberincidentes entre las instituciones del Estado y los propietarios de las ICD aprobado.	MIDENA Y MINTEL
4. Resguardar la seguridad pública y ciudadana en el ciberespacio previniendo y contribuyendo a la investigación de delitos cibernéticos, para el normal desarrollo de sus actividades públicas y privadas y el ejercicio de los derechos fundamentales de la ciudadanía, en un entorno de confianza			
4.1. Proteger los activos digitales tanto públicos como privados dentro del ámbito de delitos informáticos que atenten a la seguridad ciudadana en el ciberespacio.	Incrementar la generación de los productos de inteligencia sobre incidentes cometidos a través de medios tecnológicos, electrónicos y telemáticos	Número de productos de inteligencia generados sobre incidentes cometidos a través de medios tecnológicos, electrónicos y telemáticos.	MDG, Dirección General de Inteligencia Policial
4.2. Fortalecer las capacidades institucionales y operativas para la prevención, previsión y respuesta ante la suscitación de ciberdelitos.	Incrementar la asistencia a las denuncias de delitos cometidos a través de medios tecnológicos, electrónicos y telemáticos derivadas al Sistema de Investigación.	Porcentaje trimestral de detenidos sobre investigaciones realizadas. Número de denuncias de delitos cometidos a través de medios tecnológicos, electrónicos y telemáticos.	Ministerio de Gobierno Dirección General de Investigación Dirección Nacional de Investigación de la Policía Judicial Fiscalía General del Estado
4.3. Establecer y promoverán mecanismos de denuncia del delito cibernético.		Número de reportes recibidos a través de los mecanismos de denuncia establecidos.	El Ministerio de Gobierno, el SDH, FISCALIA
5. Potenciar la diplomacia ecuatoriana en el ciberespacio por medio de los espacios de cooperación a nivel regional e internacional, en línea con el interés nacional y la política exterior del Ecuador.			

5.2. Representar al Ecuador en las negociaciones sobre la temática en foros internacionales y posicionar la agenda digital en las relaciones bilaterales, regionales y multilaterales.	Propuesta sobre asuntos digitales en negociaciones de documentos en el ámbito regional o en foros multilaterales.	Número de propuestas sobre asuntos digitales presentadas en negociaciones de documentos en el ámbito regional o en foros multilaterales.	MREMH
5.3. Liderar el camino para la adhesión del Ecuador al Convenio de Budapest y otros instrumentos internacionales, que respondan al interés nacional.	Hasta el 2023, se ha continuado con el proceso para la adhesión del Ecuador al Convenio de Budapest.	Avance en el proceso para la adhesión del Ecuador al Convenio de Budapest y, de existir, a otros instrumentos internacionales.	MREMH
5.4. Transversalizar los asuntos digitales nacionales en el marco de cumplimiento de la Agenda 2030 para el Desarrollo Sostenible.	Hasta el 2023, se ha presentado el tercer Examen Nacional Voluntario en el Foro Político de Alto Nivel sobre Desarrollo Sostenible en el cual se ha visibilizado los avances y reducción de brecha en temas de asuntos digitales en el Ecuador.	Examen Nacional Voluntario en el Foro Político de Alto Nivel sobre Desarrollo Sostenible, que incluye avances y reducción de brecha en temas de asuntos digitales en el Ecuador.	MREMH
5.5. Fortalecer la cooperación internacional en asuntos digitales.	Hasta el 2023, se han logrado al menos un acuerdo de cooperación para capacitación en asuntos digitales.	Número de acuerdos de cooperación para capacitación en asuntos digitales.	MREMH
6. Generar una cultura de ciberseguridad y promover el uso responsable del ciberespacio en el Ecuador			
6.1. Fomentar la conciencia ciudadana, empleo responsable de las tecnologías y promoción de conocimiento en el ámbito de la ciberseguridad, así como también promover campañas de sensibilización sobre las distintas formas de violencia y delitos cibernéticos para su prevención.	Incrementar las capacidades de los servidores públicos en ciberseguridad.	Porcentaje de servidores de las instituciones capacitados en temas de ciberseguridad.	MDT
		Número de campañas nacionales para la prevención de ciberdelitos y la protección de niños, niñas y adolescentes (NNA) en entornos digitales.	MDG (POLICÍA NACIONAL) Consejo Nacional para la Igualdad Intergeneracional.

6.2. Impulsar planes, proyectos e iniciativas de educación en ciberseguridad en todos los niveles, que contribuyan al fortalecimiento en la construcción de las capacidades nacionales.	Incrementar al 2023 la realización de campañas nacionales de sensibilización sobre ciberseguridad.	Número de campañas nacionales de información y sensibilización sobre ciberseguridad, ejecutadas.	MINTEL, MDN, MDG (POLICÍA NACIONAL), CIES, MREMH MINEDUC, ACADEMIA.

Tabla 1: Objetivos y Líneas de acción.

Referencias

CCN-CERT Centro Criptológico Nacional . (2015). *https://www.ccn-cert.cni.es/.* Obtenido de https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

E-government Survey 2020. (julio de 2020). *https://publicadministration.un.org/en/Research/UN-e-Government-Surveys.*

ESET. (2020). *Security Report Latinoamerica 2020.* Obtenido de https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

INTERPOL. (2017). *INFORME ANUAL DE INTERPOL - 2017.*

Joint Committee on Human Rights. (2002). *https://publications.parliament.uk/pa/jt200203/jtselect/jtrights/117/117.pdf.* Obtenido de https://publications.parliament.uk/pa/jt200203/jtselect/jtrights/117/117.pdf

UIT - Unión Internacional de Telecomunicaciones. (Noviembre de 2019). *ITU* . Obtenido de https://www.itu.int/es/mediacentre/Pages/2019-PR19.aspx

UNCRC La Convención de las Naciones Unidas sobre los Derechos del Niño. (2002). *https://publications.parliament.uk/pa/jt200203/jtselect/jtrights/117/117.pdf.* Obtenido de https://publications.parliament.uk/pa/jt200203/jtselect/jtrights/117/117.pdf

República del Ecuador

Junta de Regulación Monetaria Financiera

Resolución No. 665-2021-G

LA JUNTA DE POLÍTICA Y REGULACIÓN MONETARIA Y FINANCIERA

CONSIDERANDO:

Que el artículo 13 del Código Orgánico Monetario y Financiero, publicado en el Segundo Suplemento del Registro Oficial No. 332 de 12 de septiembre de 2014, creó la Junta de Política y Regulación Monetaria y Financiera, parte de la Función Ejecutiva, responsable de la formulación de las políticas públicas y la regulación y supervisión monetaria, crediticia, cambiaria, financiera, de seguros y valores;

Que la Junta de Política y Regulación Monetaria y Financiera, conforme al numeral 43 del artículo 14 del Código Orgánico Monetario y Financiero, mediante resolución No. 386-2017-G de 1 de junio de 2017, designó a la economista Verónica Artola Jarrín como Gerente General del Banco Central del Ecuador;

Que la Disposición Transitoria Primera de la Ley Orgánica Reformatoria del Código Orgánico Monetario y Financiero para la Defensa de la Dolarización, publicada en el Suplemento del Registro Oficial No. 443 de 3 de mayo de 2021, previene: *"Primera.- La estructura y funciones de la Junta de Política y Regulación Monetaria y Financiera y del Banco Central del Ecuador se mantendrán según lo establecido en el Código Orgánico Monetario y Financiero vigente hasta antes de esta reforma, mientras se conforman dentro del plazo de 90 días, contados a partir de la expedición de la presente ley, la Junta de Política y Regulación Financiera, la Junta de Política y Regulación Monetaria y se designe al Gerente General del Banco Central del Ecuador.*

Una vez constituidas las Juntas y nombrado el Gerente General del Banco Central del Ecuador, cada uno en el ámbito de sus competencias atenderá todos los temas y trámites pendientes que venía atendiendo la Junta de Política y Regulación Monetaria y Financiera.";

Que mediante oficio No. BCE-BCE-2021-0689-OF de 25 de mayo de 2021 dirigido al doctor Simón Cueva Armijos, Ministro de Economía y Finanzas, Presidente de la Junta de Política y Regulación Monetaria y Financiera, la economista Verónica Artola Jarrín presenta su renuncia al cargo de Gerente General del Banco Central del Ecuador;

Que de conformidad con el artículo 14, numeral 43 del Código ibídem, en concordancia con lo establecido en la Disposición Transitoria Primera de la Ley Orgánica Reformatoria del Código Orgánico Monetario y Financiero para la Defensa de la Dolarización, publicada en el Suplemento del Registro Oficial No. 443 de 3 de mayo de 2021, la Junta de Política y Regulación Monetaria y Financiera tiene la función de nombrar al Gerente General del Banco Central del Ecuador;

Que la Junta de Política y Regulación Monetaria y Financiera en sesión extraordinaria por medios tecnológicos convocada el 8 de junio de 2021, y celebrada el 9 de junio de 2021, conoció la renuncia de la economista Verónica Artola Jarrín; y la postulación efectuada por el Ingeniero Marco López Narváez, para que el economista Guillermo Enrique Avellán Solines sea designado como Gerente General del Banco Central del Ecuador; y,

En ejercicio de sus funciones,

RESUELVE:

ARTÍCULO ÚNICO.- En el Capítulo IV "Renuncias, Encargos y Designaciones", del Título I "De la Junta de Política y Regulación Monetaria y Financiera", del Libro Preliminar "Disposiciones Administrativas y Generales", de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros, expedida por la Junta de Política y Regulación Monetaria y Financiera, incluir los siguientes artículos:

Art. 11.- Aceptar la renuncia presentada por la economista Verónica Artola Jarrín al cargo de Gerente General del Banco Central del Ecuador y agradecerle por los servicios prestados.

Art. 12.- Nombrar Gerente General del Banco Central del Ecuador al economista Guillermo Enrique Avellán Solines.

DISPOSICIÓN FINAL.- Esta resolución entrará en vigencia a partir de la presente fecha, sin perjuicio de su publicación en el Registro Oficial.

COMUNÍQUESE.- Dada en el Distrito Metropolitano de Quito, el 9 de junio de 2021.

EL PRESIDENTE,

Dr. Simón Cueva Armijos

Proveyó y firmó la resolución que antecede el doctor Simón Cueva Armijos, Ministro de Economía y Finanzas - Presidente de la Junta de Política y Regulación Monetaria y Financiera, en el Distrito Metropolitano de Quito, el 9 de junio de 2021.- **LO CERTIFICO.**

SECRETARIO ADMINISTRATIVO, ENCARGADO

Ab. Ricardo Mateus Vásquez

SECRETARÍA ADMINISTRATIVA
JUNTA DE POLÍTICA Y REGULACIÓN MONETARIA Y FINANCIERA
Quito, 11 JUN 2021
Es copia del documento que reposa en los archivos de la Junta.
LO CERTIFICO:
Ab. Ricardo Mateus Vásquez

Superintendencia de Control del Poder de Mercado

RESOLUCIÓN No. SCPM-DS-2021-17

Danilo Sylva Pazmiño
SUPERINTENDENTE DE CONTROL DEL PODER DE MERCADO

CONSIDERANDO:

Que el artículo 82 de la Constitución de la República del Ecuador, señala: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes"*;

Que el número 6 del artículo 132 de la Constitución de la República del Ecuador determina que se requerirá de Ley para: "O*torgar a los organismos públicos de control y regulación la facultad de expedir normas de carácter general en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales.*";

Que el artículo 213 de la Constitución de la República del Ecuador, dispone: "*Las superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general. Las superintendencias actuarán de oficio o por requerimiento ciudadano. Las facultades específicas de las superintendencias y las áreas que requieran del control, auditoría y vigilancia de cada una de ellas se determinarán de acuerdo con la ley.* (…)";

Que en el artículo 226 de la Constitución de la República del Ecuador, establece: "*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 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 del Ecuador, señala que: "*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 la Superintendencia de Control del Poder de Mercado fue creada mediante la Ley Orgánica de Regulación y Control del Poder de Mercado, publicada en el Registro Oficial Suplemento No. 555 de 13 octubre de 2011, como un órgano técnico de control, con capacidad sancionatoria, de administración desconcentrada, con personalidad jurídica, patrimonio propio y autonomía administrativa, presupuestaria y organizativa;

Que el 06 de noviembre de 2018, la Asamblea Nacional de conformidad con lo dispuesto en la Constitución de la República del Ecuador y de acuerdo a la Resolución del Consejo de Participación Ciudadana y Control Social No. PLE-CPCCS-T-O-163-23-10-2018 de 23 de octubre de 2018, según fe de erratas, de 05 de noviembre de 2018, posesionó al doctor Danilo Sylva Pazmiño como Superintendente de Control del Poder de Mercado;

Que la Ley Orgánica de Regulación y Control del Poder del Mercado, en su artículo 31, señala: *"La Superintendencia de Control del Poder de Mercado examinará permanentemente las ayudas públicas conferidas en virtud de las disposiciones de este capítulo, y evaluará que cumplan con los fines que motivaron su implementación.* (…) *Si la Superintendencia comprobare que una ayuda otorgada por el Estado o mediante recursos públicos no cumple con el fin para el cual se otorgó, o se aplica de manera abusiva o es contraria al objeto de esta Ley, mediante informe motivado, instará y promoverá su supresión o modificación dentro del plazo que determine."*;

Que el artículo 32 de la Ley Orgánica de Regulación y Control del Poder del Mercado, estipula: *"*(…) *La Superintendencia de Control del Poder de Mercado examinará permanentemente los efectos de las políticas de precios autorizada bajo este artículo. De determinar que se ha aplicado de manera abusiva o que el efecto es pernicioso en términos agregados, procederá inmediatamente de conformidad con el inciso segundo del artículo 31 de esta Ley."*;

Que el artículo 37 de la Ley Orgánica de Regulación y Control del Poder de Mercado, establece: *"Corresponde a la Superintendencia de Control del Poder de Mercado asegurar la transparencia y eficacia en los mercados y fomentar la competencia; la prevención, investigación, conocimiento, corrección, sanción y eliminación del abuso de poder de mercado, de los acuerdos y prácticas restrictivas, de las conductas desleales contrarias al régimen previsto en esta Ley; y el control, la autorización, y de ser el caso la sanción de las concentraciones económicas."*;

Que la Ley Orgánica de Regulación y Control del Poder del Mercado, en su artículo 38 dentro de las atribuciones de la Superintendencia de Control del Poder de Mercado, señala: *"*(…) *9. Cuando lo considere pertinente, emitir opinión en materia de competencia respecto de leyes, reglamentos, circulares y actos administrativos, sin que tales opiniones tengan efecto vinculante.* (…) *13. Requerir a las instituciones públicas que considere necesario, la implementación de acciones adecuadas para garantizar la plena y efectiva aplicación de la presente Ley.* (…) *21. Promover medidas de control tendientes a la eliminación de barreras a la libre concurrencia al mercado, de acuerdo con los lineamientos fijados por la ley.* (…) *24. Proponer la remoción de barreras, normativas o de hecho, de entrada a mercados, que excluyan o limiten la participación de operadores económicos.* (…) *28. Promover el estudio y la investigación en materia de competencia y su divulgación* (…)*"*;

Que el artículo 44 de la Ley Orgánica de Regulación y Control del Poder de Mercado, determina como atribuciones y deberes del Superintendente: *"*(…) *6. Elaborar y aprobar la normativa técnica general e instrucciones particulares en el ámbito de esta Ley*. (…) *16. Expedir resoluciones de carácter general, guías y normas internas para su correcto funcionamiento.* (…)*"*;

Que la Ley Orgánica de Regulación y Control del Poder del Mercado, establece en sus artículos 48, 49 y 50, la facultad que tiene la Superintendencia de Control del Poder de Mercado para solicitar informes, documentación e información a cualquier operador económico o institución u órgano del sector público o privado;

Que mediante Resolución No. SCPM-DS-012-2017 de 16 de marzo de 2017, el Superintendente de Control del Poder de Mercado, expidió el "Instructivo de Gestión Procesal Administrativa de la Superintendencia de Control del Poder de Mercado";

Que mediante Resoluciones números SCPM-DS-2019-64 de 03 de diciembre de 2019, SCPM-DS-2020-018 de 20 de abril de 2020, SCPM-DS-2020-020 de 04 de mayo de 2020, SCPM-DS-2020-026

de 03 de julio de 2020, y SCPM-DS-2021-01 de 04 de enero de 2021, se reformó parcialmente el Instructivo de Gestión Procesal Administrativa de la Superintendencia de Control del Poder de Mercado;

Que mediante memorando SCPM-IGT-INAC-2021-068 de 07 de mayo de 2021, el Intendente Nacional de Abogacía de la Competencia (E), solicitó a la Intendenta Nacional Jurídica: *"*(…) *considere y trabaje sobre la propuesta de reforma normativa al Instructivo de Gestión Procesal Administrativa de la Superintendencia de Control del Poder de Mercado* (…)*"*, para lo cual adjuntó el respectivo Formulario para solicitud de elaboración de normativa así como el borrador de proyecto de resolución; y;

Que es necesario realizar la reforma al Instructivo de Gestión Procesal Administrativa de la Superintendencia de Control del Poder de Mercado para establecer el procedimiento a seguir para la emisión de los informes de opinión y de exhortos en materia de competencia que tiene a cargo la Dirección Nacional de Promoción de la Competencia, con la finalidad de contar con procedimientos claros y eficientes.

En ejercicio de las atribuciones que le confiere la Ley,

RESUELVE:

REFORMAR PARCIALMENTE EL INSTRUCTIVO DE GESTIÓN PROCESAL ADMINISTRATIVA DE LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO

Artículo 1.- Incluir dentro del "Capítulo IV" correspondiente a la "Gestión Procesal en la Intendencia de Abogacía de la Competencia" a continuación del artículo 43 una "Segunda Sección" denominada: "Realización de informes de opinión y de exhortos en materia de competencia".

Artículo 2.- Sustituir el texto del artículo 44 por el siguiente:

"**Art. 44.- Realización de informes de opinión y de exhortos en materia de competencia.-** La Intendencia Nacional de Abogacía de la Competencia, en cumplimiento de sus atribuciones, podrá elaborar informes de opinión en materia de competencia. Para el efecto, procederá de la siguiente forma:

a. La Intendencia Nacional de Abogacía de la Competencia aperturará un expediente y solicitará la información necesaria a las instituciones competentes y operadores económicos involucrados.

b. Los informes de opinión en materia de competencia serán emitidos en el término de sesenta (60) días contados desde la disposición de apertura del expediente en el módulo ANKU, término que podrá ser prorrogado excepcionalmente hasta por quince (15) días término adicionales. Las prórrogas contenidas en la presente letra, serán adoptadas de acuerdo al criterio del Intendente Nacional de Abogacía de la Competencia y serán comunicadas a la Intendencia General Técnica en el término de tres (3) días contados a partir desde su adopción.

c. De necesitarse prórrogas adicionales a los tiempos establecidos en la letra anterior, estas serán únicamente autorizadas por el Intendente General Técnico, para el efecto, el Intendente Nacional

de Abogacía de la Competencia acompañará a la solicitud de prórroga las justificaciones correspondientes.

d. La Intendencia Nacional de Abogacía de la Competencia emitirá dicho informe a la Intendencia General Técnica; quien enviará al Superintendente para su análisis y aprobación.

e. Con la aprobación del Superintendente se procederá a publicar la opinión en materia de competencia, según sea el caso.

Para el caso de exhortos en materia de competencia, el Superintendente o el Intendente General Técnico podrán disponer de forma directa a la Intendencia Nacional de Abogacía de la Competencia, las condiciones y tiempos para la elaboración y emisión del exhorto respectivo".

Artículo 3.- Sustituir el texto del artículo 56 por el siguiente:

"**Art. 56.- Procedimiento para el requerimiento de información.-** Cuando se solicite información, dentro de los procedimientos investigativos, estudios o investigaciones de mercado, evaluación de ayudas públicas y de políticas de precios, análisis de barreras normativas, informes de opinión de competencia, o exhortos en materia de competencia, conforme los artículos 31, 32, 38 numerales 1, 9, 13, 21, 24 y 28; 48, 49 y 50 de la LORCPM, el Intendente correspondiente dispondrá al operador económico que entregue la información, para lo cual le concederá un término de hasta treinta (30) días para el cumplimiento de la entrega de información, el cual podrá prorrogarse, de oficio o a petición de parte, y por una sola vez hasta por el término de veinte (20) días.

Si los operadores económicos no remitieren la información solicitada en el término dispuesto, la Intendencia correspondiente realizará una insistencia, previniéndole al operador económico que en caso de incumplimiento se le impondrá la sanción prevista en el penúltimo inciso del artículo 79 de la LORCPM".

Artículo 4.- Sustituir el nombre de la "Segunda Sección" del "Capítulo XIII" correspondiente a "De las Ayudas Públicas" por la denominación: "De las Ayudas Públicas y Políticas de Precios";

Artículo 5.- Sustituir el texto del artículo 80 por el siguiente:

"**Art. 80.- De las ayudas públicas y políticas de precios.-** La Superintendencia de Control del Poder de Mercado a través de la Intendencia Nacional de Abogacía de la Competencia, conforme a la LORCPM, tiene la facultad de monitorear y evaluar las ayudas públicas, y de examinar permanentemente los efectos de las políticas de precios autorizadas.

En virtud del artículo 29 de la LORCPM, las ayudas públicas se podrán otorgar por el Estado mediante la utilización de recursos públicos, por el tiempo que fuere necesario por razones de interés social o público, o en beneficio de los consumidores.

De acuerdo con el artículo 32 de la LORCPM, la definición de políticas de precios corresponde a la Función Ejecutiva, de modo excepcional y temporal, para beneficio del consumo popular, así como para la protección de la producción nacional y la sostenibilidad de la misma".

Artículo 6.- Sustituir el texto del artículo 81 por el siguiente:

"**Art. 81.- Notificaciones de ayudas públicas y examen permanente de políticas de precios.-** Por disposición del artículo 30 de la LORCPM, es obligatoria la notificación de ayudas públicas detalladas en el artículo 29 ibídem a la SCPM, para efectos de control y evaluación, a más tardar después de quince (15) días de haber sido otorgadas o establecidas.

Sin perjuicio de lo previsto en el inciso anterior, en el caso que no se notifique una ayuda pública, la SCPM de oficio a través de la Intendencia Nacional de Abogacía de la Competencia (INAC), podrá requerir información a la entidad del Estado, responsable del otorgamiento de la ayuda pública para su posterior evaluación.

En el caso de evaluación de las políticas de precios, con base en el artículo 32 de la LORCPM, la SCPM realizará el examen permanentemente de los efectos de las políticas de precios autorizadas. Por su parte, conforme al artículo 40 del RLORCPM, la SCPM a través de la INAC podrá solicitar a la Función Ejecutiva toda la información que estime necesaria, la que será entregada en un plazo no mayor a treinta (30) días contados a partir de la fecha de presentación de la solicitud".

Artículo 7.- Sustituir el texto del artículo 82 por el siguiente:

"**Art. 82.- Procedimiento para evaluación de ayudas públicas y políticas de precios.-** Recibida la notificación de las entidades del Estado acerca del establecimiento de ayudas públicas, o para la realización del examen permanente de políticas de precios, la Intendencia Nacional de Abogacía de la Competencia procederá de la siguiente forma:

1. En el término de cuarenta y cinco (45) días, realizará un informe preliminar de los posibles impactos en el mercado o sector de aplicación de las ayudas públicas o de la definición de la política de precios, en el que consten todos los elementos técnicos y legales de verificación así como los resultados óptimos previstos o esperados. Para el efecto la Intendencia Nacional de Abogacía de la Competencia aperturará un expediente y solicitará la información necesaria a las instituciones competentes y operadores económicos involucrados. La Intendencia Nacional de Abogacía de la Competencia emitirá dicho informe a la Intendencia General Técnica, quien enviará al Superintendente para su análisis, a fin de que pueda instar a la entidad del Estado responsable, suprima o modifique la ayuda pública o política de precios materia de evaluación;

2. La evaluación se realizará mediante una matriz de control y seguimiento; la cual deberá ser revisada y alimentada con los nuevos datos obtenidos de manera trimestral, tomando especial consideración el cumplimiento de los objetivos deseados en forma real y medible;

3. Transcurrido la mitad del plazo establecido para la vigencia de las ayudas públicas notificadas, o de las políticas de precios establecidas, la Intendencia Nacional de Abogacía de la Competencia en forma técnica y de acuerdo al monitoreo respectivo, emitirá un segundo informe de evaluación en el término máximo de cuarenta y cinco (45) días; el cual deberá verificar si las ayudas públicas notificadas o las políticas de precios han cumplido el fin para el cual se otorgaron, si están distorsionando el mercado, o actuando de manera contraria a la LORCPM;

4. La Intendencia Nacional de Abogacía de la Competencia entregará el segundo informe a la Intendencia General Técnica, quien después de analizarlo técnicamente, podrá solicitar se hagan correcciones o nuevos requerimientos;

5. La Intendencia General Técnica enviará el informe definitivo de evaluación al Superintendente para su conocimiento y de ser el caso, instará a la entidad del Estado responsable, suprima o modifique la ayuda pública o política de precios materia de la evaluación.

DISPOSICIÓN DEROGATORIA

Única.- Deróguese toda disposición de igual o menor jerarquía que se oponga a la presente Resolución.

DISPOSICIONES GENERALES

PRIMERA.- Encárguese la Intendencia Nacional Jurídica de la elaboración de la Codificación del Instructivo de Gestión Procesal Administrativa de la Superintendencia de Control del Poder de Mercado.

SEGUNDA.- Encárguese la Secretaría General de la publicación de la presente resolución en la intranet y en la página Web Institucional.

TERCERA.- Encárguese la Secretaría General de la difusión interna de esta Resolución y la realización de las gestiones correspondientes para su publicación en el Registro Oficial.

CUARTA.- La presente Resolución entrará en vigencia a partir de su publicación en el Registro Oficial.

CÚMPLASE Y PUBLÍQUESE.-

Dada en el Distrito Metropolitano de Quito, el 17 de mayo de 2021.

Firmado electrónicamente por:
DANILO IVANOB SYLVA PAZMINO

Danilo Sylva Pazmiño
SUPERINTENDENTE DE CONTROL DEL PODER DE MERCADO

Firmado electrónicamente por:
RUTH ELIZABETH LANDETA TOBAR

Firmado electrónicamente por:
RICARDO AUGUSTO FREIRE GRANJA

Firmado electrónicamente por:
DANIEL ESTEBAN GRANJA MATOVELLE

Firmado electrónicamente por:
JUAN RAUL GUAÑA

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ISABELA

GAD MUNICIPAL Isabela De gran porvenir.

LICENCIA FUNCIONAMIENTO ESTABLECIMIENTOS TURÍSTICOS CANTÓN ISABELA

EL CONCEJO MUNICIPAL DEL GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE ISABELA.

Considerando:

Que, el artículo 3 de la Constitución de la República del Ecuador establece como deber primordial del Estado planificar el desarrollo nacional, erradicar la pobreza, promover el desarrollo sustentable y la redistribución equitativa de los recursos y la riqueza para acceder al buen vivir;

Que, el artículo 85 de la Constitución de la República define a las políticas públicas como garantías constitucionales de los derechos, y por tanto es necesario establecer los roles que ejercen los distintos actores públicos, sociales y ciudadanos en el ámbito del proceso de formulación, ejecución, evaluación y control;

Que, de acuerdo a lo establecido en el artículo 238 de la Constitución de la República, los Gobiernos Autónomos Descentralizados Municipales gozan de autonomía plena para legislar y dictar ordenanzas;

Que, el artículo 240 de la Constitución de la República, indica que los Gobiernos Autónomos Descentralizados cantonales, tendrán facultades legislativas en el ámbito de sus competencias y jurisdicciones territoriales;

Que, de conformidad al Artículo 264, numeral 5 de la Constitución de la República, dentro de las atribuciones de los Gobiernos Autónomos Descentralizados Municipales es de su competencia crear, modificar o suprimir mediante ordenanzas, tasas y contribuciones especiales de mejoras;

Que, el artículo 54, del Código Orgánico de Organización Territorial, Autonomía y Descentralización COOTAD, señala que son funciones del gobierno autónomo descentralizado municipal las siguientes: g) Regular, controlar y promover el desarrollo de la actividad turística cantonal, en coordinación con los demás gobiernos autónomos descentralizados, promoviendo especialmente la creación y funcionamiento de organizaciones asociativas y empresas comunitarias de turismo;

Que, el Art. 57 literal c) del COOTAD, indica que al Concejo Municipal le corresponde Crear, modificar, exonerar o extinguir tasas y contribuciones especiales por los servicios que presta y obras que ejecute;

Que, de conformidad a los artículos 566 y 568 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, las municipalidades podrán aplicar tasas retributivas de servicios públicos;

Que, el artículo 1 de la Ley de Turismo establece "La presente Ley tiene por objeto determinar el marco legal que regirá para la promoción, el desarrollo y la regulación del Sector Turístico, las potestades del Estado, las obligaciones y derechos de los prestadores y usuarios";

Que, según el Art. 3 de la Ley de Turismo, son principios de la actividad turística, los siguientes:

a) La iniciativa privada como pilar fundamental del sector; con su contribución mediante la inversión directa, la generación de empleo y promoción nacional e internacional;
b) La participación de los gobiernos provincial y cantonal para impulsar y apoyar el desarrollo turístico, dentro del marco de la descentralización;
c) El fomento de la infraestructura nacional y el mejoramiento de los servicios públicos básicos para garantizar la adecuada satisfacción de los turistas;
d) La conservación permanente de los recursos naturales y culturales del país; y,
e) La iniciativa y participación comunitaria indígena, campesina, montubia o afro ecuatoriana, con su cultura y tradiciones preservando su identidad, protegiendo su ecosistema y participando en la prestación de servicios turísticos, en los términos previstos en esta Ley y sus reglamentos;

Que, el Estado Ecuatoriano, representado por el Ministerio de Turismo firmó el Convenio de Descentralización y de Transferencia de Competencias hacia el Gobierno Municipal de Isabela; el mismo que por lo señalado en la Disposición General Primera del COOTAD, se mantiene vigente, según la norma que se transcribe:

Primera. - Vigencia de los convenios de descentralización. -Los convenios de descentralización de competencias suscritos con anterioridad a este Código, entre el gobierno central y los gobiernos autónomos descentralizados, o que hayan entrado en vigencia por vencimiento de los plazos establecidos, mantendrán su vigencia, en el marco de la Constitución y este Código;

Estas competencias no podrán ser revertidas. Si existiere contradicción, el Consejo Nacional de Competencias emitirá resolución motivada que disponga los ajustes necesarios, previo acuerdo entre las partes involucradas, para el pleno ejercicio de las competencias descentralizadas, así como el ejercicio concurrente de la gestión en la prestación de servicios públicos y los mecanismos de gestión contemplados en el presente Código;

Que, existe el Convenio de Transferencia de Competencias celebrado entre el Ministerio de Turismo y el Gobierno Autónomo Descentralizado Municipal de Isabela, en donde se transfirieron varias responsabilidades en el ámbito turístico al GAD Municipal del cantón Isabela, entre ellos la concesión y renovación de la Licencia Única Anual de Funcionamiento de los Establecimientos Turísticos que previamente estén registrados en el Ministerio de Turismo y desarrollen su actividad dentro del Cantón Isabela;

Que, el turismo, en sí mismo, constituye una importante industria de interés comunitario y estimula el desarrollo de otros sectores productivos, tanto de bienes como de servicios;

Que, mediante Acuerdo No. 2006-0085 del Ministerio de Turismo, publicado en el Registro Oficial No. 396 de 14 de noviembre del 2006, se establece la Política Nacional de Descentralización Turística y Gestión Local del Turismo; y, se aprueba la matriz de competencias por niveles de gobierno, que contiene las atribuciones y funciones asignadas por niveles de gobierno. En esta matriz, en el Tipo/Atribución: REGULACION, REGISTRO, LICENCIA Y CONTROL, punto se establece como competencias de los Municipios: Conceder y renovar la Licencia Única Anual de Funcionamiento (LUAF); y Determinar y reglamentar el cobro de la LUAF;

Que, el Art. 60 del Reglamento General de aplicación de la Ley de Turismo, establece: "Pago de la licencia. - El valor que deberá pagarse es igual al valor que se paga por registro. En los municipios descentralizados el valor será fijado mediante la expedición de la ordenanza correspondiente";

En uso de las facultades y atribuciones que le concede la Constitución de la República del Ecuador y el Código Orgánico de Organización Territorial, Autonomía y Descentralización.

Expide:

LA ORDENANZA QUE ESTABLECE LA TASA PARA EL OTORGAMIENTO O RENOVACIÓN DE LA LICENCIA UNICA ANUAL DE FUNCIONAMIENTO (LUAF) PARA LAS ACTIVIDADES TURISTICAS EN EL CANTÓN ISABELA.

TITULO I
AMBITO DE APLICACIÓN

Art. 1.- AMBITO DE APLICACIÓN. - El ámbito de aplicación de la presente Ordenanza es cantonal, por tanto, regula todas las actividades turísticas y afines que se realizan en el cantón Isabela, mismas que para funcionar deben obtener la Licencia Única Anual de Funcionamiento.

Art. 2.- OBJETO. - El Objeto de la presente ordenanza es la regulación y fijación de la tasa, para la obtención o renovación de la Licencia Única Anual de Funcionamiento (LUAF) de los Establecimientos y negocios que desarrollan alguna actividad turística en el Cantón Isabela.

Art. 3.- AUTORIDAD DE CONTROL. - La Dirección de Desarrollo Social y Sostenible del Gobierno Autónomo Descentralizado Municipal de Isabela será la encargada de controlar las actividades turísticas que se desarrollen en el Cantón Isabela; y coordinará su administración, actividades, proyectos y programas con otras instituciones públicas y privadas del Cantón Isabela y la Provincia de Galápagos, para un adecuado cumplimiento de sus objetivos observando las leyes sobre la materia.

Art. 4.- AUTORIDAD ADMINISTRATIVA. - El Gobierno Autónomo Descentralizado Municipal de Isabela, es la autoridad administrativa, y por intermedio de la Dirección de Desarrollo Social y Sostenible Municipal, otorgará La Licencia Única Anual de Funcionamiento (LUAF) a los negocios que ejerzan actividades turísticas en el cantón Isabela, que estén registrados en el Ministerio de Turismo.

TITULO II
DEL REGISTRO

Art. 5.- DEL REGISTRO. - Toda persona natural o jurídica para ejercer las actividades turísticas previstas en la Ley de Turismo y sus reglamentos, deberá registrarse en el Ministerio de Turismo por una sola vez, donde se establecerá la clasificación y categoría que corresponda, y posteriormente obtendrá la Licencia Única Anual de Funcionamiento en el Gobierno Autónomo Descentralizado Municipal de Isabela, con anterioridad a la fecha de inicio de su actividad; sin la LUAF no podrá operar ningún negocio turístico. Los requisitos y los procedimientos para el registro están establecidos en el reglamento de alojamientos turísticos de la Provincia de Galápagos.

Art. 6.- CATASTRO TURISTICO. - El Gobierno Autónomo Descentralizado Municipal de Isabela a través de la Dirección de Desarrollo Social y Sostenible en base al Registro turístico otorgado por el Ministerio de Turismo, creará un catastro municipal de turismo para el control de los negocios turísticos que funcionen en el cantón y cumplan con la obtención de la LUAF. Las instituciones mantendrán este catastro actualizado cada año.

TITULO III
DE LAS ACTIVIDADES TURISTICAS

Art. 7.- DE LAS ACTIVIDADES TURISTICAS. - De conformidad al Art. 5 de la Ley de Turismo, se consideran actividades turísticas las desarrolladas por personas naturales o jurídicas que se dediquen a la prestación remunerada de modo habitual a una o más de las siguientes actividades:

a.- Alojamiento;
b.- Servicio de Alimentos y Bebidas;
c.-Transportación. - Cuando se dedica principalmente al turismo, inclusive el transporte aéreo, marítimo, fluvial, terrestre y el alquiler de vehículos para este propósito;
d.- Operación. - Cuando las agencias de viajes provean su propio transporte, esa actividad se considerará parte del agenciamiento;
e.- La de Intermediación. - Agencia de servicios turísticos y organizadoras de eventos congresos y convenciones; y,
f.- Casinos, Salas de Juego (bingo-mecánicos) Hipódromos y Parques de Atracciones estables.

TITULO IV
DE LA LICENCIA UNICA ANUAL DE FUNCIONAMIENTO

Art. 8.- DEFINICIÓN. - La Licencia Única Anual de Funcionamiento, constituye la autorización legal conferida por el Gobierno Autónomo Descentralizado Municipal de Isabela, sin la cual no se podrá ejercer la actividad turística dentro de su jurisdicción cantonal.

Art. 9.- BENEFICIOS DE LA LICENCIA UNICA ANUAL DE FUNCIONAMIENTO. - De conformidad al Art. 10 de la Ley de Turismo, los beneficios son los siguientes:
a. Acceder a los beneficios tributarios que contempla la Ley de Turismo y sus reglamentos;
b. Dar publicidad a su categoría;

c. Que la información o publicidad oficial se refiera a esa categoría cuando haga mención de ese empresario, instalación o establecimiento;
d. Que las anotaciones del Libro de Reclamaciones, autenticadas por un Notario puedan ser usadas por el empresario, como prueba a su favor a falta de otra; y,
e. No tener que sujetarse a la obtención de otro tipo de Licencias de Funcionamiento, salvo en el caso de las Licencias Ambientales, que por disposición de la ley de la materia deban ser solicitadas y emitidas.

Art. 10.- VIGENCIA DE LA LUAF. - La Licencia Única Anual de Funcionamiento tendrá validez de un año fiscal (01 de enero a 31 de diciembre de cada año), por lo tanto, deberá renovarse cada año.

Art. 11.- PLAZO Y CALCULO PARA EL PAGO DE LA LICENCIA UNICA ANUAL DE FUNCIONAMIENTO DE ESTABLECIMIENTOS NUEVOS. - Las personas naturales o jurídicas que inicien su nueva operación, tendrán el plazo de 30 días para el pago de la tasa por la obtención de la licencia única anual de funcionamiento. Luego de este periodo, a instancia de la Dirección de Desarrollo Social y Sostenible, la Comisaria Municipal procederá a clausurar las actividades y el local de quienes no hubieren obtenido la LUAF.
El cálculo de la tasa de la LUAF en establecimientos nuevos se realizará de acuerdo a la tabla vigente del año en curso.

Art. 12.- CALCULO DEL PAGO POR ACTIVIDADES INICIADAS CON POSTERIORIDAD A LOS TREINTA DÍAS DEL AÑO. - Cuando un establecimiento turístico no inicie sus operaciones dentro de los primeros 30 días del año, el pago por concepto de licencia anual de funcionamiento, se calculará por el valor equivalente a los meses que restaren del año calendario.

En caso de emergencias sanitarias y desastres naturales y que estas afecten económicamente y de manera directa a los establecimientos turísticos, se realizará un cálculo especial por los meses que estuvieron operativos.

Art. 13.- PLAZO PARA RENOVACIÓN DE LA LUAF. - El plazo para renovar y pagar la tasa de la LUAF es hasta el 30 de abril del año en curso es decir vence terminado el primer cuatrimestre del año fiscal, luego de lo cual se procederá al cobro aplicando el interés por mora establecido en el Código Tributario.

Art. 14.- USO DE DENOMINACIÓN. - Ningún establecimiento podrá usar denominación, razón social o nombre comercial y clasificación o categoría distintas a las que constan en el registro. El incumplimiento de esta disposición se sancionará según lo que está establecido en la Ley de Turismo.

Los establecimientos que no realizan actividades turísticas no pueden usar denominación, razón social, publicidad, promociones, o cualquier otro mecanismo que provoque confusión en el público respecto a los servicios que se ofrecen.

La Comisaría Municipal con el apoyo de la Policía Nacional, actuará de oficio para clausurar esos establecimientos hasta que superen las causas que motivaron su intervención, es decir retiren letreros, facturas, rótulos, publicidad y demás elementos materiales que configuren esta infracción.

Art. 15.- INDEPENDENCIA DE CADA LOCAL PERTENECIENTE A UN MISMO PRESTADOR DE SERVICIOS TURISTICOS. - La Licencia Única Anual de Funcionamiento se otorga por cada local o negocio existente para el desarrollo de la actividad turística que el propietario o representante legal que ejerza en el cantón Isabela, por lo tanto, cada local o negocio se considera independiente.

Art. 16.- SUJETO ACTIVO. - El sujeto activo de la tasa de la LUAF es el GAD Municipal de Isabela.

Art. 17.- SUJETOS PASIVOS. - Son sujetos pasivos de la tasa para la obtención de la LICENCIA UNICA ANUAL DE FUNCIONAMIENTO (LUAF), las personas naturales o jurídicas que realicen actividades turísticas en el cantón Isabela, previo a la obtención del Registro del Ministerio de Turismo.

Art.18.-REQUISITOS PARA LA OBTENCIÓN DE LA LICENCIA UNICA ANUAL DE FUNCIONAMIENTO (LUAF).- Para el otorgamiento de la Licencia Única Anual de Funcionamiento, el prestador de servicios turísticos presentará según su actividad la siguiente documentación:

a).- POR PRIMERA VEZ:
1. Solicitud dirigida al Alcalde o Alcaldesa del Cantón.
2. Copia de la cédula de ciudadanía a color del solicitante.
3. Copia del certificado de votación a color del solicitante.
4. Copia del carnet de residente permanente a color del solicitante.
5. Copia de la patente municipal vigente.
6. Copia del Registro Único de Contribuyente.
7. Copia del certificado de Registro de Turismo otorgado por el Ministerio de Turismo.
8. Copia del comprobante de pago del 1 x 1.000 del Ministerio de Turismo sobre el valor de los activos fijos, de conformidad con lo establecido por la Ley de Turismo y el reglamento general de aplicación de la misma.
9. Copia del comprobante de pago del 1.5 por mil a los activos totales al GAD Municipal de Isabela (obligados a llevar contabilidad).
10. Lista actualizada de precios de los servicios que se ofertan.
11. Certificado de no adeudar al GADMI.
12. Tasa de trámite Municipal.
13. Copia de certificado de pago de predio urbano o copia del contrato de arriendo del local.
14. Copia de Escritura Pública de Constitución de compañía, legalmente inscrita.
15. Copia del nombramiento del Representante legal.
16. Copia de la Matricula vigente de la embarcación otorgada por Capitanía de Puerto.
17. Copia del Permiso o Patente de Operación Turística de la embarcación, otorgada por el Parque Nacional Galápagos, vigente.
18. Certificado de Uso de Suelo, para funcionamiento.
19. Copia del comprobante de Pago realizado al GADMI por concepto de LUAF.
20. Copia de ficha o licencia ambiental aprobada por el PNG en el caso que corresponda.
21. Copia del Plan de gestión de riesgos/contingencia/ seguridad.

b). - PARA RENOVACIÓN DE LUAF:
1. Solicitud dirigida a la Dirección de Desarrollo Social y Sostenible del GADMI.
2. Copia de Documentos personales si se hubieran caducados.
3. Copia del Comprobante de pago del uno por mil del Ministerio de Turismo.
4. Lista actualizada de precios por los servicios que ofrecen.
5. Copia de la patente municipal vigente.
6. Certificado de no adeudar al GADMI.
7. Tasa de trámite municipal.
8. Copia del nombramiento del representante legal vigente (en caso de caducarse el nombramiento).
9. Copia de Matrícula vigente de la embarcación otorgada por Capitanía de Puerto (en caso de embarcaciones).
10. Copia del Permiso o Patente de Operación Turística de la embarcación, otorgada por el Parque Nacional Galápagos, vigente (en caso de embarcaciones).
11. Copia del comprobante de pago por concepto de LUAF.

Art. 19.- PROCEDIMIENTO PARA EL COBRO DE LA LUAF: Primero se verifica el tipo de establecimiento, categoría, y el valor que corresponde al año, de ese valor que corresponda al año se MULTIPLICA por las habitaciones, mesas o plazas, etc.

Art. 20.- VALORES DE RECAUDACIÓN POR CONCEPTO DE LICENCIA ÚNICA ANUAL DE FUNCIONAMIENTO. - Las personas naturales o jurídicas que desarrollen actividades turísticas remuneradas de manera habitual o temporal, deberán proceder con el pago de los mencionados valores de manera obligatoria.

1. ALOJAMIENTO. - Se deberá observar las siguientes tarifas para aquellos establecimientos que prestan los servicios de alojamiento turístico.

ACTIVIDAD TURÍSTICA: ALOJAMIENTO TURÍSTICO		
POR HABITACIÓN		
CLASIFICACIÓN	CATEGORÍA	% SBU
Hotel	5 estrellas	20,00%
	4 estrellas	16,00%
	3 estrellas	12,00%
Hostal	3 estrellas	5,00%
POR PLAZA		
CLASIFICACIÓN	CATEGORÍA	% SBU
Campamento turístico, Casa de Huéspedes	Única	5,00%
Lodge	5 estrellas	7,00%
	4 estrellas	6,00%

La Dirección de Desarrollo Social y Sostenible del Gobierno Autónomo Descentralizado Municipal de Isabela, deberá multiplicar el porcentaje (%SBU) por el monto del Salario Básico Unificado (SBU) de Galápagos de cada año y por el número de habitaciones y/o plazas con las que cuenta el establecimiento, según corresponda.

La clasificación y categoría de un establecimiento turístico estará determinado de acuerdo al Reglamento de Alojamiento Turístico para el Régimen Especial de la Provincia de Galápagos.

El valor correspondiente al porcentaje del SBU, se ajustará anualmente de conformidad al establecido por el Gobierno Central.

2. OPERACIÓN E INTERMEDIACIÓN TURÍSTICA. - Se deberá observar las siguientes tablas para aquellos establecimientos que prestan las actividades de operación e intermediación:

ACTIVIDAD TURÍSTICA: OPERACIÓN E INTERMEDIACIÓN	
AGENCIAS DE SERVICIOS TURÍSTICOS	POR ESTABLECIMIENTO (% SBU)
Dual	86%
Internacional	86%
Mayorista	100%
Operadoras	35%
OTROS ESTABLECIMIENTOS DE INTERMEDIACIÓN	POR ESTABLECIMIENTO (% SBU)
Centro de convenciones	50%
Organizadores de eventos, congresos y convenciones	35%
Salas de recepciones y banquetes	30%

La Dirección de Desarrollo Social y Sostenible del Gobierno Autónomo Descentralizado Municipal de Isabela, deberá multiplicar el porcentaje (%SBU) por el monto del Salario Básico Unificado (SBU) de Galápagos de cada año y por establecimiento.

El valor correspondiente al porcentaje del SBU, se ajustará anualmente de conformidad al establecido por el Gobierno Central.

3. ALIMENTOS Y BEBIDAS. - Se deberá observar las siguientes tablas para aquellos establecimientos que prestan la actividad turística de alimentos y bebidas:

			(% SBU)	
ALIMENTOS Y BEBIDAS	RESTAURANTES Y CAFETERIAS	Por mesas	LUJO	5,00%
			PRIMERA	3,50%
			SEGUNDA	2,20%
			TERCERA	2,00%
			CUARTA	2,00%
	BARES	Por mesa	PRIMERA	6,00%
			SEGUNDA	5,00%
			TERCERA	4,00%
	FUENTES DE SODA	Por plaza	PRIMERA	6,00%
			SEGUNDA	5,00%
			TERCERA	4,00%
	DISCOTECAS Y SALAS DE BAILE	Por plaza	LUJO	3,00%
			PRIMERA	2,00%
			SEGUNDA	1,50%
			TERCERA	1,00%
	PEÑAS Y KARAOKE	Por establecimiento	PRIMERA	45,00%
			SEGUNDA	40,00%

La Dirección de Desarrollo Social y Sostenible del Gobierno Autónomo Descentralizado Municipal de Isabela, deberá multiplicar el porcentaje (%SBU) por el monto del Salario Básico Unificado (SBU) de Galápagos de cada año y por el número de mesas, plazas o establecimiento.

El valor correspondiente al porcentaje del SBU, se ajustará anualmente de conformidad al establecido por el Gobierno Central.

4. TRANSPORTE TURíSTICO TERRESTRE Y AÉREO. - Se establece el máximo del cobro para transporte turístico terrestre y aéreo, para lo cual el Gobierno Autónomo Descentralizado no podrá establecer un valor mayor, lo que no exime que este establezca un valor menor.

En el caso de no contar con información oficial respecto a ventas, la clasificación estará determinada únicamente por el criterio de empleo.

		(% SBU)	
TRANSPORTE TERRESTRE	Por Vehículo	SERVICIO D ETRANSPORTE TERRESTRE TURISTICO	45%
		SERVICIO DE TRANSPORTE DE CARRETAS Y TRANSPORTE URBANO Y RURAL	30%
		ALQUILER DE TRICAR, CUADRONES, MOTOS, BICICLETAS Y AFINES	20%
TRANSPORTE AEREO	Por Plaza	TRANSPORTE AEREO Y AVIONETAS	40%
		TRANSPORTE AEREO EN AVIONES / JET	50%

La Dirección de Desarrollo Social y Sostenible del Gobierno Autónomo Descentralizado Municipal de Isabela, deberá multiplicar el porcentaje (%SBU) por el monto del Salario Básico Unificado (SBU) de Galápagos de cada año y por el número de vehículos o establecimiento, agencia, oficina o sucursal, según corresponda.

El valor correspondiente al porcentaje del SBU, se ajustará anualmente de conformidad al establecido por el Gobierno Central.

4.1 TRANSPORTE TURíSTICO MARíTIMO. - Para la actividad turística de transporte marítimo se utilizará la siguiente fórmula de cálculo:

		(% SBU)	
TRANSPORTE MARITIMO	Por Plaza	MOTONAVES	25%
		MOTOVELEROS	20%
		YATES DE PASAJEROS	18%
		LANCHAS DE PASAJEROS	7%
		LANCHAS DE TOUR DIARIO	15%
		TOUR DE BAHIA	5%
		PESCA VIVENCIAL	7,50%
		TOUR DIARIO DE BAHIA Y BUCEO	8%

La Dirección de Desarrollo Social y Sostenible del Gobierno Autónomo Descentralizado Municipal de Isabela, deberá multiplicar el porcentaje (%SBU) por el monto del Salario Básico Unificado (SBU) de Galápagos de cada año y por plaza.

El valor correspondiente al Salario Básico Unificado, se ajustará anualmente de conformidad al establecido por el Gobierno Central.

TITULO V
DE LAS OBLIGACIONES:

Art. 21.- Toda persona natural o jurídica dedicada a actividades turísticas deberá cumplir con las siguientes obligaciones específicas:

1. Facilitar al personal de la Dirección de Desarrollo Social y Sostenible y más funcionarios del Gobierno Autónomo Descentralizado Municipal de Isabela las inspecciones y comprobaciones que fueren necesarias, a efectos del cumplimiento de las disposiciones en esta ordenanza; y,
2. Proporcionar a la Dirección de Desarrollo Social y Sostenible del Gobierno Municipal de Isabela los datos estadísticos e información que les sean requeridos, especialmente sobre el ingreso de turistas a los alojamientos turísticos.
3. Exhibir en lugar visible del negocio turístico, la Licencia Única Anual de Funcionamiento y los servicios que brinda con sus respectivas tarifas.

TITULO VI

Art. 22.- DEL ARRENDAMIENTO O TRANSFERENCIA DEL ESTABLECIMIENTO TURISTICO. - En caso de arrendamiento o transferencia del establecimiento turístico, las partes están obligadas a comunicar a la autoridad de control, dentro de los treinta días siguientes de celebrado el contrato. De no darse cumplimiento a esta disposición, para fines tributarios se entenderá que el local continúa a nombre y responsabilidad de la persona natural o jurídica catastrada.

Art. 23.- CAMBIO DE ACTIVIDAD TURISTICA. - En caso de cambio de actividad turística, se deberán realizar los trámites como si se tratara de un nuevo establecimiento turístico (debe presentar los documentos antes mencionados en el art. 18 literal a.).

Art. 24.- DE LA TERMINACIÓN DE LA ACTIVIDAD TURISTICA. - En caso de dar por terminada la actividad turística, la persona natural o jurídica catastrada deberá notificar a la Dirección de Desarrollo Social y Sostenible y Jefatura de Rentas Municipales, previa cancelación de sus obligaciones a la Municipalidad y cumplir con los demás requisitos para la baja de establecimientos.
Los documentos a presentar son los siguientes:

- Solicitud dirigida a la directora/or de Turismo del GADMI.
- Copia del oficio del Ministerio de Turismo (en respuesta a la baja del establecimiento).

TITULO VII
DE LAS INSPECCIONES

Art. 25.- INSPECCIONES. - El Gobierno Autónomo Descentralizado Municipal de Isabela a través de la Dirección de Desarrollo Social y Sostenible Municipal, tiene la facultad para en cualquier momento y sin notificación previa, disponer inspecciones a los negocios turísticos a fin de verificar el cumplimiento de las condiciones y obligaciones que corresponden a la categoría o clasificación que se le otorgó.

Si de la inspección se comprobare el incumplimiento de las normas que regulan las actividades turísticas, se notificará a la persona natural o al representante legal, para que de manera inmediata efectúe los correctivos del caso. El incumplimiento de esta disposición se sancionará según lo establecido en la Ley de Turismo, en la presente Ordenanza y en las normas de procedimiento que fueren aplicables.

TITULO VIII
DE LAS SANCIONES Y SU PROCEDIMIENTO.
DE LAS SANCIONES

Art. 26.- PROCESO ADMINISTRATIVO.- Sin perjuicio de lo dispuesto en el artículo 10 de esta ordenanza, la Dirección de Desarrollo Social y Sostenible emitirá el informe a la Dirección Financiera sobre las personas naturales o jurídicas que adeuden por concepto de LUAF a la Municipalidad; la Comisaría Municipal será la encargada de sancionar con la clausura de actividades y el local de quienes hasta el 30 de abril del año en curso, no hayan procedido a obtener la Licencia Única Anual de Funcionamiento para el periodo respectivo.

Toda sanción de clausura se notificará por escrito al Ministerio de Turismo, Dirección del Parque Nacional Galápagos y Capitanía de Puerto para que procedan a suspender de acuerdo a sus competencias, las actividades del prestador de servicios.

Art. 27.- CLASES DE SANCIONES. - Las clases de sanciones de acuerdo a su grado de infracción se clasifican en:
- Amonestación escrita
- Multas
- Clausura del establecimiento turístico o suspensión del servicio turístico.

Art. 28.- AMONESTACIÓN ESCRITA. - Se sancionarán con una amonestación escrita las siguientes Faltas, consideradas faltas leves:
- El no exhibir la Licencia Única Anual de Funcionamiento en un lugar visible al público;
- No permitir el acceso al establecimiento a funcionarios municipales para inspecciones;
- El incumplimiento en la obtención de la LUAF después del plazo establecido en el art. 12 y art. 13 de esta ordenanza;
- No brindar información oportuna sobre estadísticas, capacitación, denuncias y otros que sean requeridos de acuerdo a los proyectos de la entidad municipal;
- No exhibir las tarifas de los servicios que brinda, en un lugar visible al público, por parte de los establecimientos turísticos señalados en esta Ordenanza.

Art. 29.- MULTAS. - Las multas se sancionarán aplicando lo establecido en la Ley de Turismo y su Reglamento y demás normativas vigentes, cuando incurriere en unas de las siguientes faltas, consideradas graves:

- Reincidir en una de las faltas leve establecidos en el artículo anterior;
- Que los establecimientos turísticos no cuenten con la Licencia Única Anual de Funcionamiento previo informe de la Comisaria Municipal;
- Incumplir con el horario de funcionamiento de los establecimientos turísticos del Cantón Isabela;
- Incumplimiento en los servicios inicialmente ofertados previo contrato con el establecimiento turístico, una vez que se ha comprobado el mismo;
- Por escándalos realizados en el interior del establecimiento o negocio turístico;
- Maltrato verbal a los funcionarios municipales, autoridades encargadas del Control y ejecución al momento de solicitar información del negocio turístico;
- Quejas o denuncias de los usuarios del servicio turístico previamente justificados o comprobados.

Art. 30.- CLAUSURA.- Se sancionará con la clausura ocho días por primera vez a los establecimientos turísticos y/o servicio turístico de las personas naturales o jurídicas cuando exista reincidencia en una o algunas de las faltas consideradas graves; sanción que será impuesta por la Comisaria Municipal y/o ejecutada a través de los niveles de apoyo.
Se sancionará con la clausura de quince días a los establecimientos turísticos y/o servicio turístico de las personas naturales o jurídicas, si reinciden en la misma falta es cierre definitivo.
El Comisario Municipal del GAD Municipal de Isabela ejercerá la potestad sancionadora, respetando las garantías del debido proceso contempladas en la Constitución de la República.

TITULO IX
DEL PROCEDIMIENTO

Art. 31.- PROCEDIMIENTO PARA LA AMONESTACIÓN ESCRITA. - La autoridad de control a través de sus funcionarios luego de realizar la inspección correspondiente y si verifica que el prestador de servicio turístico ha incurrido en una falta leve comunicará a la autoridad de ejecución para que proceda a la sanción pertinente misma que deberá estar debidamente motivada.

Art. 32.- PROCEDIMIENTO PARA IMPOSICIÓN DE MULTAS Y CLAUSURA O SUSPENSIÓN. - La autoridad de control comunicará a la autoridad de ejecución sobre las faltas graves cometidas por el prestador de servicios turísticos, sin perjuicio que la autoridad de ejecución actúe de oficio e inicie el procedimiento administrativo siguiendo las reglas del debido proceso, y comprobada la falta cometida procederá con la sanción que corresponda conforme a las normativas vigentes.

Art. 33.- INICIO AL PROCEDIMIENTO ADMINISTRATIVO.- Una vez que avoca conocimiento la autoridad de ejecución por cualquier forma iniciará el procedimiento administrativo sumarísimo para lo cual procederá a citar al prestador de servicio turístico en persona o por boleta a fin de que conteste y presente las pruebas que considere pertinentes sobre las faltas presuntamente cometidas en un término de dos días contados desde la última citación; con la contestación o en rebeldía, se expedirá la resolución en un término de dos días, misma que deberá ser debidamente motivada.

El Comisario Municipal, procederá a la clausura, mediante la aplicación de los respectivos sellos, los que no podrán ser retirados bajo ningún concepto, hasta que se cumpla la sanción impuesta.

Art. 34.- ROTURA DE SELLOS.- En el caso que se violenten o rompan los sellos de clausura se procederá a sancionar con dos remuneraciones básicas unificadas del trabajador en Galápagos sin perjuicio de las acciones penales a que hubiere lugar conforme lo determina el Código Orgánico Integral Penal.

Art. 35.- PAGO DE MULTAS. - El valor de las multas impuestas serán canceladas en la Tesorería Municipal previa la emisión del título correspondiente.

DISPOSICIONES GENERALES

Primera. - Para evitar la innecesaria acumulación de documentos, únicamente en caso de variar el contenido de la información solicitada en el artículo 18 de esta ordenanza, se exigirá la actualización respectiva, durante el proceso de renovación. Toda modificación de la información será notificada a la Dirección de Desarrollo Social y Sostenible del Gobierno Municipal de Isabela, la que será la encargada de llevar un registro actualizado de la información.

Segunda.- Las personas que ejerzan actividades turísticas en el cantón Isabela, deberán asistir al menos al 50% de las capacitaciones auspiciadas por la Dirección de Desarrollo Social y Sostenible del GADMI.

Tercera.- Todos los establecimientos y quienes presten servicios turísticos deberán obligatoriamente colocar en un lugar visible la lista de precios y su categorización y contar con un letrero visible en la parte exterior del establecimiento.

Cuarta. - Los sellos por clausura serán especies valoradas numeradas o su respectiva especie en caso de que no exista en stock.

Quinta. - Los establecimientos de alojamiento turístico no podrán desarrollar actividades de intermediación u operación turística directamente, solo a través de operadoras turísticas legalmente registradas, quedando habilitado únicamente el servicio de traslado del huésped desde el establecimiento a puertos o aeropuertos y viceversa.

Sexta. - La presente ordenanza tendrá una vigencia hasta el año 2025.

DISPOSICIONES TRANSITORIAS

Primera. - El Gobierno Autónomo Descentralizado Municipal de Isabela, actualizará anualmente el catastro turístico a través de la autoridad de control.

Segunda: La pandemia del COVID-19, ha afectado de manera significativa en el turismo de la provincia de Galápagos, especialmente del cantón Isabela, motivo por el cual se concede el descuento del 50% a todas las personas naturales o jurídicas que cancelen el pago de la LUAF hasta el término del mes de julio del 2021, caso contrario se procederá al respectivo cobro del 100% de conformidad a los valores establecidos en la presente ordenanza.

DISPOSICIÓN DEROGATORIA

Se deroga expresamente: La Ordenanza para el cobro de tasa por el otorgamiento de la licencia única anual de funcionamiento de los establecimientos y actividades turísticas, publicada en el Registro Oficial Edición Especial No. 524 del 04 de marzo del 2016; y, del Registro Oficial No. 728 del 07 de abril de 2016.

Todas las Resoluciones, reformatoria para el cobro de tasa por el otorgamiento de la Licencia Única Anual de Funcionamiento de los establecimientos y actividades turísticas del cantón Isabela, provincia de Galápagos.

Se deroga toda otra norma de igual o menor jerarquía que se oponga a la presente ordenanza.

DISPOSICIÓN FINAL

En todo aquello que no estuviere previsto en la presente Ordenanza se estará a lo dispuesto en la Ley de Turismo, su Reglamento, Reglamento de Alojamientos turísticos para la provincia de Galápagos, sus anexos, La Ley Orgánica de Defensa del Consumidor y sus Reglamentos, así como al Código de Ética para el Turismo, en lo que fuere aplicable.

La presente ordenanza regirá a partir de su aprobación sin perjuicio de su publicación en el Registro Oficial.

Dada y firmada en la sala de sesiones del Concejo Municipal del Gobierno Autónomo Descentralizado Municipal de Isabela a los 28 días del mes de abril de 2021.

Lic. Leonardo Bolívar Tupiza Gil, Alcalde del Cantón Isabela.

Abg. Gisella Rodríguez Suárez, Secretaria del Concejo Municipal.

CERTIFICACIÓN DE DISCUSIÓN

La infrascrita Secretaria del Concejo Municipal de Isabela, CERTIFICA que la presente ORDENANZA QUE ESTABLECE LA TASA PARA EL OTORGAMIENTO O RENOVACIÓN DE LA LICENCIA ÚNICA ANUAL DE FUNCIONAMIENTO (LUAF) PARA LAS ACTIVIDADES TURÍSTICAS EN EL CANTÓN ISABELA, fue conocida, discutida y aprobada en dos debates, el primer debate en sesión ordinaria del día miércoles 31 de marzo del 2021; y, en segundo debate en sesión ordinaria del día miércoles 28 de abril del 2021. Puerto Villamil, miércoles 28 de abril del 2021.- LO CERTIFICO.

GOBIERNO AUTÓNOMO
DESCENTRALIZADO
MUNICIPAL DE ISABELA

Abg. Gisella Rodríguez Suárez, Secretaria del Concejo Municipal.

SECRETARÍA DE CONCEJO MUNICIPAL DE ISABELA. - Que en cumplimiento de lo dispuesto en el cuarto inciso del Art. 322 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, remito al Lcdo. Leonardo Bolívar Tupiza Gil, Alcalde del Cantón Isabela, la "ORDENANZA QUE ESTABLECE LA TASA PARA EL OTORGAMIENTO O RENOVACIÓN DE LA LICENCIA ÚNICA ANUAL DE FUNCIONAMIENTO (LUAF) PARA LAS ACTIVIDADES TURÍSTICAS EN EL CANTÓN ISABELA", para su sanción y promulgación. Puerto Villamil, miércoles 28 de abril del 2021.

Abg. Gisella Rodríguez Suárez, Secretaria del Concejo Municipal.

ALCALDÍA DEL GAD MUNICIPAL DE ISABELA.- Lcdo. Leonardo Bolívar Tupiza Gil, Alcalde del Gobierno Autónomo Descentralizado Municipal de Isabela, en ejercicio de la atribución conferida en el inciso cuarto del Art. 322 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, por cuanto la "ORDENANZA QUE ESTABLECE LA TASA PARA EL OTORGAMIENTO O RENOVACIÓN DE LA LICENCIA ÚNICA ANUAL DE FUNCIONAMIENTO (LUAF) PARA LAS ACTIVIDADES TURÍSTICAS EN EL CANTÓN ISABELA", que antecede, ha sido aprobada por el Concejo Municipal, cumpliendo con las formalidades legales y se ajusta a la Constitución de la República y la ley sobre la materia, RESUELVO: sancionar y disponer su publicación en el Registro Oficial y ejecución.- Notifíquese y cúmplase.- Puerto Villamil, miércoles 28 de abril del 2021.

Lcdo. Leonardo Bolívar Tupiza Gil, Alcalde del Cantón Isabela.

RAZÓN DE SANCIÓN. - Abg. Gisella Rodríguez Suárez, Secretaria del Concejo Municipal, **CERTIFICO:** Que el Lcdo. Leonardo Bolívar Tupiza Gil, Alcalde del cantón Isabela, sancionó y firmó la ordenanza que antecede, el 28 de abril de 2021.

Puerto Villamil, 28 de abril del 2021.

Abg. Gisella Rodríguez Suárez, Secretaria del Concejo Municipal.

FE DE ERRATAS

- **En virtud de la publicación efectuada de la Ordenanza del Cantón Yaguachi: *"Sustitutiva a la Ordenanza de estímulos tributarios para atraer inversiones industriales privadas que favorezcan el desarrollo del cantón"*, efectuada en la Edición Especial del Registro Oficial Nº 1406 de 18 de diciembre de 2020, la cual consta incompleta, procedemos a publicarla nuevamente.**

LA DIRECCIÓN

Alcaldía San Jacinto de YAGUACHI
Juntos hacemos el cambio

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE "SAN JACINTO DE YAGUACHI" SECRETARÍA GENERAL

EL MUY ILUSTRE CONCEJO DEL CANTÓN SAN JACINTO DE YAGUACHI

CONSIDERANDO:

Que, la Constitución de la República del Ecuador, en su Art. 238, consagra la plena autonomía política, administrativa y financiera de los gobiernos autónomos descentralizados;

Que, el Art. 54, literal b) Código Orgánico de Organización Territorial, Autonomía y Descentralización "COOTAD" preceptúa que, dentro de las funciones del Gobierno Autónomo Descentralizado Municipal, le corresponde a éste el diseñar e implementar políticas de promoción y construcción de equidad e inclusión en su territorio, en el marco de sus competencias constitucionales y legales;

Que, con sujeción al Art. 57, literal b) del Código Orgánico de Organización Territorial, Autonomía y Descentralización "COOTAD", al Concejo Municipal le corresponde, dentro de sus atribuciones, regular, mediante ordenanza, la aplicación de los tributos previstos en la ley a su favor;

Que, al tenor del Art. 498 del Código Orgánico de Organización Territorial, Autonomía y Descentralización "COOTAD", los concejos cantonales, mediante ordenanza, pueden disminuir hasta en un cincuenta por ciento los valores que corresponda cancelar a los diferentes sujetos pasivos de los tributos establecidos en dicho código, por un plazo máximo de diez años, con la finalidad de estimular el desarrollo del turismo, la construcción, la industria, el comercio u otras actividades productivas, culturales, deportivas, de beneficencia, así como las que protegen y defienden el medio ambiente;

Que, en la Disposición Transitoria Vigésima Segunda del Código Orgánico de Organización Territorial, Autonomía y Descentralización, se establece que en el período actual de funciones, todos los órganos normativos de los gobiernos autónomos descentralizados deben actualizar y codificar las normas vigentes en cada circunscripción territorial;

Que, el Director Financiero Municipal ha propuesto un proyecto de ordenanza que sustituya a la vigente con el fin de poner a disposición de los inversionistas, estímulos tributarios que aliente la llegada de capitales y recursos nacionales o extranjeros, así como, la generación de empleo con mano de obra local.

Que, en el Suplemento del Registro Oficial No. 451 de fecha 04 de marzo del 2015, *se publicó la ordenanza de estímulos tributarios para atraer inversiones industriales privadas que favorezcan el desarrollo del cantón San Jacinto de Yaguachi.*

En ejercicio de la facultad legislativa que confiere la Constitución de la República del Ecuador en el artículo 240, en concordancia con lo establecido en los artículos 7 y 57 letra a) del Código Orgánico de Organización Territorial, Autonomía y Descentralización.

EXPIDE:

ORDENANZA SUSTITUTIVA A LA ORDENANZA DE ESTÍMULOS TRIBUTARIOS PARA ATRAER INVERSIONES INDUSTRIALES PRIVADAS QUE FAVOREZCAN EL DESARROLLO DELCANTÓN SAN JACINTO DE YAGUACHI.

Artículo 1.- El Gobierno Autónomo Descentralizado del cantón San Jacinto de Yaguachi con la finalidad de estimular el desarrollo de la industria y las que protejan y defiendan el medio ambiente, establece la reducción de los tributos municipales a las personas naturales o jurídicas, nacionales o extranjeras que se establezcan en el cantón San Jacinto de Yaguachi y realicen nuevas inversiones orientadas a construir inversiones industriales, polos de desarrollo, Zonas Especiales de Desarrollo Económico (ZEDE), Parques Industriales y Proyectos Multipropósitos en las actividades descritas a partir de la fecha de publicación de la presente ordenanza.

Artículo 2.- TRIBUTOS SUSCEPTIBLES DE REDUCCIÓN.- Los tributos a los cuales se aplicará la disminución, según corresponda, son los siguientes:

a) Hasta el 50% sobre el impuesto predial sobre la propiedad urbana y rural;
b) Hasta el 50% sobre el impuesto de matrículas y patentes;
c) Hasta el 50% sobre el impuesto de alcabalas;
d) Hasta el 50% sobre el impuesto del 1,5 por mil sobre activos totales;
e) Hasta el 50% de la tasa del permiso de construcción.
f) Hasta el 50% de la tasa de uso de suelo.

2.1.- Sobre el restante 50% de los tributos que no se aplica la reducción, el GAD Municipal del cantón San Jacinto de Yaguachi, podrá conceder convenios de pago con los contribuyentes que lo soliciten.

Artículo 3.- PLAZO DEL ESTÍMULO TRIBUTARIO.- El plazo para acogerse a los beneficios que otorga el estímulo tributario es de hasta diez años, improrrogables, contados a partir de la vigencia de esta ordenanza.

Artículo 4.- BENEFICIARIO DEL ESTÍMULO TRIBUTARIO.- Podrán gozar de los beneficios que se establecen en la presente ordenanza, todas aquellas personas naturales o jurídicas nacionales o extranjeras que realicen nuevas inversiones productivas y/o favorezcan el desarrollo de obras de infraestructura y/o el buen vivir del cantón San Jacinto de Yaguachi; así como aquellas que generen empleo utilizando mano de obra local, por cuantías que excedan los cien mil dólares de los Estados Unidos de América (USD$100.000), con el objetivo de fomentar el desarrollo de la industria, así como las que protejan y defiendan el medio ambiente:

Artículo 5.- DETERMINACIÓN DE LAS REDUCCIONES TRIBUTARIAS.- Las personas naturales o jurídicas que se acojan a la reducción tributaria determinadas en el artículo 2 de la presente ordenanza, accederán a la misma, por un porcentaje de hasta el cincuenta por ciento (50%) de los valores que les correspondiere a pagar, con sujeción a la ley y las ordenanzas municipales, y que será calculado, de conformidad con la siguiente tabla:

RELACIÓN AL MONTO DE LA INVERSIÓN: 40%

MONTO DE LA INVERSIÓN		ESTÍMULO
DESDE	HASTA	
$100.000,00	$399.999,99	12%
$400.000,00	$799.999,99	16%
$800.000,00	$1.199.999,99	24%
$1.200.000,00	$1.599.999,99	32%
$1.600.000,00	EN ADELANTE	40%

RELACIÓN A LOS EMPLEADOS LOCALES: 10%

EMPLEADOS CONTRATADOS		ESTÍMULO
DESDE	HASTA	
1%	10%	2%
11%	20%	4%
21%	30%	6%
31%	40%	8%
41%	EN ADELANTE	10%

NÚMERO DE AÑOS A REDUCIR

MONTO INVERSIÓN		AÑOS
DESDE	HASTA	
$100.000,00	$399.999,99	6
$400.000,00	$799.999,99	7
$800.000,00	$1.199.999,99	8
$1.200.000,00	$1.599.999,99	9
$1.600.000,00	EN ADELANTE	10

De igual manera, las personas naturales o jurídicas que se acojan a la reducción de la tasa municipal descritas en los literales e) y f) del artículo 2 de la presente ordenanza, accederán a la misma por un porcentaje de hasta el cincuenta por ciento (50%) de los valores que le

correspondiera paga, cuando los permisos de construcción y/o tasa de uso de suelo sean solicitados para las siguientes actividades:

a) Recuperación de propiedades de interés patrimonial en el cantón.
b) Proyectos inmobiliarios con fines turísticos, culturales y artísticos tales como museos, escuelas de arte, teatro, cines, plazas comerciales, o cualquier actividad comercial.
c) Proyectos inmobiliarios de construcción de parques logísticos, industriales, ZEDE, polos de desarrollo, terminales y/o puertos secos.

Artículo 6.- Aplicación de la Mesa Técnica.- Previo al ingreso de toda documentación requerida y a la concesión de una aprobación de proyecto de desarrollo del turismo, construcción, de industria, comercio u otras actividades productivas, culturales, educativas, deportivas, de beneficencia, así como las que protejan y defiendan el medio ambiente, se requerirá de una mesa técnica, integrada por las Direcciones Municipales de: Financiera, Planificación, Obras Públicas, Uso de Suelo y Ambiente ; así como, la Jefatura del Benemérito Cuerpo de Bomberos de San Jacinto de Yaguachi, un representante de la Unidad de Movilidad del cantón San Jacinto de Yaguachi; Uno de la Dirección de Gestión de Riesgo, si fuera el caso, y la Dirección de AAPP Y alcantarillado sanitario, para que en el plazo máximo de quince días emitan un único informe conjunto dentro de sus correspondientes competencias, respecto a la solicitud requerida.

Artículo 7.- EXENCIONES.- Quedan exentos del pago del impuesto de Alcabala los aportes de bienes raíces, que se efectúen para formar o aumentar el capital de sociedades industriales de capital solo en la parte que le corresponda a la sociedad, conforme lo dispone los literales g) y h) del artículo 534 Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD).

Artículo 8.- DEL TRÁMITE.- El trámite para ser beneficiario del estímulo tributario se dictará a través de resolución administrativa, debidamente suscrita por el Alcalde

Artículo 9.- EXIGIBILIDAD DE OTROS TRÁMITES.- El ser beneficiario de los incentivos tributarios, no exime de realizar los trámites de habilitación y demás requeridos por el Gobierno Autónomo Descentralizado del cantón San Jacinto de Yaguachi a través de otra normativa, así como de presentar en el departamento de Rentas la documentación que acredite su condición de beneficiario para obtener los beneficios tributarios municipales. Si estos trámites municipales no se completaren al cabo de tres (3) meses, la persona o empresa no podrá seguir obteniendo los beneficios municipales que le correspondan y estarán obligados a los pagos totales sin dilación alguna, más el pago de los intereses y multas que la norma tributaria establezca.

Artículo 10.- DE LA APLICACIÓN DE LAS REBAJAS.- De otorgarse la reducción tributaria, por parte del Ejecutivo, su aplicación le corresponderá a la Dirección Financiera.

Artículo 11.- CESE DE LA VIGENCIA DE LA ORDENANZA.- En caso de revocatoria, caducidad, derogatoria o, en general, cualquier forma de cese de la vigencia de esta ordenanza, los nuevos valores o alícuotas a regir no podrán exceder de la cuantía o porcentaje establecido en la presente ordenanza

Artículo 12.- SANCIÓN POR INCUMPLIMIENTO.- Cuando por cualquier medio el Gobierno Autónomo Descentralizado del cantón San Jacinto de Yaguachi determine el incumplimiento de los requisitos establecidos en la presente ordenanza, La Mesa Técnica, previo informe debidamente motivado, y a través de la Dirección Financiera informará del particular al Alcalde, el cual, luego de evacuar el procedimiento administrativo aplicable que asegure el debido proceso, resolverá sobre la caducidad de los beneficios consagrados en ella y otorgados a los correspondientes sujetos pasivos. En caso de definir la caducidad de los beneficios, dispondrá la reliquidación de los tributos correspondientes desde la fecha en que se produjo la violación o incumplimiento y exigirá el pago por el monto correspondiente a la reliquidación, más los intereses, de forma inmediata. En caso de incumplimiento en el pago correspondiente el Gobierno Autónomo Descentralizado del cantón San Jacinto de Yaguachi aplicará el procedimiento coactivo.

DISPOSICIONES TRANSITORIAS.

PRIMERA.- Las nuevas inversiones que con sujeción a la presente ordenanza, se llegaren a realizar en el cantón San Jacinto de Yaguachi, dentro del periodo comprendido entre su aprobación y posterior publicación en el Registro Oficial, podrán acogerse a las reducciones aquí previstas, y se harán efectivas cuando la ordenanza esté vigente.

SEGUNDA.- Velando por el desarrollo futuro del cantón, todo impuesto, que no haya sido considerado o que a la fecha no existiere, se incorporará posteriormente, una vez aprobado por la autoridades competentes, mediante ordenanza reformatoria.

DISPOSICION DEROGATORIA.

Derogase la *ordenanza de estímulos tributarios para atraer inversiones industriales privadas que favorezcan el desarrollo del cantón San Jacinto de Yaguachi*, publicada en el suplemento del Registro Oficial No. 451 de fecha 04 de marzo del 2015.

DISPOSICION FINAL

La presente ordenanza entrara en vigencia a partir de su promulgación, sin perjuicio de su publicación en la página web institucional y en el Registro Oficial.

Dado en San Jacinto de Yaguachi a los 25 días del mes de Noviembre del año 2020

Dr. Kleber Falcón Ortega.
ALCALDE DEL CANTÓN SAN JACINTO DE YAGUACHI

Ab. Manuel A. Decker Gómez.
SECRETARIO GENERAL MUNICIPAL

Alcaldía San Jacinto de YAGUACHI Juntos hacemos el cambio
Dr. Kleber Falcón Ortega ALCALDE
alcaldiadeyaguachi alcaldiadeyaguachi

San Jacinto de Yaguachi, 25 de Noviembre del 2020.

Secretaría General del Gobierno Autónomo Descentralizado Municipal del cantón San Jacinto de Yaguachi. CERTIFICA.- Que la presente *ordenanza sustitutiva a la ordenanza de estímulos tributarios para atraer inversiones industriales privadas que favorezcan el desarrollo del cantón San Jacinto de Yaguachi,* fue conocida, discutida y aprobada en las sesiones ordinarias del 20 y 25 de noviembre del 2020; de conformidad con el Art. 322 inciso Tercero del Código Orgánico de Organización Territorial, Autonomía y Descentralización – COOTAD.

Ab. Manuel Alberto Décker Gómez.
SECRETARIO GENERAL MUNICIPAL.

San Jacinto de Yaguachi, 26 de Noviembre de 2020.

Alcaldía del Gobierno Autónomo Descentralizado Municipal del cantón San Jacinto de Yaguachi.-Toda vez que la *ordenanza sustitutiva a la ordenanza de estímulos tributarios para atraer inversiones industriales privadas que favorezcan el desarrollo del cantón San Jacinto de Yaguachi,* ha sido conocida, discutida y aprobada por el concejo cantonal de San Jacinto de Yaguachi, en las sesiones ordinarias del 20 y 25 de Noviembre del 2020, habiendo cumplido con las disposiciones contempladas en el Código Orgánico de Organización Territorial, Autonomía y Descentralización - COOTAD, esta Alcaldía en uso de las facultades contenidas en el Art. 322, inciso cuarto de la mencionada ley **SANCIONA** en todas sus partes la *ordenanza sustitutiva a la ordenanza de estímulos tributarios para atraer inversiones industriales privadas que favorezcan el desarrollo del cantón San Jacinto de Yaguachi.*

DR. KLEBER FALCON ORTEGA.
ALCALDE DEL CANTÓN SAN JACINTO DE YAGUACHI.

San Jacinto de Yaguachi, 26 de Noviembre del 2020.

Dr. Kleber Falcón Ortega
ALCALDE

Secretaria General del Gobierno Autónomo Descentralizado Municipal de San Jacinto de Yaguachi.- Proveyó y firmó el Decreto que antecede el Dr. Kleber Falcón Ortega, Alcalde del cantón San Jacinto de Yaguachi, a los 26 días del mes de Noviembre del 2020.

Ab. Manuel Alberto Décker Gómez.
SECRETARIO GENERAL MUNICIPAL.

CERTIFICO
QUE LA PRESENTE COPIA
ES IGUAL A SU ORIGINAL

Ing. Hugo Del Pozo Barrezueta
DIRECTOR

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Telf.: 3941-800
Exts.: 3131 - 3134

www.registroficial.gob.ec

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"