Tercer Suplemento del Registro Oficial No.245 , 7 de Febrero 2023

Normativa: Vigente

Última Reforma: Quinto Suplemento del Registro Oficial 290, 22-V-2026

LEY ORGÁNICA PARA LA TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL

(Ley s/n)

EL PLENO

CONSIDERANDO

Que el artículo 3 de la Constitución de la República indica que son deberes primordiales del Estado la planificación del desarrollo nacional, la erradicación de la pobreza y la promoción del desarrollo sustentable;

Que el artículo 120, numeral 6, de la Constitución de la República, en concordancia con el artículo 9, numeral 6, de la Ley Orgánica de la Función Legislativa, dispone que es competencia de la Asamblea Nacional para "expedir, codificar, reformar y derogar las leyes, e interpretarlas con carácter generalmente obligatorio";

Que el artículo 140 de la Constitución de la República prescribe que el Presidente de la República podrá enviar a la Asamblea Nacional proyectos de ley calificados de urgencia en materia económica para su tramitación dentro de un plazo máximo de treinta días a partir de su recepción;

Que el numeral 11 del artículo 147 de la Constitución de la República le atribuye la facultad al Presidente de la República para participar con iniciativa legislativa en el proceso de formación de leyes;

Que el artículo 261 de la Constitución de la República determina, entre las competencias exclusivas del Estado Central, el desarrollo de la política económica, tributaria, aduanera, arancelaria, fiscal, monetaria, comercio exterior y endeudamiento; la planificación nacional; el espectro radioeléctrico y el régimen general de comunicaciones y telecomunicaciones, puertos y aeropuertos; los recursos energéticos, minerales, hidrocarburos, hídricos, biodiversidad y recursos forestales; las áreas naturales protegidasy los recursos naturales; el registro de personas, nacionalización de extranjeros y control migratorio;

Que los numerales 1 y 2 del artículo 276 de la Constitución de la República establecen que el régimen de desarrollo tiene como objetivos mejorar la calidad de vida y aumentar las

capacidades y potencialidades de la población;

Que los numerales 2, 5 y 6 del artículo 277 de la Constitución de la República prevén los deberes del Estado para la consecución del buen vivir, entre los que se encuentran el dirigir, planificar y regular el proceso de desarrollo; impulsar el desarrollo de las actividades económicas mediante un orden jurídico e instituciones políticas que las promuevan, fomenten y defiendan mediante el cumplimiento de la Constitución y la ley; así como promover e impulsar la ciencia, la tecnología, las artes, los conocimientos tradicionales y las actividades de la iniciativa creativa, comunitaria, asociativa, cooperativa y privada;

Que el artículo 283 de la Constitución de la República prescribe que el sistema económico propende una relación dinámica entre sociedad, Estado y mercado;

Que en el artículo 284 de la Constitución de la República, en sus numerales 6 y 7, indica que entre los objetivos de la política económica se encuentran los siguientes: "impulsar el pleno empleo y valorar todas las formas de trabajo, con respeto a los derechos laborales"; y, "mantener la estabilidad económica, entendida como el máximo nivel de producción y empleos sostenibles en el tiempo";

Que el artículo 301 de la Constitución de la República dispone que sólo el Presidente de la República, mediante ley sancionada por la Asamblea Nacional, podrá establecer, modificar, exonerar o extinguir impuestos; mientras que las tasas y contribuciones se crean y regulan por acto normativo de órgano competente, de conformidad con la ley;

Que el artículo 304 de la Constitución de la República señala que la política comercial tendrá como objetivos desarrollar mercados internos y fortalecer el aparato productivo, asícomo regular, promover y ejecutar las acciones correspondientes para impulsar la inserción estratégica del país en la economía mundial;

Que el artículo 317 de la Constitución de la República determina que los recursos naturales no renovables son de propiedad inalienable e imprescriptible del Estado;

Que el artículo 319 de la Constitución de la República reconoce diversas formas de organización de la producción en la economía, en tal virtud alentará la producción que satisfaga la demanda interna y garantice una activa participación del Ecuador en elcontexto internacional;

Que el artículo 320 de la Constitución de la República establece que la producción, en cualquiera de sus formas, se sujetará a principios y normas de calidad, sostenibilidad, productividad sistémica, valoración del trabajo, y eficiencia económica y social, gestionando que los procesos productivos sean participativos, transparentes y eficientes;

Que el artículo 321 de la Constitución de la República determina que el Estado reconoce y

garantiza el derecho a la propiedad en sus diversas formas;

Que el artículo 334 de la Constitución de la República establece que le corresponderá al Estado, entre otras cosas, desarrollar políticas de fomento a la producción nacional en todos los sectores;

Que el artículo 339 de la Constitución de la República determina que el Estado promoverá las inversiones nacionales y extranjeras;

Que el artículo 395 de la Constitución de la República determina que el Estado garantizará un modelo sustentable de desarrollo, ambientalmente equilibrado y respetuoso de la diversidad cultural, que conserve la biodiversidad y la capacidad de regeneración natural, y asegure la satisfacción de las necesidades de las generaciones presentes y futuras;

Que para promover y garantizar nuevas inversiones que generen empleo se debe promulgar incentivos tributarios que brinden estabilidad y desarrollo económico en todas las industrias;

Que la administración pública debe estar guiada por una real eficiencia y simplificación administrativa; que garantice el ejercicio de los derechos, sin retrasos y demoras innecesarias; que reduzca los costos y optimice los recursos públicos, así como el tiempo de todos los ciudadanos; cumpliendo con el mandato constitucional de una administración pública eficiente, eficaz, transparentes y de calidad;

Que se ha evidenciado la necesidad de simplificar los procesos operativos para las inversiones en activos financieros de no residentes fiscales en Ecuador a fin de incentivar el ingreso de nuevos capitales al mercado ecuatoriano;

Que es necesario actualizar la clasificación de los datos públicos para dar libertad de elección de servidores de almacenamiento a las entidades públicas y así poder mantener respaldos adecuados y con altos estándares de seguridad para evitar vulneraciones de seguridad informática;

Que el eje central de la política pública debe ser la libertad de los ciudadanos para generar prosperidad y riqueza para todos los miembros de la sociedad; y,

En ejercicio de la facultad conferida por la Constitución de la República y la Ley Orgánica del Función Legislativa, expide la siguiente:

LEY ORGÁNICA PARA LA TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL

Título Preliminar
OBJETO Y ÁMBITO

Art. 1.- Objetivos.- La presente Ley tiene por objetivos generales:

a. Promover la creación de oportunidades mediante la atracción y fomento de inversiones de la economía digital global;
b. Incentivar la creación de empleos de calidad;
c. Promover la eficiencia en los mercados, la construcción y la mejora regulatoria; y,
d. La simplificación y la adopción de medios y tecnologías digitales en la prestación de servicios públicos y gestión de todo tipo de trámites administrativos (ante cualquier nivel del gobierno), judiciales o privados; impulsando el uso y apropiación de las mismas en los sectores productivos, academia y sociedad, fortaleciendo la innovación, desarrollo e investigación para dicha adopción y enfocada en potenciar el desarrollo de la economía digital en el país.

Son objetivos específicos de esta Ley:

a. Promover la inversión e innovación mediante la modernización, actualización y simplificación de trámites, proceso y trabas regulatorias;
b. Establecer el marco regulatorio para el fomento de la transformación digital de las instituciones públicas, de las empresas privadas y de la sociedad; así como fortalecer el uso efectivo y eficiente de las plataformas, las tecnologías digitales, las redes y servicios digitales con el fin de atraer inversiones, impulsar la economía digital, la eficiencia y el bienestar social, desarrollando habilidades y competencias digitales necesarias para el empleo, educación, salud y productividad;
c. Fortalecer el ciberespacio ecuatoriano procurando garantizar la seguridad de la información personal de los ciudadanos; e,
d. Incentivar el uso y la optimización de los recursos necesarios para lograr la transformación digital.
e. (Agregado por el Art. 1 de la Ley s/n, R.O. 290-5S, 22-V-2026) Fortalecer la ciberseguridad nacional como condición habilitante de la transformación digital, garantizando la protección de servicios esenciales, infraestructura crítica digital, derechos fundamentales y confianza en el ecosistema digital.
f) (Agregado por el Art. 1 de la Ley s/n, R.O. 290-5S, 22-V-2026) Garantizar la neutralidad tecnológica en la adopción de marcos y soluciones de ciberseguridad y transformación digital, promoviendo la interoperabilidad, la innovación abierta y la adaptabilidad a los avances tecnológicos.

Art. 2.- Ejes de la Ley.- Son ejes de la presente Ley los siguientes:

a. Infraestructura digital: Conectividad y Servicios de Telecomunicaciones, Sistemas de Información;
b. Cultura e Inclusión Digital: Educación Digital, Salud Digital, Cultura Digital;
c. Economía Digital: Transformación Digital de estructura productiva, Comercio

Electrónico;
d. Tecnologías emergentes para el desarrollo sostenible: Fomento de nuevas tecnologías en las industrias, Fomento de nuevas tecnologías para el medio ambiente, Ciudades Inteligentes y Sostenibles;
e. Gobierno Digital: Simplificación de trámites, Participación ciudadana por medios electrónicos, Gobierno de TICs, Identidad Digital;
f. Interoperabilidad y tratamiento de datos: Servicios de Interoperabilidad, Datos personales, Datos abiertos; y,
g. Seguridad Digital y confianza: Seguridad de la información.
h. Ciberseguridad: (Agregado por el Art. 2 de la Ley s/n, R.O. 290-5S, 22-V-2026) Protección de servicios esenciales e infraestructura crítica digital, gestión de riesgos e incidentes, resiliencia del ecosistema digital y fortalecimiento de la confianza nacional en el entorno digital.

Libro I
DE LA TRANSFORMACIÓN DIGITAL

Título I
LA RECTORÍA EN TRANSFORMACIÓN DIGITAL

Art. 3.- Rectoría.- (Reformado por el Art. 3 de la Ley s/n, R.O. 290-5S, 22-V-2026) El ente rector en materia de Telecomunicaciones y de la Sociedad de la Información será la entidad rectora en transformación digital, gobierno digital y ciberseguridad, para lo cual ejercerá atribuciones y responsabilidades, así como emitirá las políticas, directrices, acuerdos, normativa y lineamientos necesarios para su implementación.

Con la finalidad de facilitar la realización de actividades conjuntas e intercambio de información entre los distintos niveles de gobierno y las diferentes Instituciones Públicas que cuenten con plataformas tecnológicas, éstas deberán permitir y participar en la interoperabilidad con otros sistemas informáticos del Estado, conforme las directrices y metodologías que determine el ente rector.

El ente rector podrá conformar comités temporales, temáticos o sectoriales, para identificar las necesidades y formular las soluciones de transformación, con alineación al Plan Nacional de Desarrollo. Esto se realizará en coordinación con la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), Instituciones Públicas, entidades privadas, todos los niveles de gobierno y sociedad civil.

Art. 4.- De la transformación digital.- La Transformación Digital constituye el proceso continuo de adopción multimodal de tecnologías digitales que cambian fundamentalmente la forma en que los servicios gubernamentales y del sector privado se idean, planifican, diseñan, implementan y operan, con el objeto de mejorar la eficiencia, seguridad, certeza, velocidad y calidad de los servicios, optimizando sus costos y

mejorando las condiciones de transparencia de los procesos y actuaciones del Estado en su interrelación con los ciudadanos.

Art. 5.- Definiciones.- Para efectos de la aplicación de la presente Ley, se tendrán en cuenta las siguientes definiciones:

a. Tecnologías Digitales.- Se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

b. Entorno Digital.- Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas.

c. Servicio Digital.- Es aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

d. Gobernanza Digital.- Es el conjunto de procesos, estructuras, herramientas y normas que nos permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la organización.

e. Arquitectura Digital.- Es el conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.

f. De la Identidad Digital.- La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales. Los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo.

g. Servicio esencial.- (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Función o actividad cuya interrupción o degradación comprometa gravemente la vida, la salud, la seguridad, el orden público o la estabilidad económica del país.

h) Infraestructura crítica digital.- (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-

2026) Conjunto de sistemas, redes, plataformas o servicios de tecnologías de la información y comunicaciones, que constituyen el soporte cibernético o tecnológico de las infraestructuras críticas nacionales, cuyo funcionamiento es indispensable para la provisión continua y segura de servicios esenciales o para la protección de la seguridad nacional, cuya afectación puede generar impactos significativos en la vida, salud, economía o el orden público.

i) Ciberespacio.- (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Entorno global compuesto por infraestructuras de tecnologías de la información, redes de comunicaciones, sistemas y dispositivos interconectados, así como la interacción de sus usuarios, en el cual se desarrollan actividades sociales, económicas, políticas y de seguridad.

j) Ciberataque.- (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Acción intencional realizada mediante medios digitales, dirigida contra sistemas, redes, servicios o infraestructuras, con el fin de alterar, degradar, inutilizar, destruir, obtener acceso no autorizado, manipular información o afectar la disponibilidad, integridad o confidencialidad de los activos digitales.

k) Activo digital o informático. - (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Todo recurso digital, tangible o intangible, incluidos datos, información, sistemas, aplicaciones o plataformas, que tenga valor para una persona, organización o institución y que requiera medidas de protección frente a incidentes de ciberseguridad.

l) Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT). - (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Instancia multidisciplinaria que tiene por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques en forma rápida y efectiva, conforme a políticas y procedimientos predefinidos, contribuyendo a mitigar sus efectos.

m) Incidente de ciberseguridad.- (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Evento que compromete o tiene la capacidad de comprometer la confidencialidad, integridad, disponibilidad, resiliencia o autenticidad de la información digital, los sistemas, redes o servicios, ya sea por acción maliciosa, error humano, fallo técnico o causa natural.

n) Resiliencia digital.- (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Capacidad de anticipar, resistir, adaptarse y recuperarse frente a incidentes de ciberseguridad, asegurando la continuidad de los servicios esenciales e infraestructura crítica digital, incluso en condiciones degradadas.

o) Riesgo de ciberseguridad.- (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Probabilidad de ocurrencia de un incidente de ciberseguridad y la magnitud de sus consecuencias, cuantificada en función de la probabilidad y del impacto sobre las

personas, las instituciones, la economía o la seguridad nacional.

p) Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital.- (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Instrumento técnico, público y dinámico expedido por el ente rector, que identifica y clasifica los servicios esenciales y la infraestructura crítica digital sujetos a esta ley, de conformidad con criterios objetivos de riesgo, interdependencia y continuidad operativa.

q) Prestador de servicios digitales (PSD). - (Agregado por el Art. 4 de la Ley s/n, R.O. 290-5S, 22-V-2026) Persona natural o jurídica que provea servicios de procesamiento, almacenamiento, transmisión, intermediación o seguridad de datos y sistemas por medios electrónicos o telemáticos, incluyendo servicios en la nube, centros de datos, pasarelas de pago y plataformas de intermediación.

Art. 6.- Del Gobierno Digital.- Es el uso estratégico de tecnologías digitales y datos en la Administración Pública, como parte integral de las estrategias de modernización de los gobiernos para crear valor público.

El ecosistema de gobierno digital se encuentra compuesto por actores del sector público, sector privado, todos los niveles de gobierno y sociedad civil en general, quienes apoyan en la implementación de iniciativas y creación de servicios digitales.

El Gobierno Digital se fundamenta en los pilares de la gobernanza de datos, interoperabilidad y seguridad digital.

La Administración Pública del Estado ecuatoriano estará determinada por una real y eficiente gobernanza digital entendiéndose por aquélla al conjunto de procesos, estructuras, herramientas y normas que permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la institucionalidad.

Art. 7.- Atribuciones del ente rector de transformación digital.- El ente rector de la transformación digital tendrá las siguientes atribuciones:

a. Solicitar al Ministerio encargado de las Finanzas Públicas la asignación del presupuesto suficiente y necesario para la efectiva implementación y aplicación de la presente Ley.
b. Emitir políticas públicas, lineamientos, metodologías, regulaciones para la transformación digital, gobierno digital y evaluar su cumplimiento por parte de las entidades del sector público.
c. Coordinar la elaboración periódica de la “Agenda Digital Integral del Ecuador” orientada a los diversos sectores del país y a todos los niveles de gobierno y controlar su ejecución.
d. Promover el uso y la apropiación de las tecnologías digitales y de la información y comunicación en las actividades de las empresas, de la sociedad civil y de la academia para alcanzar los objetivos del país en la adopción de la transformación digital en sus

procesos.
e. Aprobar los planes que, en función de lo dispuesto por el Reglamento a esta Ley, deban presentar los sujetos sometidos a su ámbito de aplicación, asociados a la "Agenda Digital Integral del Ecuador".
f. Dar seguimiento al cumplimiento de las metas planteadas en la Agenda Digital Integral del Ecuador.
g. Proponer y promover reformas a cuerpos normativos a fin de impulsar la transformación digital.
h. Estructurar programas de capacitación para todos los servidores del sector público, los actores del sector privado, así como la ciudadanía en general, con el fin de mejorar sus habilidades digitales.
i. Establecer, disponer y evaluar el cumplimiento de planes de digitalización y automatización de trámites y procesos administrativos de las entidades del sector público.
j. Identificar, disponer y evaluar los trámites, servicios y procesos administrativos de las entidades del sector público que obligatoriamente deberán ser digitalizados y automatizados.
k. Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales.
l. Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía digital.
m. Promover la colaboración entre las entidades de la Administración Pública, así como la participación de ciudadanos y otros interesados para el desarrollo del gobierno digital y sociedad del conocimiento.
n. Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales.
o. Emitir las directrices y establecer los parámetros en materia de la seguridad de la información y ciberseguridad, que las entidades deberán observar en el establecimiento y ejecución de sus planes de transformación digital y monitorearlos a través del Centro de Respuestas o Incidentes de seguridad Informática, que será puesto en marcha y operado por el ente rector de la transformación digital.

Art. 7-A.- Atribuciones del ente rector en ciberseguridad.- (Agregado por el Art. 5 de la Ley s/n, R.O. 290-5S, 22-V-2026) Corresponde al ente rector en materia de ciberseguridad, lo siguiente:

a) Elaborar, mantener y actualizar el Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital, con criterios objetivos y basados en riesgo, en coordinación con las autoridades competentes.

Este catálogo incluirá, al menos, los siguientes conceptos: energía en todas sus formas, telecomunicaciones, recursos naturales no renovables, transporte y refinación de

hidrocarburos, biodiversidad y patrimonio genético, espectro radioeléctrico, agua, saneamiento, energía eléctrica, vialidad, infraestructura portuaria y aeroportuaria, el sistema financiero y el crédito, la educación, la salud y la seguridad social.

El catálogo se mantendrá actualizado de manera permanente, debiendo revisarse al menos cada dos (2) años o cuando se produzcan cambios significativos en los riesgos, tecnologías o interdependencias sectoriales.

La incorporación de otros sectores o servicios se realizará mediante resolución motivada del ente rector.

b) Ejercer funciones de rectoría normativa, planificación y coordinación interinstitucional en materia de ciberseguridad, sin sustituir la fiscalización ni las potestades sancionadoras atribuidas por la Constitución y la ley a los órganos de control especializados. En los sectores no regulados por órganos especializados, el ente rector podrá disponer verificaciones técnicas con fines preventivos, sin perjuicio de los informes técnicos de carácter no vinculante que emita en procesos de coordinación interinstitucional.

c) Establecer lineamientos técnicos de carácter general para la gestión de incidentes digitales, promoviendo mecanismos de prevención, detección, respuesta y recuperación, en coordinación con el CSIRT Nacional y sin duplicar procedimientos definidos por órganos de control especializados en sus respectivos sectores.

d) Formular y actualizar la Política Nacional de Ciberseguridad, articulada con los planes nacionales de desarrollo, en coordinación con los sectores público, privado, académico y la sociedad civil.

e) Promover campañas de sensibilización, educación digital y programas de capacitación que fomenten la seguridad en el ciberespacio para todos los usuarios, con atención especial a grupos en situación de vulnerabilidad.

f) Establecer lineamientos técnicos para la actualización de los mecanismos criptográficos utilizados en el sector público y en los prestadores de servicios digitales, incorporando estándares internacionales seguros frente a riesgos derivados de tecnologías emergentes, incluyendo la computación cuántica, conforme al avance científico y a los procesos de estandarización internacional.

g) Las demás atribuciones necesarias para garantizar la seguridad y resiliencia del ecosistema digital, en el marco de la Constitución y la ley.

Art. 8.- Ambiente de pruebas regulatorio (Sandbox).- Es un mecanismo regulatorio provisional y de prueba, que no exime de las responsabilidades legales de quien accede al mecanismo provisional, que permita probar productos, servicios, soluciones,

implementación de tecnologías emergentes inclusive con espectro licenciado o no licenciado, nuevos marcos regulatorios, pruebas de competencia en el mercado, comportamientos del mercado ante la desregulación, nuevos modelos de negocios, entre otros, bajo un conjunto de exenciones técnicas, económicas, tributarias y regulatorias por un periodo de tiempo no superior a los 24 meses.

Con el fin de promover y atraer la inversión; así como mejorar la productividad en el país, el Ministerio rector de Industrias y Productividad emitirá lineamientos generales conforme las mejores prácticas internacionales dadas por organismos internacionales para esta figura, con el fin de que las autoridades competentes de regulación de cada sector emitan un marco regulatorio flexible, que determine dichas exenciones.

El Reglamento establecerá normas que regulen: los principios que rigen esta institución; requerimientos generales para la implementación y las medidas de protección al consumidor, el régimen de entrada y salida, parámetros para delimitar el alcance del marco regulatorio flexible y exenciones, parámetros para el otorgamiento y revocatoria de la autorización temporal de operación del producto o servicio en prueba, y, medidas mínimas que deberá tener en cuenta la autoridad sectorial competente al constituir el ambiente regulatorio de pruebas.

Art. 9.- Destino de residuos digitales.- Con la finalidad de realizar un manejo ecológicamente responsable, el ente rector deberá desarrollar la reglamentación adecuada para establecer que la importación sea de tecnología nueva y que el destino de los desechos tecnológicos que han cumplido su vida útil tenga un manejo adecuado que procure que nuestro país no se convierta en un botadero de este tipo de desechos.

Título II
DE LA IDENTIDAD DIGITAL

Art. 10.- Marco de Identidad Digital.- El Marco de Identidad Digital está constituido por lineamientos, especificaciones, guías, directivas, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la identificación y autenticación de los ciudadanos y personas en general cuando acceden a los servicios digitales.

Art. 11.- Credencial de Identidad Digital.- Es la representación de una identidad digital que comprende los atributos inherentes a la persona definidos en el Marco de Identidad Digital, a fin de facilitar la autenticación digital.

Art. 12.- Identificación Digital.- La identificación digital es el procedimiento de reconocimiento de una persona como distinta de otras en el entorno digital. Las entidades de la Administración Pública deben establecer los procedimientos para identificar a las personas que accedan a los servicios digitales.

Art. 13.- Autenticación Digital.- La autenticación digital es el procedimiento de verificación de la identidad digital de una persona, mediante el cual se puede afirmar que es quien dice ser. Para el acceso a un servicio digital las entidades de la Administración Pública deben adoptar los mecanismos o procedimientos de autenticación digital, considerando los niveles de seguridad a establecerse en la norma reglamentaria.

Art. 14.- Inclusión digital.- La inclusión digital es el acceso y uso de los servicios digitales por parte de los ciudadanos a través de su identidad digital, promoviendo la ciudadanía digital. Para tal fin las entidades de la Administración Pública adoptan las disposiciones que emite el ente rector para la prestación de dichos servicios.

Título III
DE LA PRESTACIÓN DE SERVICIOS DIGITALES

Art. 15.- Garantías para la prestación de servicios digitales.- Las entidades de la Administración Pública, de manera progresiva y cuando corresponda, deben garantizar a las personas el establecimiento y la prestación de los servicios digitales, comprendidos en el ámbito de aplicación de la presente Ley, debiendo para tal efecto:

1. Reconocer y aceptar el uso de la identidad digital de todas las personas según lo regulado en la presente Ley.
2. Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia.
3. Capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y gobierno digital.
4. Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que se encuentren en soporte electrónico, únicamente para el ejercicio de sus funciones en el ámbito de sus competencias. Queda excluida del intercambio la información que pueda afectar la seguridad nacional, la información personal o la prohibida por la Ley de Transparencia y Acceso a la Información Pública.
5. Implementar servicios digitales haciendo un análisis de la arquitectura digital y rediseño funcional.
6. Facilitar a las personas información detallada, concisa y entendible sobre las condiciones de tratamiento de sus datos personales.
7. Garantizar la conservación de las comunicaciones y documentos generados a través de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales.
8. Garantizar que en el diseño y configuración de los servicios digitales se adoptan las

medidas técnicas, organizativas y legales para la debida protección de datos personales y la confidencialidad de las comunicaciones.

Art. 16.- Domicilio Digital.- Es uno de los atributos de la identidad digital que se constituye en el domicilio habitual de un ciudadano en el entorno digital, el cual es utilizado por las entidades de la Administración Pública para efectuar comunicaciones o notificaciones.

Título IV
DE LA SEGURIDAD DIGITAL

Art. 17.- De la Seguridad Digital.- La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

Art. 18.- Marco de Seguridad Digital.- El Marco de Seguridad Digital se constituyen en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

Art. 19.- Gestión del Marco de Seguridad Digital.- El Marco de Seguridad Digital del Estado se tienen que observar y cumplir con lo siguiente:

a. Defensa: El Ministerio de Defensa en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa.

b. Inteligencia: El Centro de Inteligencia Estratégica o la entidad que haga sus veces, como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.

c. Justicia: El Ministerio de la Mujer y Derechos Humanos, el Ministerio del Interior, la Policía Nacional, la Fiscalía General del Estado y la Corte Nacional de Justicia, en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. Institucional: Las entidades de la Administración Pública deberán establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información.

Art. 20.- Articulación de la Seguridad Digital con la Seguridad de la Información.- El Marco de Seguridad Digital se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

Título (...)
DE LA CIBERSEGURIDAD

(El presente Título y todo su Articulado fue Agregado por el Art. 6 de la Ley s/n, R.O. 290-5S, 22-V-2026)

Art. 20-A.- Ámbito de aplicación.- Las disposiciones de este Título serán aplicables a:

a) Las entidades que integran el sector público, conforme a lo previsto en el artículo 225 de la Constitución de la República, en lo que corresponda a la gestión de servicios esenciales o infraestructura crítica digital;

b) Los prestadores de servicios digitales únicamente respecto de los elementos que se encuentren bajo su esfera de control, conforme al principio de responsabilidad compartida y a lo previsto en el artículo 20-I; y,

c) Las personas jurídicas privadas responsables de infraestructura crítica digital o cuya actividad tenga incidencia directa en la continuidad de servicios esenciales, de conformidad con criterios objetivos establecidos en la normativa técnica.

En ningún caso estas disposiciones serán exigibles a personas naturales, ni a personas jurídicas cuya actividad no haya sido previamente clasificada como crítica o esencial por el ente rector, salvo lo dispuesto en el literal c).

Capítulo I
Principios y Coordinación

Art. 20-B.- Principios de ciberseguridad.- La implementación de políticas, medidas y mecanismos de ciberseguridad por parte de las entidades públicas, los prestadores de servicios digitales y los operadores de infraestructura crítica digital se regirá por los siguientes principios:

a) Confidencialidad.- Garantizar que los datos, sistemas y activos digitales sean accesibles

únicamente por personas, entidades o sistemas autorizados, evitando divulgaciones, accesos o exposiciones indebidas.

b) Integridad.- Asegurar que la información, los sistemas y los procesos digitales se mantengan completos, coherentes y sin alteraciones no autorizadas o accidentales, preservando su exactitud y fiabilidad.

c) Disponibilidad.- Garantizar que los servicios, plataformas, sistemas y datos digitales estén accesibles y operativos cuando sean requeridos por usuarios autorizados, incluso en situaciones de contingencia o ataque.

d) Control de daños.- Ante incidentes, actuar rápida y coordinadamente para evitar la propagación y escalada.

e) Cooperación con la autoridad.- Obligación de colaborar con el ente rector y, cuando corresponda, entre sectores público y privado.

f) Coordinación interinstitucional.- Las autoridades deben cumplir sus funciones de manera armónica, evitando duplicidad o interferencia.

g) Seguridad en el ciberespacio.- Es deber del Estado garantizar un entorno digital seguro para todas las personas, con atención especial a grupos vulnerables.

h) Respuesta responsable.- Las medidas de ciberseguridad deben tener carácter estrictamente defensivo y no habilitan operaciones ofensivas.

i) Proporcionalidad.- Las obligaciones y medidas deben ser necesarias y acordes al nivel de riesgo, criticidad y sensibilidad del activo protegido, evitando tanto la sobreprotección como la exposición indebida.

j) Seguridad y privacidad desde el diseño y por defecto.- Los sistemas y tecnologías deben implementarse teniendo en cuenta la seguridad y la protección de datos desde su origen.

k) Resiliencia.- Capacidad de los sistemas, redes y servicios digitales para anticipar, resistir, adaptarse y recuperarse frente a incidentes de ciberseguridad, garantizando la continuidad de su funcionamiento.

l) Neutralidad tecnológica.- La adopción de marcos y soluciones de ciberseguridad debe realizarse sin favorecer tecnologías, marcas o proveedores específicos, promoviendo la interoperabilidad, la innovación abierta y la adaptabilidad tecnológica.

m) Responsabilidad compartida.- Las obligaciones de prevención, protección, respuesta y recuperación frente a incidentes de ciberseguridad deben distribuirse entre los distintos

actores del ecosistema digital, públicos y privados, de acuerdo con su rol, nivel de exposición y capacidad operativa.

n) Adaptabilidad tecnológica.- Las políticas, medidas y estándares de ciberseguridad deberán adaptarse a la evolución de tecnologías emergentes que puedan comprometer los mecanismos tradicionales de protección digital, incluyendo los riesgos derivados de la computación cuántica. El ente rector emitirá normativa técnica progresiva para orientar la adopción de mecanismos criptográficos resilientes y estándares internacionales actualizados.

Art. 20-C.- Coordinación estratégica en ciberseguridad.- El ente rector liderará la formulación y evaluación de la política pública nacional en materia de ciberseguridad, en coordinación con las autoridades rectoras en defensa nacional, seguridad interna, protección de datos personales y otras entidades competentes, exclusivamente en lo que concierna al diseño de estrategias y marcos normativos relacionados con la prevención, gestión de riesgos, protección de infraestructura crítica, servicios esenciales y derechos afectados por incidentes cibernéticos, sin perjuicio de las competencias regulatorias, técnicas o sancionadoras que correspondan a los órganos de control especializados.

Art. 20-D.- Coordinación operativa para la implementación de la política de ciberseguridad.- El ente rector coordinará con las entidades responsables de defensa nacional, seguridad interna, salud, justicia, educación, inclusión, sistema financiero, protección de datos personales y demás órganos de control especializados creados por la Constitución o la ley, la implementación armónica de medidas de ciberseguridad, garantizando la protección de la infraestructura crítica digital, la continuidad operativa de servicios esenciales y la protección de derechos frente a amenazas cibernéticas, sin perjuicio de las competencias regulatorias, técnicas o sancionadoras que correspondan a los órganos de control especializados y respetando en todo momento las competencias asignadas a cada entidad.

Esta coordinación se realizará mediante convenios, comités técnicos o instrumentos de planificación interinstitucional, conforme a lo establecido en esta ley y su normativa técnica.

En el marco de esta coordinación se reconocerá la corresponsabilidad de los distintos actores públicos y privados en la prevención, protección, respuesta y recuperación frente a incidentes de ciberseguridad, de acuerdo con su rol, nivel de exposición y capacidad operativa.

El reglamento de esta ley establecerá los criterios técnicos y el procedimiento de escalamiento para la determinación de incidentes de ciberseguridad que comprometan la seguridad y defensa nacional. Dicho procedimiento garantizará la coordinación inmediata entre el ente rector en materia de ciberseguridad y el Ministerio de Defensa Nacional, en

el marco de la seguridad integral del Estado y del respeto a las competencias constitucionales de cada entidad.

Art. 20-E.- Coordinación con la autoridad de protección de datos personales.- Las acciones que se desarrollen en el marco de la presente ley y que tengan incidencia en el tratamiento de datos personales deberán coordinarse con la Autoridad de Protección de Datos Personales, de conformidad con lo dispuesto en la Ley Orgánica de Protección de Datos Personales.

La elaboración de políticas, protocolos de gestión de incidentes, normas técnicas y toda medida que implique el uso, procesamiento, transferencia o resguardo de datos personales deberá respetar los principios, derechos y garantías previstos en dicha ley, asegurando la no duplicidad de funciones y el respeto a la competencia de cada entidad.

Capítulo II
Gestión de incidentes y notificación.

Art. 20-F.- Gestión de incidentes de ciberseguridad.- Las entidades del sector público deberán implementar políticas y procedimientos para la gestión de incidentes digitales, que incluyan mecanismos de prevención, monitoreo, detección, evaluación de impacto, notificación temprana, contención y recuperación.

El ente rector emitirá directrices técnicas para la aplicación de estas medidas y establecerá, en coordinación con el CSIRT Nacional y las autoridades competentes, los protocolos de reporte, intercambio de información y coordinación institucional necesarios, evitando duplicidad de canales en los sectores con órgano de control especializado y respetando sus procedimientos propios.

Art. 20-G.- Obligación de notificación de incidentes de ciberseguridad.- Las entidades públicas y operadores de infraestructura crítica digital deberán notificar sin dilación indebida al ente rector cualquier incidente de seguridad digital que:

a) Comprometa la disponibilidad, confidencialidad o integridad de sistemas o información relevante, incluyendo incidentes cuyo impacto genere riesgos significativos para la continuidad de servicios esenciales o la protección de derechos fundamentales vinculados al funcionamiento de sistemas o información crítica.
b) Afecte la continuidad operativa de servicios esenciales o críticos.
c) Suponga una vulneración de la seguridad que pueda escalar o propagarse.

La notificación deberá realizarse de inmediato y, en todo caso, dentro de un plazo máximo de setenta y dos (72) horas desde su detección, de conformidad con los protocolos que establezca el ente rector. La omisión injustificada será sancionada de conformidad con la normativa vigente.

La notificación realizada de buena fe y dentro de los plazos establecidos no podrá ser utilizada, por sí sola, como prueba exclusiva de negligencia o incumplimiento en procedimientos administrativos, civiles o judiciales. Esta protección será aplicable siempre que la entidad demuestre haber adoptado medidas razonables de prevención, contención y recuperación frente al incidente reportado.

La información compartida en el marco de la gestión de incidentes estará sujeta a reserva y confidencialidad, salvo las alertas tempranas que deban difundirse para salvaguardar el interés público.

En los sectores bajo supervisión de órganos de control especializados, la notificación se realizará a través de dichos órganos, los cuales consolidarán y remitirán la información al ente rector conforme a los formatos y plazos definidos por este.

Art. 20-H.- Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional).- El ente rector contará con un Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), como instancia técnica especializada para la prevención, detección, gestión y coordinación de incidentes de ciberseguridad que afecten a entidades públicas, operadores de infraestructura crítica digital y prestadores de servicios digitales.

El CSIRT Nacional actuará bajo la rectoría del ente rector y coordinará sus acciones con los CSIRT sectoriales, órganos sectoriales de supervisión y control, y con organismos internacionales, conforme los principios de colaboración, intercambio de información y protección de datos sensibles.

El CSIRT Nacional gozará de autonomía técnica y operativa para ejecutar acciones inmediatas de prevención, detección y respuesta frente a incidentes críticos, conforme a protocolos previamente aprobados por el ente rector. Dichas actuaciones no requerirán autorización previa, sin perjuicio de la obligación de informar posteriormente al ente rector para efectos de coordinación y registro.

El CSIRT Nacional realizará ejercicios de ciberseguridad de manera planificada y periódica, conforme a análisis de riesgos y a los planes que se establezcan para el efecto. La planificación, metodología y alcance de dichos ejercicios se desarrollarán mediante la normativa técnica correspondiente.

La notificación de incidentes de ciberseguridad prevista en esta ley no sustituye la obligación legal de denunciar ante la Fiscalía General del Estado los hechos que constituyan o pudieren constituir delitos de acción pública.

Capítulo III
Prestadores de servicios digitales y sector privado.

Art. 20-I.- Responsabilidades de los Prestadores de Servicios Digitales (PSD).- Las obligaciones previstas en el presente artículo serán aplicables a los PSD en lo relativo a los elementos que se encuentren bajo su esfera de control, de conformidad con el principio de responsabilidad compartida.

a) Los PSD deberán implementar medidas técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la infraestructura y servicios provistos, basadas en estándares internacionales reconocidos. Dichas medidas comprenderán, como mínimo:

1. La evaluación y gestión de riesgos respecto de los componentes bajo control del PSD.
2. La adopción e implementación de políticas globales de seguridad.
3. La aplicación de controles de privacidad conforme el marco normativo vigente.
4. El cumplimiento de la Ley Orgánica de Protección de Datos Personales.
5. La implementación de sistemas de gestión de seguridad de la información basados en certificaciones internacionales.

b) Las entidades contratantes podrán solicitar que los PSD acrediten el cumplimiento de estas medidas mediante informes de auditoría y certificaciones internacionales.
c) Los PSD deberán informar a las entidades contratantes, de manera oportuna, sobre vulnerabilidades o incidentes que afecten específicamente los recursos contratados por dicha entidad.
d) Los PSD deberán cooperar con las entidades contratantes en la gestión de incidentes, conforme al principio de responsabilidad compartida y a los límites de su modelo operacional, brindando la información y soporte en relación con los servicios provistos.
e) Los PSD deberán establecer, en los términos contractuales, un punto de contacto técnico permanente con las entidades contratantes para la gestión de incidentes que puedan afectar los servicios provistos.

Art. 20-J.- Coordinación con la autoridad competente.- Las entidades públicas y operadores de infraestructura crítica digital deberán designar un punto de contacto técnico permanente, disponible de manera continua las veinticuatro (24) horas del día y los siete (7) días de la semana, para la coordinación con el ente rector y con el CSIRT Nacional.

La normativa secundaria establecerá los protocolos de coordinación, plazos de respuesta y formatos de comunicación.

Art. 20-K.- Responsabilidades del sector privado en materia de ciberseguridad.- Los proveedores de servicios esenciales y operadores de infraestructura crítica deberán:

a) Implementar sistemas de gestión de seguridad de la información basados en estándares internacionales reconocidos, u otros equivalentes, conforme a la normativa técnica

sectorial aplicable.
b) Contar con mecanismos de monitoreo, detección y respuesta ante incidentes.
c) Notificar incidentes relevantes al ente rector en los términos del artículo 20-G.
d) Participar en simulacros, auditorías o ejercicios de ciberseguridad promovidos por el Estado.

La normativa técnica establecerá obligaciones diferenciadas según el nivel de riesgo y criticidad del servicio prestado.

En el caso de sectores supervisados por órganos de control especializados, las obligaciones serán determinadas por sus respectivas autoridades de control, siempre que dichas disposiciones sean reconocidas como equivalentes a los estándares mínimos nacionales de ciberseguridad establecidos por el ente rector.

Art. 20-L.- Evaluación de vulnerabilidades y hacking ético.- Las entidades públicas y los operadores de infraestructura crítica digital podrán autorizar la realización de pruebas controladas de seguridad, conocidas como hacking ético o pruebas de penetración, con el objeto de identificar, evaluar y mitigar vulnerabilidades de sus sistemas, redes o servicios digitales.

Estas actividades deberán observar los siguientes principios y condiciones:

a) Consentimiento expreso.- Toda prueba deberá contar con la autorización escrita del titular o responsable legal del sistema o infraestructura, delimitando su alcance, duración y objetivos técnicos.
b) Finalidad legítima.- Las pruebas se realizarán exclusivamente para fines de mejora de la seguridad, sin alterar la disponibilidad, integridad o confidencialidad de la información ni causar interrupciones no previstas.
c) Registro y requisitos profesionales.- Las personas naturales o jurídicas que realicen actividades de hacking ético deberán inscribirse en el Registro Nacional de Profesionales y Empresas de Pruebas de Seguridad, administrado por el ente rector en materia de ciberseguridad. Para su inscripción deberán presentar certificaciones técnicas vigentes emitidas por organismos de reconocimiento nacional o internacional, acreditados conforme a estándares ISO 17024 o equivalentes. La inscripción tendrá carácter obligatorio para fines de trazabilidad, coordinación y supervisión posterior, sin que implique la emisión de certificaciones, licencias o autorizaciones por parte del ente rector.

El ente rector verificará la información y documentación presentada. La inscripción en el registro será obligatoria respecto de la habilitación profesional y no eximirá a los inscritos de las responsabilidades civiles, administrativas o penales derivadas del ejercicio de sus actividades.

El ente rector podrá requerir información adicional, informes de ejecución, evidencias

técnicas y demás documentación necesaria para asegurar que las actividades de evaluación de vulnerabilidades se realicen conforme a esta Ley y su normativa técnica.

Los inscritos deberán suscribir de manera obligatoria un código de ética y responsabilidad profesional que establezca principios de conducta, estándares mínimos de actuación y obligaciones de confidencialidad. Su incumplimiento podrá dar lugar a la suspensión o cancelación del registro, sin perjuicio de las demás responsabilidades civiles, administrativas o penales a que hubiere lugar.
d) Confidencialidad y protección de datos.- Toda información obtenida durante las pruebas se considerará reservada y no podrá divulgarse ni utilizarse para otros fines distintos de la evaluación de seguridad, conforme a la Ley Orgánica de Protección de Datos Personales.
e) Reporte y remediación.- Los resultados deberán ser documentados y comunicados al responsable del sistema, quien adoptará las medidas correctivas pertinentes. En caso de detectarse vulnerabilidades críticas, deberá notificarse también al CSIRT Nacional conforme a los protocolos establecidos.

El ente rector establecerá mediante normativa técnica los procedimientos, estándares y requisitos mínimos para la ejecución de pruebas de hacking ético, así como la operatividad progresiva del Registro Nacional.

Capítulo IV
Infraestructura crítica digital y fiscalización.

Art. 20-LL.- Clasificación de infraestructura crítica digital.- El ente rector, en coordinación con las entidades responsables de los sectores que presten servicios esenciales o administren infraestructura crítica, definirá los criterios para la identificación, clasificación y protección de la infraestructura crítica digital, considerando:

a. El impacto potencial de una disrupción.
b. La interdependencia con otros sectores.
c. La criticidad de la información procesada para la continuidad operativa de servicios esenciales.
d. La existencia de sistemas de control industrial, automatización o tecnología operacional (OT) cuya alteración pueda afectar el funcionamiento de infraestructuras o servicios esenciales.

La clasificación no altera ni sustituye las atribuciones regulatorias, técnicas o sancionadoras de las autoridades sectoriales competentes, que mantendrán la plenitud de sus facultades en los respectivos ámbitos.

Las entidades que operen dicha infraestructura deberán implementar planes de protección, continuidad operativa, monitoreo y respuesta ante incidentes, conforme a los

estándares mínimos nacionales de ciberseguridad, desarrollados mediante normativa técnica.

Art. 20-M.- Fiscalización y acciones de adecuación técnica.- El ente rector podrá realizar acciones de fiscalización técnica únicamente en los sectores que no cuenten con órganos de control especializados. En los sectores regulados, las acciones de fiscalización serán exclusivas de dichos órganos, sin perjuicio de que el ente rector emita lineamientos técnicos generales o participe en comités de coordinación interinstitucional. En caso de incumplimiento, podrá disponer:

a. Instrucciones técnicas de cumplimiento obligatorio para subsanar deficiencias.
b. Medidas de prevención o contención de riesgos.
c. Requerimientos de capacitación o auditoría externa.

En caso de reincidencia o negativa a implementar las recomendaciones, se informará a las autoridades competentes para la imposición de sanciones administrativas conforme a la ley.

En los sectores supervisados por órganos de control especializados, la fiscalización y medidas correctivas serán conducidas por dichos órganos; el ente rector podrá emitir lineamientos técnicos generales y participar en evaluaciones conjuntas mediante informes técnicos no vinculantes.

Capítulo V
Gobernanza y cooperación.

Art. 20-N.- Comité Nacional de Ciberseguridad.- El Comité Nacional de Ciberseguridad es la instancia de coordinación estratégica interinstitucional para la formulación, articulación y seguimiento de la Política Nacional de Ciberseguridad.

Este comité será presidido por el ente rector y estará conformado por las instituciones establecidas en el reglamento de esta ley.

Dependiendo de la naturaleza de los temas a tratarse, el Comité contará con la participación de representantes del sector privado, del sistema académico y científico especializado en ciberseguridad, y de otros actores cuya intervención se considere necesaria para la toma de decisiones o la implementación de políticas específicas.

El reglamento establecerá los mecanismos de convocatoria, designación y funcionamiento del Comité, en ejercicio de la facultad reglamentaria del Ejecutivo.

Art. 20-Ñ.- Cooperación internacional en ciberseguridad.- El ente rector, en coordinación con el ente rector de las Relaciones Exteriores y otros órganos competentes, promoverá la

cooperación internacional en ciberseguridad mediante:

a. Participación en redes regionales y globales de respuesta a incidentes (CSIRT/CERT).
b. Adopción de estándares y marcos normativos internacionales.
c. Celebración de acuerdos de asistencia mutua, intercambio de información y fortalecimiento de capacidades.

Art. 20-O.- Regímenes especiales.- La Asamblea Nacional, la Función Judicial, la Contraloría General del Estado, el Banco Central del Ecuador, la Fiscalía General del Estado, el Consejo Nacional Electoral deberán adoptar las medidas de seguridad pertinentes para la protección de sus redes y sistemas informáticos.

Las instituciones y órganos señalados en este artículo no estarán sujetos a la regulación, fiscalización o supervisión del ente rector en materia de ciberseguridad; sin perjuicio de la obligación de convenir mecanismos de reporte de incidentes y de coordinación y cooperación para la respuesta a incidentes de ciberseguridad.

Capítulo VI
Del Régimen Administrativo Sancionador

Art. 20-P.- Principios aplicables.- El régimen administrativo sancionador en materia de ciberseguridad se regirá por los principios de legalidad, tipicidad, proporcionalidad, seguridad jurídica, debido proceso, especialidad, cooperación interinstitucional, responsabilidad, transparencia y non bis in ídem.

Toda potestad sancionadora deberá ejercerse con sujeción a las garantías previstas en la Constitución de la República y en el Código Orgánico Administrativo, asegurando la debida separación entre las fases de instrucción, resolución, impugnación y ejecución del procedimiento.

Las disposiciones de este capítulo se aplicarán en armonía con las competencias de los órganos de regulación, supervisión y control especializados, y conforme al plazo de vigencia determinado en la Disposición Transitoria Segunda.

Art. 20-Q.- Sujetos responsables.- Serán responsables administrativamente por el incumplimiento de las obligaciones establecidas en este Título:

a) Las entidades y organismos del sector público, conforme a su respectivo régimen jurídico, en lo relativo a la gestión de servicios esenciales o infraestructura crítica digital bajo su administración. Las sanciones aplicables tendrán carácter correctivo o preventivo, sin perjuicio de las responsabilidades administrativas o civiles de sus autoridades o servidores públicos.

b) Los prestadores de servicios digitales exclusivamente en lo relativo a los elementos bajo su esfera de control, conforme al artículo 20-I y al principio de responsabilidad compartida.

c) Las personas jurídicas privadas responsables de infraestructura crítica digital o cuya actividad tenga incidencia directa en la continuidad de servicios esenciales, de acuerdo con la normativa técnica, expedida por el ente rector.

d) Las demás personas jurídicas privadas que, sin ser prestadores digitales, participen en la provisión de servicios tecnológicos indispensables para la operación de servicios esenciales, según los criterios objetivos y parámetros técnicos determinados por el rector.

Art. 20-R.- Clasificación de infracciones.- Las infracciones administrativas en materia de ciberseguridad se clasifican en leves, graves y muy graves:

Infracciones leves:

Se consideran infracciones leves las siguientes:

1. Retrasar la actualización de políticas, planes o protocolos de ciberseguridad sin generar impacto operativo.
2. Omitir reportes periódicos o notificaciones menores a la autoridad competente.

Infracciones graves:

Se consideran infracciones graves las siguientes:

1. No implementar la política y estrategia de ciberseguridad.
2. Ocultar incidentes significativos que afecten la disponibilidad o integridad de sistemas.
3. No implementar medidas mínimas obligatorias de seguridad digital.
4. Obstaculizar verificaciones técnicas o auditorías dispuestas por la autoridad.
5. Reincidir en infracciones leves.
6. No implementar medidas técnicas organizativas o de cualquier índole, necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones de ciberseguridad.

Infracciones muy graves:

Se consideran infracciones muy graves las siguientes:

1. Ocultar incidentes críticos o comprometer la integridad de la información.
2. No informar a la autoridad competente eventos de ataques cibernéticos o brechas de información causadas por ciberataques ocurridos que afecten derechos de terceros.

3. Negarse a cooperar con la autoridad competente o manipular evidencia.
4. Destruir registros digitales o incumplir planes de resiliencia en infraestructura crítica.

Las sanciones se aplicarán conforme a la naturaleza del sujeto infractor.

Art. 20-S.- Sanciones por infracciones leves.- La autoridad competente, de conformidad con lo previsto en los artículos 20-Y y 20-Z de esta ley, impondrá las siguientes sanciones administrativas en caso de verificarse el cometimiento de una infracción leve, conforme a los presupuestos establecidos en el presente Capítulo:

1. Servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente ley, serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general.

2. Entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

La autoridad competente establecerá la multa aplicable en función del principio de proporcionalidad.

Art. 20-T.- Sanciones por infracciones graves.- La autoridad competente, de conformidad con lo previsto en los artículos 20-Y y 20-Z de esta ley, impondrá las siguientes sanciones administrativas en caso de verificarse el cometimiento de una infracción grave, conforme a los presupuestos establecidos en el presente Capítulo:

1) Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente ley serán sancionados con una multa de entre 10 a 20 salarios básicos unificados del trabajador en general.

2) Para una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

La autoridad competente establecerá la multa aplicable en función del principio de proporcionalidad.

Art. 20-U.- Sanciones por infracciones muy graves.- La autoridad competente, de conformidad con lo previsto en los artículos 20-Y y 20-Z de esta ley, impondrá las siguientes sanciones administrativas en caso de verificarse el cometimiento de una infracción muy grave, conforme a los presupuestos establecidos en el presente Capítulo:

1) Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones muy graves establecidas en la presente ley serán sancionados con una multa de entre 20 a 40 salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;

2) Para una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 1% y el 1.5% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

La autoridad competente establecerá la multa aplicable en función del principio de proporcionalidad.

Art. 20-V.- Volumen de negocio.- A efectos del régimen sancionatorio de la presente ley, se entiende por volumen de negocio, a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.

Art. 20-W.- Medidas accesorias y correctivas.- La autoridad competente podrá disponer, de manera accesoria a la resolución sancionadora aplicable, medidas orientadas a la corrección o prevención de riesgos, tales como:

a) Elaboración y ejecución de planes de adecuación en materia de ciberseguridad con plazos y metas verificables.
b) Realización de auditorías técnicas independientes.
c) Publicación de la resolución sancionadora en el portal institucional del sujeto obligado, resguardando la información de carácter reservado o confidencial.
d) Restricciones temporales para contratar con el Estado respecto del objeto de la infracción, conforme a la ley y previa notificación al ente rector de la contratación pública.

Art. 20-X.- Criterios de graduación.- Para determinar las sanciones dentro de los rangos previstos en los artículos 20-S, 20-T y 20-U, se considerarán, entre otros, los siguientes criterios:

a) La gravedad del daño o riesgo causado;
b) La intencionalidad o negligencia;
c) Las medidas preventivas adoptadas previamente;
d) La cooperación con la autoridad;
e) El tamaño y capacidad económica del infractor;
f) La existencia y efectividad de programas de cumplimiento;
g) El riesgo sistémico y la criticidad del servicio; y,
h) La reincidencia.

En todo caso, las sanciones deberán ser proporcionales al daño potencial o efectivo causado.

Art. 20-Y.- Coordinación interinstitucional y non bis in ídem.- La potestad sancionadora en materia de ciberseguridad será ejercida por los órganos de regulación, supervisión o control especializados dentro de su ámbito de competencia.

El ente rector ejercerá esta potestad únicamente en los sectores que carezcan de órgano especializado, previa coordinación interinstitucional con las autoridades competentes.

Se garantizará el principio de non bis in ídem. Ninguna entidad podrá imponer dos sanciones por los mismos hechos y fundamento.

Las entidades coordinarán entre sí para evitar duplicidades y determinar la autoridad prevalente conforme a la materia, el bien jurídico protegido y el principio de especialidad.

Art. 20-Z.- Competencia y procedimiento sancionador.- En lo referente al procedimiento aplicable para efecto de la determinación de infracciones e imposición de sanciones, se estará a lo dispuesto en el Código Orgánico Administrativo (COA) respecto de las fases previas, de instrucción y de resolución del procedimiento administrativo sancionador. El referido procedimiento se sustanciará observando las particularidades previstas en el Reglamento de esta Ley, garantizando en todo momento las garantías del debido proceso, la imparcialidad, el derecho a la defensa y la separación entre las funciones instructora y resolutora.

En los sectores con órganos de regulación, supervisión o control especializados, tales como el financiero y de telecomunicaciones, estos instruirán y resolverán los procedimientos sancionadores conforme a su normativa sectorial, incluidos los aspectos de ciberseguridad.

En los sectores que carezcan de órgano especializado y regulación previa en materia de ciberseguridad, el ente rector instruirá y resolverá los procedimientos sancionadores de manera subsidiaria y en coordinación con las autoridades competentes, aplicando criterios de gradualidad y proporcionalidad en atención al tamaño, capacidad económica, nivel de criticidad del servicio y riesgo sistémico.

En estos sectores, las medidas sancionadoras deberán privilegiar el carácter preventivo y correctivo, reservando las sanciones económicas para casos de incumplimiento grave o deliberado que comprometa directamente la continuidad de servicios esenciales o la integridad de infraestructura crítica digital.

Título V
CONSOLIDACIÓN DE LA TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL

Art. 21.- Publicidad y transparencia de la administración pública.- Los diferentes órganos de la Asamblea Nacional, el pleno del Consejo de la Judicatura, el pleno de la Corte Nacional de Justicia, el pleno de la Corte Constitucional, el pleno del Consejo de Participación Ciudadana y Control Social, el pleno de la Función de Transparencia y Control Social, el pleno del Consejo Nacional Electoral y el pleno del Tribunal Contencioso Electoral deberán transmitir en vivo y en directo sus sesiones ordinarias y extraordinariasa través de los canales de comunicación oficiales de los nombrados organismos de la administración pública.

Únicamente en casos excepcionales tales como motivos de seguridad nacional o situaciones donde se vean involucrados derechos de niñas, niños y adolescentes, así como también controversias o negociaciones comerciales del Estado, el Pleno de los organismos prenombrados podrá declarar las sesiones con carácter reservado, para lo cual será necesario el voto de la mayoría calificada de sus integrantes.

La publicidad y transparencia de los organismos nombrados en el inciso anterior incluye la publicación de las convocatorias a sesiones ordinarias o extraordinarias a través de los canales de comunicación oficiales.

En el caso de los órganos jurisdiccionales de la Función Judicial, el Tribunal Contencioso Electoral y la Corte Constitucional, las audiencias también deberán ser de carácter público y al alcance de la conexión de la ciudadanía, salvo los casos en donde la ley expresamente reconozca reserva. Las y los juzgadores únicamente deberán solicitar del público que se registren como tales al momento de su conexión.

Art. 22.- Implementación de la firma electrónica.- Los diferentes organismos de la administración pública, así como el sector privado, deberán implementar y aceptar dentro de sus diferentes procesos el uso de la firma electrónica por parte de los administrados.

Será a elección del administrado la utilización de su firma manuscrita en los diferentes procesos de la administración pública o del sector privado.

Art. 23.- De los casilleros virtuales.- Los organismos del Estado bajo ningún concepto, ni aún bajo pretexto de escasez de recursos, podrán negar la recepción o exigir la presentación física de los documentos que hayan sido presentados con firma electrónica en los casilleros o ventanillas virtuales a su cargo.

Título VI
DEL SECTOR AUDIOVISUAL

Art. 24.- De la producción audiovisual.- Como parte de la transformación digital y fomento a la inversión y dinamización de actividades económicas, se establece como

sector de interés nacional a la producción audiovisual incluyendo el desarrollo, preproducción, producción, postproducción y distribución de contenidos audiovisuales.

Art. 25.- Régimen especial de exoneración.- A fin de promover la transformación digital, la importación de bienes que se requieran para la producción de obras audiovisuales que conste en el listado que apruebe el Comité de Comercio Exterior (COMEX) a recomendación del Instituto de Fomento a la Creatividad y la Innovación, IFCI, estará exenta de todo derecho arancelario, impuesto, gravamen, tasa o contribución en régimen de consumo o internación temporal. A fin de facilitar la importación, aplicará en este caso el procedimiento aplicable a aquellos sujetos pasivos que según su actividad económica, se dediquen a la producción audiovisual.

Art. 26.- Exoneración del ISD.- Se exonera de Impuesto a la Salida de Divisas los siguientes pagos al exterior que se realicen con el objeto de realizar producciones audiovisuales y actividades artísticas y culturales:

a. Importación de equipos y bienes destinados a la producción, promoción y difusión audiovisual local y extranjera en el Ecuador.
b. Pago de salarios, honorarios, remuneraciones o viáticos a personas naturales o jurídicas que tengan residencia fiscal en el extranjero, para que presten sus servicios en la producción audiovisual nacional y extranjera en el Ecuador.

El reglamento determinará el mecanismo de verificación de la actividad productiva conforme al presente artículo.

Art. 27.- Exoneración de Impuesto a la Renta en pagos al exterior.- Los pagos al exterior que se realicen a personas naturales o jurídicas con residencia fiscal en el extranjero, por la prestación de servicios en la producción audiovisual nacional y extranjera en Ecuador, no estarán sujetos a retención en la fuente del impuesto a la renta, el cual los beneficiarios de estos pagos deberán acreditar con su respectivo certificado de su residencia fiscal, el cual deberá permanecer en custodia del beneficiario del servicio.

Art. 28.- Exoneración del Impuesto al Valor Agregado.- Los servicios digitales que paguen el Impuesto al Valor Agregado que estén avalados por el Servicio de Rentas Internas pueden tener una exoneración de este impuesto en función de lo dispuesto por el Reglamento a esta Ley, siempre y cuando presten sus conocimientos, bienes o cualquier otra clase de apoyo técnico al desarrollo, preproducción, producción, postproducción y distribución en todas las etapas de su producción a los contenidos audiovisuales nacionales.

Art. 29.- Certificado de Inversión Audiovisual.- Se crea el Certificado de Inversión Audiovisual (CIA) el cual será emitido por el SRI a favor de productoras nacionales y extranjeras por el 37% de los costos y gastos que incurran en el Ecuador en servicios

audiovisuales y logísticos necesarios siempre que se encuentre soportados en comprobantes de venta válidos. El CIA es un título valor y podrá ser utilizado como crédito tributario de los impuestos administrados por el Servicio de Rentas Internas.

El ingreso por la transferencia del Certificado de Inversión Audiovisual obtenido por una persona natural o jurídica nacional o extranjera, no será gravable ni sujeto a retención en la fuente del impuesto a la renta en el Ecuador. El Ministerio de Economía y Finanzas imperativamente fijará en los dos últimos meses de cada año, el monto máximo de Certificados de Inversión Audiovisual que podrá otorgarse en el año calendario siguiente, el cual no podrá ser menor de 1000 fracciones básicas exentas de impuesto a la renta, con fundamento en el informe económico que reciba del Servicio de Rentas Internas sobre las condiciones del sector audiovisual, así como el monto mínimo de las inversiones requeridas en el país tanto para las producciones nacionales como para las extranjeras. En el Reglamento a esta Ley, se determinarán los requisitos de inversión, destinatarios y demás aspectos para su ejecución.

Art. 30.- Incentivo al desarrollo del talento y la economía nacional.- Como un aporte de los sujetos pasivos del sector audiovisual que accedan a las exoneraciones y certificado de crédito tributario previsto en el presente título, en el marco de su responsabilidad social corporativa, y con la finalidad de incentivar y promover la participación local y nacional, así como el empleo de materiales, insumos, equipo y mano de obra de origen ecuatoriano, deberán en el desarrollo, preproducción, producción, postproducción y distribución de contenidos audiovisuales, en cuánto les fuera posible para la ejecución de sus proyectos, contratar proveedores de obras, bienes y servicios de origen local y nacional.

En las contrataciones se preferirá al oferente de bienes, obras o servicios que incorpore mayor componente de origen ecuatoriano o a los actores de la Economía Popular y Solidaria y Micro, Pequeñas y Medianas Empresas.

Art. 31.- La interculturalidad será un eje prioritario de la actividad audiovisual y los incentivos otorgados deberán considerar, entre uno de los factores, al involucramiento de pueblos y nacionalidades en la actividad audiovisual que se promueva.

Título VII
EDUCACIÓN PARA LA TRANSFORMACIÓN DIGITAL

Art. 32.- (Sustituido por el Art. 7 de la Ley s/n, R.O. 290-5S, 22-V-2026) Las instituciones públicas y privadas involucradas en procesos de Transformación Digital, deberán implementar planes y programas accesibles y gratuitos de formación y capacitación al usuario en el ámbito de desarrollo tecnológico a ser digitalizado, incluyendo la alfabetización en seguridad digital, ciberseguridad, protección de datos personales y ciudadanía digital, todos estos planes y programas, deberán ser diseñados en relación a la

presente Ley.

Dentro del proceso obligatorio de rendición de cuentas a cargo de cada entidad del Estado, deberá incluirse un segmento de Rendición de Cuentas en el ámbito de la Transformación Digital.

Art. 33.- De la transformación digital de las mallas curriculares.- (Reformado por el Art. 8 de la Ley s/n, R.O. 290-5S, 22-V-2026) Las escuelas, colegios y universidades deberán determinar dentro de sus ofertas educativas los programas o materias que, por su naturaleza, puedan ser cursadas por los estudiantes de manera virtual, incorporando progresivamente contenidos de seguridad digital, ciberseguridad, ética digital y protección de datos personales incluyendo su evaluación.

En el caso de las instituciones de educación superior públicas y privadas, de acuerdo a la naturaleza de la carrera o del programa de posgrado, deberán adecuar el desarrollo de sus programas de estudios al entorno virtual para elección del estudiante. El reglamento normará lo indicado en el presente artículo.

Las instituciones de educación superior públicas y privadas, deberán contar dentro de su planta docente con un mínimo de 5% de profesores contratados o titulares para ejercer labores académicas en modalidad virtual, sin perjuicio del lugar de su residencia, con el objetivo de contribuir al desarrollo del aprendizaje en línea, fomentar la internacionalización de la oferta académica, así como para promover el intercambio de experiencias y la integración de docentes dentro y fuera del país.

El Estado promoverá, además, la educación y la alfabetización digital en todos los niveles del Sistema Nacional de Educación, de tal manera que los estudiantes adquieran las habilidades y capacidades digitales necesarias para su adaptación a las nuevas tecnologías, en el marco de la transformación digital. Para el efecto, el ente rector de transformación digital, en coordinación con el ente rector de educación, emitirá las políticas, planes, programas y proyectos que sean necesarios.

Se aplicarán los principios de calidad y calidez para la determinación de los programas o materias que, por su naturaleza, puedan ser cursadas por los estudiantes de manera virtual, incluyendo su evaluación.

Art. 34.- Infocentros.- Los Gobiernos Autónomos Descentralizados en todos sus niveles, especialmente en la ruralidad, deberán implementar en sus dependencias un espacio destinado para un infocentro comunitario con acceso a internet libre y gratuito, con el fin de reducir la brecha digital.

Libro II
REFORMAS A VARIOS CUERPOS LEGALES

Título I
REFORMAS A LA LEY ORGÁNICA DE TELECOMUNICACIONES

Art. 35.- En el artículo 3 agregar como numeral 18 el siguiente texto:

"18. Fomentar el despliegue de redes comunitarias de telecomunicaciones en zonas urbano-marginales, rurales, fronterizas y prioritarias, así como garantizar el desarrollo de redes comunitarias de telecomunicaciones, para garantizar el acceso a las tecnologías de la información y comunicación que coadyuven a disminuir la brecha digital."

Art. 36.- Sustitúyase el último inciso del artículo 9 por el siguiente texto:

"De acuerdo con su utilización las redes de telecomunicaciones se clasifican en:

a) Redes Públicas de Telecomunicaciones.
b) Redes Privadas de Telecomunicaciones.
c) Redes Comunitarias de Telecomunicaciones."

Art. 37.- A continuación del artículo 13, incorpórese un artículo 13.1, con el siguiente texto:

"

Art. 13.1.- Redes comunitarias de telecomunicaciones.- Las redes comunitarias son aquellas desplegadas y/o utilizadas por personas naturales o jurídicas públicas o privadas, sin fines de lucro, o por organizaciones de la economía popular y solidaria legalmente constituidas, que tienen el propósito de satisfacer las necesidades de servicios de telecomunicaciones propias de una o varias comunidades de conformidad a esta Ley.

Estas organizaciones auto provisionarán y auto gestionarán servicios de telecomunicaciones exclusivamente en zonas urbano-marginales, rurales, fronterizas y priorizadas que sean determinadas por el ente rector de las Telecomunicaciones y de la Sociedad de la Información.

Estas tenderán a un diseño de red abierta, sin protocolos ni especificaciones de tipo propietario y permitirá la interconexión, acceso y conexión con otras redes públicas. Su operación requiere de un registro realizado ante la Agencia de Regulación y Control de las Telecomunicaciones y en caso de requerir de uso de frecuencias del espectro radioeléctrico, del título habilitante respectivo.

La Agencia de Regulación y Control de las Telecomunicaciones regulará el establecimiento, garantizará la ciberseguridad y uso de redes comunitarias de telecomunicaciones; así como establecerá un régimen tarifario preferente."

Art. 38.- En el primer inciso del artículo 51, incorporar como numeral 9 el siguiente texto:

"9. Redes comunitarias de telecomunicaciones."

Art. 39.- Sustitúyase el último inciso del artículo 63 de la Ley Orgánica de Telecomunicaciones por el siguiente texto:

"Para favorecer el desarrollo del servicio universal y reducción de brecha digital, se regulará tarifas preferenciales que permitan el desarrollo económico de regiones, grupos sociales de atención prioritaria, y, de zonas rurales, urbano marginales y de frontera."

Art. 40.- A continuación del artículo 88 de la Ley Orgánica de Telecomunicaciones incluir el siguiente:

"Artículo 88.1.- De la Sociedad de la Información y el Conocimiento.- La Sociedad de la Información es aquella que a través de la transformación digital usa y se apropia de las telecomunicaciones y de las TIC, para mejorar la calidad de vida, la competitividad y el crecimiento económico.

El acceso y uso de las Tecnologías de la Información y Comunicaciones, el desarrollo de aplicaciones y contenidos digitales, la apropiación de nuevas tecnologías, el desarrollo de una cultura digital y proporcionar formación en tecnologías, son pilares de la consolidación de la Sociedad de la Información.

Todas las personas tienen el derecho a participar en la sociedad de la información. El Estado garantizará el acceso universal al servicio público de internet, de conformidad con la Constitución de la República.

La sociedad de la información y el conocimiento tendrá los siguientes fines:

a. Promover el uso y apropiación de las TIC;
b. Promover el desarrollo de contenidos y aplicaciones, y la prestación de servicios que usen Tecnologías de la Información y las Comunicaciones;
c. Promover políticas de competencia acordes a la era digital;
d. Incentivar y promover el desarrollo de la industria ecuatoriana de software y servicios TI para contribuir al crecimiento económico, la competitividad, la generación de empleo y las exportaciones;
e. Promover la transformación digital, con especial énfasis en los sectores de salud, educación y productividad; y,
f. Las entidades que forman parte del Gobierno Central deben dirigir sus actuaciones enfocadas al cumplimiento de los fines de la Sociedad de la Información."

Art. 41.- Incluir la siguiente Disposición Transitoria en la Ley Orgánica de Telecomunicaciones:

"Se dispone la optimización de los recursos por contribución del Servicio Universal, dispuesto en el artículo 92 de la Ley Orgánica de Telecomunicaciones. Para el empleo de estos recursos, el ente rector de las telecomunicaciones establecerá la priorización de proyectos que permitan la ampliación de conectividad de servicios de telecomunicaciones y el cierre de la brecha digital en las zonas urbano- marginales, rurales y fronterizas. En caso de existir recursos excedentes, éstos podrán ser ejecutados por la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, quien establecerá los criterios técnicos a fin de destinar dicho excedente para el desarrollo del ámbito tecnológico.

Los criterios para la priorización de proyectos que permitan la ampliación de conectividad de servicios de telecomunicaciones y el cierre de la brecha digital en las zonas urbano-marginales, rurales y fronterizas, serán definidos por el Ministerio de Telecomunicaciones y Sociedad de la Información en el término de 60 días contados a partir de la expedición de la presente reforma a la Ley Orgánica de Telecomunicaciones."

Art. 42.- Inclúyase después de la Disposición General Cuarta, la Disposición General Quinta, con el siguiente texto:

"Quinta.- Las frecuencias del espectro radioeléctrico para uso de emergencia, y uso para fines humanitarios, que cumplan con los lineamientos dispuestos por el ente rector de telecomunicaciones, estarán exentos del pago de tarifas por asignación y uso del espectro radioeléctrico. La Agencia de Regulación y Control de las Telecomunicaciones reglamentará la explotación de estos servicios."

Título II
(Derogado por la Disposición Derogatoria Vigésima Segunda de la Codificación de la Ley Orgánica de Educación Intercultural, R.O. 689-5S, 22-XI-2024).

Art. 43.- (Derogado por la Disposición Derogatoria Vigésima Segunda de la Codificación de la Ley Orgánica de Educación Intercultural, R.O. 689-5S, 22-XI-2024).

Título III
REFORMAS A LA LEY ORGÁNICA DE EDUCACIÓN SUPERIOR

Art. 44.- En el artículo 8 incorporar un nuevo literal:

"m) Fortalecer la formación profesional en las nuevas tecnologías para afrontar los retos de la economía digital, identificando habilidades tecnológicas y adaptando las mallas curriculares de la educación superior de acuerdo al nivel de desarrollo de tecnologías digitales."

Título IV
REFORMAS AL CÓDIGO DE COMERCIO

Art. 45.- Reemplácese el artículo 78 por el siguiente:

“

Art. 78.- Los títulos valores, físicos, desmaterializados o electrónicos, son documentos que representan el derecho literal y autónomo que en ellos se incorpora, permitiendo a su titular o legítimo tenedor ejercitar el derecho mencionado en él. Pueden ser de distinta naturaleza dependiendo del derecho o bien que ellos aluden.

Los títulos valores, físicos, desmaterializados o electrónicos, circulan de la manera establecida en la ley.

Los documentos y los actos a que se refiere este título sólo producirán los efectos en él previstos cuando contengan las menciones y llenen los requisitos que la ley señale.”

Art. 46.- Reemplácese el artículo 79 por el siguiente:

“

Art. 79.- El suscriptor, o la persona que firma un título valor, quedará obligado conforme al tenor literal del título valor, físico, desmaterializado o electrónico, a menos que firme con salvedades compatibles con su esencia.”

Art. 47.- En el artículo 80, eliminar el segundo inciso posterior al literal b, cuyo artículo quedaría redactado de la siguiente manera:

“

Art. 80.- Además de lo dispuesto para cada título valor en particular, los títulos valores deberán tener los siguientes requisitos:

a) La mención del derecho que en el título se incorpora, con indicación del objeto en que consiste y de su valor. Si la obligación consiste en una cantidad de dinero y ésta devenga intereses, la indicación de estos, o el porcentaje del cupo, margen o descuento sobre el importe del título, de ser el caso. De no haberse señalado la tasa de interés a pagar y/u otra forma de fijar ganancias en el título, y si la obligación de pago se funda en un mutuo o préstamo de consumo, se entenderá que la obligación devenga la tasa máxima de interés legal vigente, publicada por el Banco Central del Ecuador o la institución que haga sus veces en el futuro; y, a partir de que se haya constituido al deudor en mora, la tasa máxima de mora que corresponderá al uno punto un (1.1) veces la tasa legal antes indicada; y,
b) La firma, autógrafa o electrónica, de quién lo crea.

c) La aceptación podrá expresarse de la manera en la que lo pacten las partes tales como: teléfonos celulares, token, OTP, firma certificada u otro tipo de dispositivos o aplicaciones tipo APP o web u otras que hayan sido habilitadas con tal objetivo por el emisor del título.

La firma podrá sustituirse, bajo la responsabilidad del creador del título, por un signo o contraseña inserto mecánicamente. Este signo o contraseña debe ser protocolizado en una notaría previo su utilización.

La falta de fecha de creación del título, y si la ley no dispone otra cosa, no lo anulará y hará presumir iuris tantum que fue emitido en la misma fecha de vencimiento.

La indicación de los intereses, bajo ningún concepto podrá superar la tasa máxima de interés legal vigente publicada por el Banco Central del Ecuador o la institución que haga sus veces en el futuro, o caso contrario dicha indicación se entenderá como no escrita, sin perjuicio de las responsabilidades penales y civiles que se desprenda de este hecho."

Art. 48.- Reemplácese el artículo 85 por el siguiente:

"

Art. 85.- El título valor, físico, desmaterializado o electrónico, que cumpla los requisitos señalados en este Código adquiere eficacia a partir de su entrega al tenedor, salvo los casos de entrega realizada a terceros con finalidad de custodia o transporte.

Cuando el título se halle en poder de persona distinta del suscriptor se presumirá tal entrega."

Art. 49.- Reemplácese el artículo 88 por el siguiente:

"

Art. 88.- Cuando dos o más personas suscriban un título valor, físico, desmaterializado o electrónico, como giradores, otorgantes, emisores, endosantes, avalistas o fiadores, quedan obligados solidariamente a su pago. Los cedentes o quienes los transfieran, deberán limitar su responsabilidad mediante una leyenda que deberá constar en el mismo título o en una hoja adherida a éste o mediante cualquier medio gráfico, mecánico o electrónico; si no lo hicieran, responderán solidariamente del cumplimiento de la obligación que el título contiene.

Quien solucione o pague la obligación contenida en el título goza de los derechos que confiere la ley al codeudor solidario que paga respecto de los restantes codeudores."

Art. 50.- Reemplácese el artículo 90 por el siguiente:

"

Art. 90.- La reivindicación, el secuestro, o cualquier otra afectación o gravamen sobre los derechos consignados en un título valor, físico, desmaterializado o electrónico, o sobre las mercancías por él representadas, no surtirán efectos si no comprenden el título mismo materialmente."

Art. 51.- Reemplácese el artículo 92 por el siguiente:

"

Art. 92.- La fianza podrá constar en el título valor mismo, sea este físico, desmaterializado o electrónico o en hoja adherida a él o mediante cualquier medio gráfico, mecánico o electrónico. Podrá también, otorgarse por escrito separado en que se identifique plenamente el título cuyo pago total o parcial se garantiza. Se expresará con la fórmula por "fianza", "aval" u otra equivalente y deberá llevar la firma de quien lo presta. La sola firma puesta en el título, cuando no se le pueda atribuir otra significación se tendrá como firma de avalista y con el carácter de deudor solidario.

Cuando el aval se otorgue en documento separado del título, la negociación de éste implicará la transferencia de la garantía que surge de aquel."

Art. 52.- Reemplácese el artículo 95 por el siguiente:

"

Art. 95.- Si el título valor, físico, desmaterializado o electrónico, fuese emitido por más de una persona, la fianza o aval debe indicar la persona avalada. A falta de indicación quedarán garantizadas las obligaciones de todas y cada una de las partes en el título y la obligación será solidaria."

Art. 53.- Reemplácese el artículo 96 por el siguiente:

"

Art. 96.- El fiador o avalista que pague adquiere los derechos derivados del título valor, físico, desmaterializado o electrónico, contra la persona garantizada y contra los que sean responsables respecto de esta última por virtud del título."

Art. 54.- En el artículo 84, al final del penúltimo inciso, agréguese lo siguiente:

"Aquellos títulos valores desmaterializados o electrónicos que no se negocien en el mercado de valores, podrán utilizar cualquier tipo de tecnología y sistema tecnológico como forma probatoria de la existencia de los valores electrónicos o desmaterializados, conforme a los principios de neutralidad tecnológica, equivalencia funcional y autonomía de las partes.

Los títulos electrónicos emitidos por los bancos a través de la aceptación de cualquier medio calificado son distintos a los a los títulos desmaterializados."

Art. 55.- En el artículo 109, luego de la frase: "El endoso de títulos valores desmaterializados", agréguese la frase: "negociables en el mercado de valores".

Art. 56.- En el artículo 112 realícese los siguientes cambios:

a. Reemplácese el segundo inciso por el siguiente:

"En el caso de títulos valor electrónicos se seguirán las reglas del anterior inciso y las disposiciones sobre posesión en títulos valor contenidas en la Ley de Comercio Electrónico. Para aquellos títulos valores que se negocien en el mercado de valores seguirán las reglas de la Ley de Mercado de Valores y regulaciones conexas."

b. Agréguese como tercer inciso lo siguiente:

"En el endoso, cesión, transmisión de derechos y de documentos, notificación o entrega de títulos electrónicos, se podrá utilizar medios electrónicos, telemáticos y firmas manuscritas o electrónicas."

Art. 57.- A continuación del artículo 112, agréguese el siguiente artículo innumerado:

"**Artículo (...).- Reconocimiento jurídico de los títulos valor electrónicos**.- Se reconoce igual validez jurídica y efectos jurídicos a los títulos valor electrónicos respecto de los emitidos en papel, siempre que cumplan con los requisitos legales contenidos en el presente Código, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento, y demás normativa aplicable.

No se negarán efectos jurídicos, validez ni fuerza ejecutoria a un título valor por la sola razón de que esté en forma electrónica. Los títulos valor al portador no serán susceptibles de emitirse ni existir de manera electrónica."

Art. 58.- Después del artículo 113, agréguese el siguiente artículo innumerado:

"

Art. (...).- La firma de quien cede o avala una letra de cambio podrá realizarse por medio de firma electrónica, la cual tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita, de acuerdo con lo establecido en la ley."

Art. 59.- Sustitúyase el artículo 126 por el siguiente:

"Artículo 126.- El endoso deberá constar en la letra de cambio o en un documento adherido a la misma, en físico o electrónico o anexo accesible mediante un enlace electrónico directo o mediante cualquier tecnología fiable. Deberá ser firmado física o

electrónicamente por el endosante.

El endoso será válido aun cuando en él no se designe la persona a cuyo favor se haga, o cuando el endosante se hubiera limitado a poner su firma en el dorso de la letra o en una hoja adherida a la misma (endoso en blanco).”

Art. 60.- Después del artículo 189, agréguese el siguiente:

“

Art. (...).- La firma de quien suscribe, endosa, cede o avala un pagaré a la orden, podrá realizarse por medio de firma electrónica, la cual tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita, de acuerdo con lo establecido en la ley.”

Art. 61.- Agréguese un segundo inciso en el artículo 272 con el siguiente texto:

“En la cesión o transmisión de derechos, obligaciones, contratos, deudas y documentos mercantiles, entrega de títulos y documentos, se podrá utilizar medios electrónicos o telemáticos y firmas manuscritas o electrónicas.”

Título V
REFORMAS A LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

Art. 62.- A continuación del artículo 11, añádase el siguiente artículo innumerado:

“Artículo (...).- La posesión en los títulos valor electrónicos.- Cuando por ley se requiera o permita la posesión de un título valor, tal requisito se dará por cumplido respecto de los títulos valor electrónicos si se utiliza un método fiable:

1. Para determinar qué ese título valor electrónico está bajo el control exclusivo de una persona; y,
2. Para identificar a dicha persona como la persona que tiene el control sobre el título valor electrónico.

Cuando por ley se requiera o permita que se transfiera la posesión de un título valor, tal requisito se cumplirá con respecto de los títulos valor electrónicos mediante la transferencia del control del mismo.

En el caso de que se empleen sistemas para la gestión de los títulos valor electrónicos, como los basados en registros descentralizados, que identifiquen a la persona que ejerce el control empleando seudónimos o cualquier mecanismo que no sea directamente el nombre verdadero, esta forma de identificación, y la posibilidad de vincular el seudónimo

al nombre verdadero, de ser necesario, permitirá cumplir el requisito de identificar a la persona que tiene el control conforme el numeral 2 del presente artículo. En el caso de que se utilice un seudónimo la persona que se encuentra en poder del título valor debe ser plenamente identificable."

Art. 63.- Veracidad de la firma electrónica dentro de distintos tipos de procedimiento.- La autoridad a cargo de la resolución de un proceso, cualquiera que sea su índole, en el caso de que tenga dudas fundamentadas al respecto de la veracidad de la firma electrónica contenida en un documento sometido a su consideración, deberá proceder a la verificación de la veracidad de la firma electrónica estampada en un documento electrónico.

Para el efecto, el ente rector en materia de telecomunicaciones dispondrá el software adecuado que utilizarán las autoridades con capacidad resolutoria para dar cumplimiento a lo previsto en este artículo. El ente regulador en materia de telecomunicaciones deberá fundamentar la determinación de cuál será el software adecuado a través de la aplicación del principio de neutralidad funcional de la tecnología y estándares y buenas prácticas internacionales.

Título VI
REFORMAS A LA LEY NOTARIAL

Art. 64.- Sustitúyase el contenido del artículo 5 por el siguiente:

"

Art. 5.- Para el ejercicio de la función notarial, así como la prestación de su servicio, serán hábiles todos los días y horas del año.

Todos los servicios notariales serán prestados de manera física o telemática de conformidad con lo previsto en la ley; en el caso de prestación telemática, se realizará a través de medios compatibles con el sistema informático autorizado por el Consejo de la Judicatura. El Consejo de la Judicatura autorizará sistemas digitales cumpliendo con los principios de equivalencia funcional de la tecnología y neutralidad tecnológica y acatando las directrices emitidas por el Consejo de la Judicatura. Las y los solicitantes de servicios notariales expresarán formalmente la modalidad para la prestación del servicio.

Los servicios telemáticos serán prestados a través de videoconferencia u otro medio telemático compatible con el sistema informático autorizado por el Consejo de la Judicatura de acuerdo con la naturaleza del acto o contrato, debiendo encontrarse una de las partes en la circunscripción territorial del notario y, pudiendo las demás encontrarse en cualquier lugar. Si no fuere factible prestar el servicio notarial telemático y las partes no pudieren concurrir al despacho notarial, el notario podrá desplazarse a prestar su servicio fuera de su despacho en forma física, dentro de su circunscripción cantonal."

Art. 65.- Suprímase el numeral 4 del artículo 18.2.

Art. 66.- Sustitúyase el numeral 6 del artículo 18.2 por el siguiente:

"6. Autenticación de firmas manuscritas puestas ante él o ella, en documentos que no sean escrituras públicas."

Art. 67.- Inclúyase el siguiente inciso al final del artículo 22:

"Los protocolos digitales de las diligencias y actuaciones notariales telemáticas deberán contar con todas las medidas de ciberseguridad necesarias para garantizar la seguridad de la información que reposa en ellos, así como su confidencialidad, integridad y disponibilidad, incluyendo las garantías de protección de datos personales, de conformidad con la normativa vigente y las directrices que para el efecto emita el ente rector de transformación digital y otros organismos competentes."

Art. 68.- Sustitúyase el inciso final del artículo 28 por el siguiente:

"En la prestación del servicio notarial telemático la notaría o el notario verificará el cumplimiento de las obligaciones previstas en el artículo 27 de esta Ley, priorizando al empleo de la tecnología, para garantizar los principios de celeridad, eficiencia, seguridad de la información y transparencia en el servicio."

Art. 69.- Suprímase el numeral 10 del artículo 29.

Título VII
REFORMAS AL CÓDIGO ORGÁNICO GENERAL DE PROCESOS

Art. 70.- Refórmese el artículo 4 con la siguiente redacción:

"La sustanciación de los procesos en todas las instancias, fases y diligencias se desarrollarán mediante el sistema oral, salvo los actos procesales que deben realizarse por escrito. Las audiencias también podrán realizarse por videoconferencia u otros medios telemáticos, la o el juzgador negará la comparecencia telemática de manera excepcional y únicamente cuando se justifique la imperiosa necesidad de que esta sea de manera personal.

La o el juzgador está obligado a justificar de manera motivada la negativa de la comparecencia telemática."

Art. 71.- Refórmense los incisos segundo y cuarto del artículo 25 con los siguientes textos, respectivamente:

"Una vez citada la recusación se suspenderá la competencia del juez conforme al Código Orgánico General de Procesos y su citación será única y exclusivamente al correo institucional de la o el juzgador recusado, salvo cuando se fundamente en el retardo injustificado, en cuyo caso sólo se suspenderá la competencia cuando la recusación haya sido admitida.

Si la recusación se presenta contra todos los miembros de una sala o tribunal, la autoridad competente determinará a las o los juzgadores que deberán continuar con la causa principal. La citación también será única y exclusivamente al correo institucional de las o los juzgadores recusados."

Art. 72.- Sustitúyase el artículo 53 por el siguiente:

"La citación es el acto por el cual se le hace conocer a la o al demandado, el contenido de la demanda o de la petición de una diligencia preparatoria y de las providencias recaídas en ellas. Se realizará en forma personal, mediante boletas físicas o electrónicas, o a través del medio de comunicación ordenado por la o el juzgador.

Si una parte manifiesta que conoce determinada petición o providencia o se refiere a ella en escrito o en acto del cual quede constancia en el proceso, se considerará citada o notificada en la fecha de presentación del escrito o en la del acto al que haya concurrido.

Toda citación será publicada de manera íntegra, esto es, con sus razones y actas de citación en el sistema automático de consultas de la página electrónica del Consejo de la Judicatura, a través de los medios electrónicos y tecnológicos de los que disponga la Función Judicial, en la que constará la forma de citación o los motivos por los cuales no se pudo efectuar dicha diligencia.

Si la o el actor ha proporcionado la dirección de correo electrónico de la o del demandado, la o el juzgador ordenará también que se le haga conocer a la o al demandado, por correo electrónico, el extracto de la demanda y del auto inicial, de lo cual, se dejará constancia en el sistema. Esto no sustituye a la citación oficial, salvo los casos previstos por este Código."

Art. 73.- Agréguese continuación del artículo 55, el siguiente artículo:

"Artículo 55.1- Citación por boletas en el domicilio electrónico.- A las personas naturales o jurídicas que hayan pactado expresamente en un contrato un domicilio electrónico para citaciones se les citará en las direcciones de correo electrónico. La citación se realizará conforme las reglas de la citación telemática previstas a continuación del numeral 3 del tercer párrafo del artículo 55.

El actuario del despacho que proceda a la citación por boletas en el domicilio electrónico,

procederá a dejar constancia de las boletas de citación y las razones de las mismas, so pena de las sanciones administrativas que correspondan.”

Art. 74.- Sustitúyase el artículo 55 por el siguiente:

“Citación por boletas y por boletas electrónicas.- Si no se encuentra personalmente a la o el demandado, se le citará por medio de tres boletas que se entregarán en días distintos y seguidos en su domicilio, residencia, lugar de trabajo o asiento principal de sus negocios a cualquier persona de la familia. Si no se encuentra a persona alguna a quien entregarlas, se fijarán en la puerta del lugar de habitación, de este particular el citador dejará constancia fotográfica adjunta a las actas de citación.

La citación por boletas a la o al representante legal de una persona jurídica se hará en el respectivo establecimiento, oficina o lugar de trabajo, en días y horas hábiles, entregándolas a uno de sus dependientes o empleados, previa constatación de que se encuentra activo. De no encontrarse persona alguna o no recibir respuesta en los lugares detallados en el presente inciso, el citador procederá a dejar las boletas de citación fijadas en la puerta o debajo de esta, o en un sitio de visible del establecimiento, para lo cual deberá fotografiar su diligencia y adjuntarla a sus actas de citación.

A quien no se les pueda encontrar personalmente o cuyo domicilio o residencia sea imposible determinar previo a citar por la prensa, se le podrá citar de forma telemática por boletas bajo las siguientes reglas:

1. A las personas naturales en el buzón electrónico ciudadano previsto por la ley, una vez que lo hayan abierto.
2. A los procuradores judiciales que hayan incluido un correo electrónico dentro del poder, siempre que la o el accionante acredite que el procurador judicial accionado cuenta con poder vigente y con capacidad para contestar demandas.
3. A las personas jurídicas sometidas al control de la Superintendencia de Compañías, Valores y Seguros; Superintendencia de Bancos; y, Superintendencia de Economía Popular y Solidaria, a través del correo electrónico que se encuentre registrado en el ente de control.

La citación telemática se realizará con el envío de tres boletas de citación al demandado, en tres días distintos y seguidos, desde la cuenta institucional del actuario de la judicatura. A la citación por correo electrónico se adjuntará la demanda o la petición de una diligencia preparatoria y las providencias recaídas en ellas. El actuario del despacho que proceda a la citación por boletas en el domicilio electrónico, procederá a dejar constancia de las boletas de citación y las razones de las mismas, bajo pena de las sanciones administrativas que correspondan. La constancia y certificación de haberse practicado la citación telemática será agregada al expediente.

Dicha constancia deberá incluir tanto los correos electrónicos enviados, así como la verificación de recepción o lectura. Para el cumplimiento de la citación telemática, no será necesaria la generación de exhortas, deprecatorios o comisiones."

Art. 75.- Refórmese el artículo 115 con el siguiente texto:

"Es el medio informático en el cual se registran las actuaciones judiciales. En el expediente electrónico se deben almacenar las peticiones y documentos que las partes pretendan utilizar en el proceso y que será público en todo su contenido, salvo las excepciones previstas en las leyes.

Las reproducciones digitalizadas o escaneadas de documentos públicos o privados que se agreguen al expediente electrónico tienen la misma fuerza probatoria del original.

Los expedientes electrónicos deben estar protegidos por medio de sistemas de seguridad de acceso y almacenados en un medio que garantice la preservación e integridad de los datos.

El expediente electrónico contendrá lo siguiente:

1. Providencias judiciales dadas durante la prosecución del proceso.
2. Escritos y diligencias debidamente digitalizadas.
3. Actas de citación.
4. Actuaciones dadas en el marco de los artículos 116, 117, 118 y 119 de este Código."

Art. 76.- Sustitúyase el artículo 193 por el siguiente:

"

Art. 193.- Prueba documental.- Es todo documento público o privado que recoja, contenga o represente algún hecho o declare, constituya o incorpore un derecho.

Se podrán desglosar los documentos sin perjuicio de que se vuelvan a presentar cuando sea requerido.

Cuando se trate de documentos electrónicos o desmaterializados, no se requerirá su materialización."

Art. 77.- Sustitúyase el artículo 194 por el siguiente:

"

Art. 194.- Presentación de documentos.- Los documentos públicos o privados se presentarán en originales o en copias.

Se considerarán copias las reproducciones del original, debidamente certificadas que se realicen por cualquier sistema.

Los documentos electrónicos o desmaterializados, no requerirán ser materializados para su validez."

Art. 78.- Sustitúyase el artículo 196 por el siguiente:

"

Art. 196.- Producción de la prueba documental en audiencia.- Para la producción de la prueba documental en audiencia de juicio o única se procederá de la siguiente manera:

1. Los documentos se leerán y exhibirán públicamente en su parte pertinente. En el caso de los documentos electrónicos o desmaterializados, la exhibición se realizará por los medios tecnológicos idóneos. No será necesaria su materialización.
2. Los objetos se exhibirán públicamente.
3. Las fotografías, grabaciones, los elementos de pruebas audiovisuales, computacionales o cualquier otro de carácter electrónico apto para producir fe, se reproducirá también en su parte pertinente en la audiencia y por cualquier medio idóneo para su percepción por los asistentes.
4. La prueba documental actuada quedará en poder de la o del juzgador para tenerla a la vista al momento de tomar su decisión sobre el fondo del asunto, dejando a salvo la facultad de las partes de volver actuar o usarla durante la audiencia de juicio. Los documentos electrónicos o desmaterializados, se entregarán en los soportes tecnológicos idóneos.

Cuando la sentencia haya quedado firme, se ordenará su devolución a las partes, dejando a salvo su derecho a solicitar que los documentos agregados al proceso le sean desglosados dejando en el expediente copias certificadas, sean estas digitales o no.

Una vez que la sentencia haya sido ejecutada y digitalizados los documentos físicos agregados al proceso, se comunicará a las partes de su obligación de retirarlos, advirtiendo que en caso de no hacerlo en el término de treinta días, estos serán destruidos."

Art. 79.- Reemplácese el contenido del artículo 347 por el siguiente:

"

Art. 347.- Títulos ejecutivos.- Son títulos ejecutivos siempre que contengan obligaciones de dar o hacer:

1. Declaración de parte hecha con juramento ante una o un juzgador competente.
2. Copia y la compulsa auténticas de las escrituras públicas.

3. Documentos privados legalmente reconocidos ante notario, reconocidos por decisión judicial, o con firma electrónica verificada ante autoridad judicial.
4. Letras de cambio físicas, desmaterializadas y electrónicas.
5. Pagarés a la orden, físicos, desmaterializados y electrónicos.
6. Testamentos.
7. Transacción extrajudicial.
8. Contratos de mutuo, cuya aceptación de la voluntad se haya dado por medios físicos u electrónicos de conformidad con la normativa especial.

Los demás a los que otras leyes otorguen el carácter de títulos ejecutivos."

Art. 80.- Reemplácese el numeral 10 del artículo 363 por el siguiente:

"10. La hipoteca, abierta o cerrada."

Art. 81.- Agréguese a continuación del numeral 7 del artículo 373 el siguiente numeral:

"8. Excepción de existencia de convenio arbitral para los casos del artículo 363 numerales 3, 4, 6, 7 y 10."

Art. 82.- Reemplácese el texto del artículo 405 por el siguiente:

"

Art. 405.- Retasa y embargo de otros bienes.- En el caso en que no haya postores, la o el acreedor podrá solicitar las retasas que sean necesarias de los bienes embargados y se reanudará el proceso de remate con el nuevo avalúo o pedir que se embarguen y rematen otros bienes liberando los bienes anteriormente embargados.

Si el valor ofrecido al contado no alcanza a cubrir el crédito de la o del ejecutante o el de la o del tercerista, podrán pedir, a su arbitrio, que se rematen como créditos los dividendos a plazo."

Título VIII
REFORMAS A LA LEY DE REGISTRO

Art. 83.- Agréguese a continuación del literal g) del artículo 11, el siguiente:

"h) Desarrollar e implementar los sistemas informáticos que permitan la transformación a formato digital de todos los registros, certificados, inventarios y demás actos o constancias físicas que genere el Registro para lo cual deberá tomar en cuenta las características y condiciones que para dicha finalidad emita la Dirección Nacional de Registros Públicos (DINARP) como ente rector de la actividad registral. El sistema informático permitirá y promoverá la interconexión progresiva entre los distintos registros

de la propiedad del país, que permita el acceso y consulta de los ciudadanos desde distintas jurisdicciones a una base de datos integrada, y se acompañará con un plan progresivo de digitalización para los cantones que no cuenten con los registros, certificados, inventarios, negocios jurídicos y demás actos o constancias digitalizadas.

Serán los Gobiernos Autónomos Descentralizados Municipales quienes deberán asignar los fondos necesarios para llevar a cabo este proceso en aquellos registros que no tengan autonomía financiera y administrativa."

Art. 84.- Sustitúyase el literal c) del artículo 11, el siguiente artículo:

"c) Llevar, con sujeción a las disposiciones de esta Ley, los libros denominados Registro de Propiedad, Registro de Gravámenes, Registro Mercantil, Registro de Interdicciones y Prohibiciones de enajenar y los demás que determine la ley.

Los libros a cargo del Registrador podrán llevarse de forma electrónica y automatizada siempre que garanticen la seguridad jurídica, publicidad y la legalidad de los derechos constituidos en los actos, contratos y negocios jurídicos de las personas. Las bases de datos y los sistemas informáticos implementados estarán sujetos al control y auditoría del ente rector de la actividad registral.

Los registros digitales que se generen como consecuencia de la transformación a la que se refiere este literal, así como todos los registros digitales que existan al momento o que se generen en el futuro, deberán contar con todas las medidas de ciberseguridad necesarias para garantizar la seguridad de la información que reposa en ellos, así como su confidencialidad, integridad y disponibilidad, incluyendo las garantías de protección de datos personales, de conformidad con la normativa vigente y las directrices que para el efecto emita el ente rector de transformación digital y otros organismos competentes."

Art. 85.- Agréguese en el artículo 18, el siguiente texto:

"El Libro Repertorio podrá llevarse de forma electrónica en aquellos Registros que implemente un proceso de digitalización y automatización de los trámites registrales a su cargo. Para lo cual el proceso electrónico de registro en este Libro debe llevarse con sujeción al presente artículo."

Art. 86.- Agréguese a continuación del artículo 24, en el TÍTULO V, el siguiente artículo innumerado:

"

Art. (...).- Los registros de las inscripciones y el libro de índice general podrán llevarse de forma electrónica, para lo cual se tomarán en consideración y serán adaptados todos los procedimientos contemplados en la presente Ley para los registros físicos de los documentos."

Título IX
REFORMAS A LA LEY DE COMPAÑÍAS

Art. 87.- Reemplácese el artículo 6 por el siguiente:

"

Art. 6.- Toda compañía nacional o extranjera que negocie o contrajere obligaciones en el Ecuador deberá tener en la república un apoderado o representante que pueda contestar las demandas y cumplir las obligaciones respectivas.

Sin perjuicio de lo que se dispone en el artículo 415, si las actividades que una compañía extranjera va a ejercer en el Ecuador implicaren la ejecución de obras públicas, la prestación de servicios públicos o la explotación de recursos naturales del país, estará obligada a establecerse en él con arreglo a lo dispuesto en la Sección XIII de la presente Ley.

En los casos mencionados en el inciso anterior, las compañías u otras empresas extranjeras organizadas como personas jurídicas, deberán domiciliarse en el Ecuador antes de la celebración del contrato correspondiente. El incumplimiento de esta obligación determinará la nulidad del contrato respectivo.

Las compañías extranjeras, cuyos capitales sociales estuvieren representados únicamente por acciones o participaciones nominativas, que tuvieren acciones o participaciones en compañías ecuatorianas, pero que no ejercieren ninguna otra actividad empresarial en el país, ni habitual ni ocasionalmente, no serán consideradas con establecimientos permanentes en el país ni estarán obligadas a establecerse en el Ecuador con arreglo a lo dispuesto en la Sección XIII de la presente Ley, ni a inscribirse en el Registro Único de Contribuyentes ni a presentar declaraciones de impuesto a la renta, pero deberán tener en la república el apoderado, representante referido en el inciso primero de este artículo, o un curador dativo que será nombrado por un juez en caso de ser necesario, el que por ningún motivo será personalmente responsable de las obligaciones de la compañía extranjera antes mencionada. El poder del representante antedicho no deberá ni inscribirse ni publicarse por la prensa, pero sí deberá ser conocido por la compañía ecuatoriana en que la sociedad extranjera fuere socia o accionista."

Art. 88.- Refórmese el artículo 188 de la siguiente manera:

"La transferencia de acciones comporta la cesión de todos los derechos y obligaciones inherentes a ellas.

La propiedad de las acciones se transfiere mediante cesión celebrada entre cedente y cesionario, fuere personalmente o por quienes los representaren. La transferencia de

acciones podrá instrumentarse por escrito o por cualquier medio electrónico verificable que demuestre la voluntad del cedente y cesionario de transferir la propiedad de las acciones.

De efectuarse una cesión por escrito, la misma podrá hacerse constar en el título correspondiente o en una hoja adherida al mismo. En aquel caso, el cedente deberá entregar los títulos de acción correspondientes al cesionario.

Las transferencias de acciones, efectuadas por medios físicos o electrónicos, surtirán efectos entre el cedente y el cesionario a partir de su celebración, realizada de conformidad con lo previsto en este artículo. Por su parte, la tradición de dicha transferencia, así como su oponibilidad frente a la compañía y terceros, se efectuará a partir de la correspondiente inscripción en el Libro de Acciones y Accionistas, de acuerdo con el artículo siguiente.

Para los títulos que estuvieren entregados en custodia en un depósito centralizado de compensación y liquidación, la cesión podrá hacerse de conformidad con los mecanismos que se establezcan para tales depósitos centralizados.

El cedente, en una transferencia física o electrónica, podrá reservarse los beneficios económicos generados durante períodos anteriores a la cesión o los que se generen en el período económico en que se efectúe la transferencia. Esta reserva deberá constar expresamente en el respectivo contrato de cesión.

Será lícita la celebración de un contrato de promesa de cesión de acciones, a través de medios físicos o electrónicos. En este caso, se observarán los requisitos exigidos por el Código Civil. El cónyuge a cuyo cargo está la administración ordinaria de los bienes sociales necesitará de la autorización expresa del otro cónyuge para realizar actos de disposición, limitación, constitución de gravámenes de las acciones y participaciones mercantiles que pertenezcan a la sociedad conyugal.

Serán nulas las transferencias realizadas con violación de lo que dispone el presente artículo sin que, por consiguiente, el cesionario pueda ejercer ninguno de los derechos que le otorga esta Ley al accionista.”

DISPOSICIONES GENERALES

Primera.- El Ministerio de Economía y Finanzas coordinará con el Consejo de la Judicatura para que, dentro de su asignación presupuestaria, se proceda a la plena implementación del expediente electrónico en el plazo de noventa (90) días contados desde la entrada en vigencia de esta Ley.

Segunda.- El Consejo de la Judicatura, dentro del marco de sus competencias y en apego a las disposiciones que rigen para la coordinación interinstitucional, deberá solicitar apoyo técnico a la Corte Constitucional para la plena implementación del expediente electrónico, bajo los parámetros definidos en esta Ley para dicha herramienta tecnológica.

Tercera.- Los procedimientos sustanciados a través del Código Orgánico Administrativo y de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, en lo que resulte aplicable, deberán observar las reformas establecidas en esta Ley al Código Orgánico General de Procesos.

DISPOSICIONES TRANSITORIAS

Primera.- En un plazo máximo de noventa (90) días contados desde la entrada en vigencia de esta Ley, el Consejo de la Judicatura deberá implementarlos sistemas informáticos que sean necesarios para la correcta e inmediata aplicación de los expedientes electrónicos.

Segunda.- El Ministerio de Educación tendrá un plazo máximo de noventa (90) días contados desde la entrada en vigencia de esta Ley, para emitir o actualizar las normativas relacionadas al desarrollo virtual de las clases de escuelas y colegios.

Tercera.- El Consejo de Educación Superior tendrá un plazo máximo de noventa (90) días contados desde la entrada en vigencia de esta Ley, para emitir o actualizar las normativas relacionadas a lo previsto en la transformación digital de las mallas curriculares.

Cuarta.- El Ministerio de Educación tendrá un plazo máximo de noventa (90) días contados desde la entrada en vigencia de esta Ley, para emitir o actualizar las normativas relacionadas al desarrollo virtual de las clases de escuelas y colegios.

Quinta.- El Presidente de la República, dentro de los noventa (90) días posteriores a la publicación de la presente Ley en el Registro Oficial, actualizará la normativa vigente, así como emitirá el Reglamento correspondiente, para viabilizar la aplicación de lo previsto en esta Ley.

Sexta.- En un plazo de ciento veinte (120) días posteriores a la publicación de la presente Ley en el Registro Oficial, el Ministerio de Telecomunicaciones deberá implementar el software adecuado que utilizarán las autoridades para la validación administrativa de firmas electrónicas. La referida contratación deberá basarse en el principio de neutralidad tecnológica, interoperabilidad y equivalencia funcional de la tecnología.

Séptima.- En el plazo máximo de ciento ochenta (180) días posteriores a la publicación de la presente Ley en el Registro Oficial, se presentará ante el Pleno de la Asamblea Nacional, un informe detallado del seguimiento y evaluación de la presente Ley, así como de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, producto de lo cual se resolverá conforme se estime conveniente.

Octava.- El monto de Certificados de Inversión Audiovisual que deberá otorgarse para el año 2023, será de al menos 1000 fracciones básicas exentas de impuesto a la renta.

DISPOSICIÓN FINAL

Única.- La presente Ley tiene el carácter de especial, prevalecerá sobre otras leyes especiales y generales que se le opongan.

Las disposiciones de la presente Ley entrarán en vigencia a partir de la fecha de su publicación en el Registro Oficial, salvo lo previsto en las disposiciones transitorias.

Dada en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de Quito, provincia de Pichincha a los treintaiún días del mes de enero del año dos mil veintitrés.

FUENTES DE LA PRESENTE EDICIÓN DE LA LEY ORGÁNICA PARA LA TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL

1.- Ley s/n (Tercer Suplemento del Registro Oficial 245, 07-II-2023).

2.- Codificación de la Ley Orgánica de Educación Intercultural (Quinto Suplemento del Registro Oficial 689, 22-XI-2024).

3.- Ley Orgánica para el Fortalecimiento de la Ciberseguridad (Quinto Suplemento del Registro Oficial 290, 22-V-2026)