QUINTO SUPLEMENTO

REGISTRO OFICIAL®
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD

Año II - Nº 290 - 104 páginas
Quito, viernes 22 de mayo de 2026

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

Oficio Nro. AN-SG-2026-0305-O

Quito, D.M., 19 de mayo de 2026

Asunto: Publicación de la "LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD"

Señorita Magíster
Martha Jaqueline Vargas Camacho
Directora del Registro Oficial
CORTE CONSTITUCIONAL DEL ECUADOR
En su Despacho

De mi consideración:

El Pleno de la Asamblea Nacional, de conformidad con lo previsto en los artículos 120 numeral 6 de la Constitución de la República del Ecuador y 9 numeral 6 de la Ley Orgánica de la Función Legislativa, trató el proyecto de "**LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD**" de acuerdo con el siguiente detalle:

1. Primer debate: 5 de agosto de 2025 (Sesión Nro. 024-AN-2025-2029);
2. Segundo debate: 10 de febrero de 2026 (Sesión Nro. 069-AN-2025-2029);
3. Fecha de aprobación: 10 de febrero de 2026 (Sesión Nro. 069-AN-2025-2029).
4. Fecha de la objeción presidencial: 13 de marzo de 2026;
5. Fecha de tratamiento y aprobación de la objeción presidencial: 31 de marzo de 2026 (Sesión Nro. 082-AN-2025-2029).

En la sesión Nro. 082-AN-2025-2029 de 31 de marzo de 2026, el Pleno de la Asamblea Nacional conoció y resolvió respecto del "Informe No Vinculante sobre la Objeción Parcial al Proyecto de **LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD"**, bajo la siguiente moción:

"*Allanarse a la objeción parcial por inconveniencia al Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, específicamente respecto al artículo 6 que comprende los artículos 20-A, 20-Q, 20-S, 20-T, 20-U y 20-X; así como al artículo 13 y de la Disposición General Primera del referido proyecto.*"

Moción que fue aprobada por el Pleno de la Asamblea Nacional, en la referida sesión.

Mediante oficio No. T.368-SGJ-26-0137 de 13 de mayo de 2026, el Secretario General Jurídico de la Presidencia de la República, Enrique Herrería Bonnet, informó a la Asamblea Nacional que:

"[...] *mediante Oficio No. T.368-SGJ-26-0136, de 13 de mayo de 2026, se remitió al Registro Oficial, para su respectiva publicación, la Disposición Transitoria Sexta de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad, de conformidad con lo dispuesto en el artículo 64 de la Ley Orgánica de la Función Legislativa y con la certificación emitida el 13 de abril de 2026 por el señor Jorge López Terán, Prosecretario General de la Asamblea Nacional, cuya parte pertinente señala:*

[…] ***el Pleno de la Asamblea Nacional no consideró la objeción parcial por inconveniencia a la Disposición General Sexta del proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad****, formulada por el señor Presidente de la República del Ecuador, ingeniero Daniel Noboa Azín, a través del oficio No. T.368-SGJ-26-0061, de fecha 12 de marzo de 2026, ingresado en el sistema de gestión documental de la Asamblea Nacional con número de trámite interno 478636, el día 13 de marzo de 2026. […] (énfasis añadido).* (sic)".

Por consiguiente, y en atención a los artículos 138 de la Constitución de la República del Ecuador y 64 de la Ley Orgánica de la Función Legislativa, se remite para su publicación en el Registro Oficial: (i) texto auténtico del proyecto de "Ley Orgánica para el Fortalecimiento de la Ciberseguridad"; (ii) la certificación de la Secretaría General, respecto de las fechas en las que el Pleno de la Asamblea Nacional realizó el tratamiento del proyecto de ley; (iii) la certificación de la Secretaría General respecto de la no consideración de la objeción parcial por inconveniencia a la Disposición General Sexta del proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad; (iv) la moción de allanamiento a la objeción parcial al proyecto de "Ley Orgánica para el Fortalecimiento de la Ciberseguridad"; (v) el oficio No. T.368-SGJ-26-0137 de 13 de mayo de 2026, suscrito por el Secretario General Jurídico de la Presidencia de la República; y, (vi) el oficio No.

T.368-SGJ-26-0136 de 13 de mayo de 2026, signado por el Secretario General Jurídico de la Presidencia de la República.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Sr. Giovanny Francisco Bravo Rodríguez
SECRETARIO GENERAL

Anexos:
- 1__texto_base_-_ley_de_ciberseguridad_op-signed-signed04877200017774874 54.pdf
- certif-op_lofc_--signed0830842001779141089.pdf
- an-abim-2026-0069-m_(2).pdf
- 481068-1.oficio_no._t.368-sgj-26-0137-1.pdf
- 481068-anexo_2__oficio_no__t_368-sgj-26-01360582459001779141141.pdf
- 2.certificacioÌn_-_ley_orgánica_para_el_fortalecimiento_de_la_ciberseguridad_op-signed.pdf

Copia:

Señor Máster
Niels Anthonez Olsen Peet
Presidente de la Asamblea Nacional

Señor Abogado
Jorge Enrique López Terán
Prosecretario General

Señor Doctor
Pablo Enrique Herreria Bonnet
Secretario General Jurídico
PRESIDENCIA DE LA REPÚBLICA

do

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
GIOVANNY FRANCISCO
BRAVO RODRIGUEZ

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

CERTIFICACIÓN

En mi calidad de Secretario General de la Asamblea Nacional, **CERTIFICO** que, el proyecto de "**LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD**", fue tratado por el Pleno de la Asamblea Nacional, de acuerdo con el siguiente detalle:

1. Primer debate: 5 de agosto de 2025 (Sesión Nro. 024-AN-2025-2029);
2. Segundo debate: 10 de febrero de 2026 (Sesión Nro. 069-AN-2025-2029);
3. Fecha de aprobación: 10 de febrero de 2026 (Sesión Nro. 069-AN-2025-2029).
4. Fecha de la objeción presidencial: 13 de marzo de 2026;
5. Fecha de tratamiento y aprobación de la objeción presidencial: 31 de marzo de 2026 (Sesión Nro. 082-AN-2025-2029).

Quito, 19 de mayo de 2026.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
GIOVANNY FRANCISCO BRAVO RODRIGUEZ

GIOVANNY FRANCISCO BRAVO RODRÍGUEZ
Secretario General

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

Oficio No. T.368-SGJ-26-0061

Guayaquil, 12 marzo de 2026

Señor Magíster
Niels Anthonez Olsen Peet
PRESIDENTE DE LA ASAMBLEA NACIONAL
En su Despacho. –

De mi consideración:

Mediante Oficio Nro. AN-SG-2026-0095-O de 11 de febrero de 2026, la Asamblea Nacional remitió a la Presidencia de la República el proyecto de **"LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD"**, discutido y aprobado en segundo debate de 10 de febrero de 2026, para la correspondiente sanción u objeción presidencial.

En ejercicio de las potestades conferidas por los artículos 137 y 138 de la Constitución de la República, notifico a usted y, por su intermedio, a la Asamblea Nacional con la siguiente **OBJECIÓN PARCIAL POR INCONVENIENCIA** al referido proyecto de ley, en los siguientes términos:

I
OBJECIÓN AL ARTÍCULO 6

(i) Artículo 20-A

1. El artículo 20-A, contenido en el artículo 6 del proyecto de ley, señala lo siguiente:

> Artículo 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-J**; 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). (énfasis añadido)

2. A continuación, se expone el argumento que fundamenta la objeción parcial por inconveniencia:

2.1. La disposición analizada establece que las normas del título denominado "DE LA CIBERSEGURIDAD", les serán aplicables a 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-J**.

2.2. Es decir, define el ámbito de aplicación del régimen de ciberseguridad respecto de los prestadores de servicios digitales, condicionando su alcance al principio de responsabilidad compartida.

2.3. Sin embargo, el artículo 20-A hace remisión al artículo 20-J, el cual establece la obligación de coordinación que tienen las entidades públicas y los operadores de infraestructura crítica digital con la autoridad competente, en tanto establece:

Artículo 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.

2.4. Por el contrario, el **artículo 20-I** efectivamente hace alusión a las responsabilidades que tienen los prestadores de servicios digitales a fin de garantizar el cumplimiento de la ley, de conformidad con el principio de responsabilidad compartida, estableciendo: i) medidas técnicas y organizativas; ii) evaluación y gestión de riesgos; iii) cooperación para gestión de incidentes; etc.

2.5. En consecuencia, la remisión al artículo 20-J resulta técnicamente incorrecta por cuanto no guarda relación con el alcance de las obligaciones derivadas del principio de responsabilidad compartida.

3. En tal virtud, y con el propósito de optimizar la claridad y técnica normativa del texto, propongo la siguiente alternativa:

> Artículo 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).

(ii) Artículo 20-Q

4. El artículo 20-Q, contenido en el artículo 6 del proyecto de ley, señala:

> Artículo 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-J** 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." (énfasis añadido)

5. Al tratarse de materia sancionadora, la norma debe prever de manera clara y expresa no solo las conductas que configuran una infracción administrativa o los sujetos responsables por dichas conductas —aspectos que efectivamente se encuentran determinados en el proyecto de ley— sino también el alcance de esta responsabilidad administrativa.

5.1. La disposición bajo análisis establece la responsabilidad administrativa que se origina como producto del incumplimiento de las disposiciones contenidas en el referido Título. Esta disposición es una norma estructural del régimen administrativo sancionador en virtud de que delimita aspectos como: sujetos responsables y el alcance material de su responsabilidad.

5.2. En este sentido, el literal b) dispone que los prestadores de servicios digitales serán responsables administrativamente, exclusivamente en lo relativo a los elementos bajo su esfera de control, conforme al **artículo 20-J** y al principio de responsabilidad compartida.

5.3. No obstante, la remisión al artículo 20-J resulta incorrecta, de acuerdo con lo expuesto en el artículo 20-A.

5.4. En consecuencia, esta inconsistencia constituye un defecto técnico que podría comprometer la correcta aplicación del régimen sancionador y generar inseguridad jurídica.[1]

6. Con el objeto de optimizar la redacción y precisión del texto normativo, se propone lo que sigue:

> Artículo 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.

(iii) Artículo 20-S

7. El artículo 20-S, contenido en el artículo 6 del proyecto de ley, señala:

> Artículo 20-S.- Sanciones por infracciones leves. - **El ente rector de ciberseguridad** impondrá las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción leve, según las siguientes reglas:
>
> 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

[1] Constitución de la República del Ecuador, Registro Oficial No. 449 de 20 de octubre de 2008, artículo 82.

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.

El ente rector de ciberseguridad establecerá la multa aplicable en función del principio de proporcionalidad." (énfasis añadido)

8. El artículo bajo análisis establece las sanciones administrativas que impondrá el ente rector de ciberseguridad en caso de verificarse el cometimiento de una infracción leve.

8.1. No obstante, el artículo 20-Y del proyecto de ley establece expresamente que "[l]a potestad sancionadora en materia de ciberseguridad será ejercida por los órganos de regulación, supervisión o control especializados dentro de su ámbito de competencia [y que] El ente rector ejercerá esta potestad únicamente en los sectores que carezcan de órgano especializado […]".

8.2. De igual forma, los incisos segundo y tercero del artículo 20-Z del proyecto de ley establecen que:

> 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 sus 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. (énfasis añadido)

8.3. Como se observa, el texto aprobado genera una contradicción interna respecto de la titularidad de la potestad sancionadora, a saber: por un lado, el artículo 20-S atribuye de manera directa y general la potestad sancionadora al ente rector; y, por otro, los artículos 20-Y y 20-Z establecen que dicha potestad corresponde primariamente a los órganos de control especializados, quedando el ente rector como autoridad subsidiaria.

8.4. El ordenamiento jurídico determina que las instituciones del Estado y sus servidores ejercerán únicamente las atribuciones expresamente conferidas por la Constitución y la Ley[2]. Asimismo, el principio de lealtad institucional prevé que las administraciones públicas respetarán, entre si, el ejercicio legítimo de las competencias y ponderarán los intereses públicos implicados[3].

8.5. El artículo 20-Y del proyecto de ley reconoce esta lógica, empero, al atribuir en el artículo 20-S la potestad sancionadora de manera directa al ente rector, se produce una desalineación normativa que podría provocar conflictos de competencia y dar lugar a procedimientos paralelos en varias instituciones.

8.6. En consecuencia, la coexistencia de disposiciones contradictorias sobre la titularidad de la potestad sancionadora podría generar incertidumbre respecto de la autoridad competente para imponer sanciones administrativas, lo que se traduce en inseguridad jurídica, así como en una afectación al principio de competencia previsto en la Constitución de la República.

9. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

> Artículo 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] Constitución de la República del Ecuador, Registro Oficial No. 449 de 20 de octubre de 2008, artículo 226.
[3] Código Orgánico Administrativo, Registro Oficial Suplemento No. 31 de 07 de julio de 2017, artículo 25.

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.

(iv) Artículo 20-T

10. El artículo 20-T, contenido en el artículo 6 del proyecto de ley, señala:

Artículo 20-T.- Sanciones por infracciones graves. - **El ente rector de ciberseguridad** impondrá las siguientes sanciones administrativas, en el 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. El ente rector de ciberseguridad establecerá la multa aplicable en función del principio de proporcionalidad. (énfasis añadido)

11. La disposición bajo análisis, al igual que en el caso del artículo 20-S, establece las sanciones administrativas que impondrá el ente rector de ciberseguridad en caso de verificarse el cometimiento de una infracción grave.

11.1. No obstante, la coexistencia de disposiciones contradictorias sobre la titularidad de la potestad sancionadora podría ocasionar inseguridad jurídica, así como una afectación al principio de competencia previsto en la Constitución de la República, de acuerdo con lo expuesto respecto del artículo 20-S.

12. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

> Artículo 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.

(v) Artículo 20-U

13. El artículo 20-U, contenido en el artículo 6 del proyecto de ley, señala:

> Artículo 20-U.- Infracciones muy graves. - **El ente rector de ciberseguridad** impondrá las siguientes sanciones administrativas, en el 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. El ente rector de ciberseguridad establecerá la multa aplicable en función del principio de proporcionalidad.

14. El artículo 20-U se titula “Infracciones muy graves”; no obstante, esta disposición busca regular las sanciones aplicables frente al presunto cometimiento de infracciones muy graves, no las infracciones *per se*. Esta duplicación en el título del artículo podría generar confusión interpretativa

debido a que en el artículo 20-R ya se encuentran definidas las infracciones muy graves en materia de ciberseguridad.

14.1. Lo correcto, entonces, sería que el artículo bajo análisis se denomine "Sanciones por infracciones muy graves", a efectos de guardar uniformidad con los artículos 20-S y 20-T, que contemplan las sanciones por el cometimiento de infracciones leves y graves, respectivamente.

14.2. Por otro lado, de la misma forma que en los artículos 20-S y 20-T, el artículo determina las sanciones administrativas que impondrá el ente rector de ciberseguridad en caso de verificarse el cometimiento de una infracción muy grave.

15. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo la siguiente alternativa:

> Artículo 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.

(vi) Artículo 20-X

16. El artículo 20-X, contenido en el artículo 6 del proyecto de ley, señala:

> Artículo 20-X.- Criterios de graduación. - Para determinar la sanción dentro de los rangos del **artículo 20-U**, se considerarán, entre otros:
>
> 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, la sanción deberá ser proporcional al daño potencial o efectivo causado. (énfasis añadido)

17. La disposición bajo análisis establece los criterios que se deben observar para determinar la sanción aplicable por el cometimiento de infracciones muy graves, conforme los rangos previstos en el artículo 20-U.

17.1. La redacción actual del artículo 20-X circunscribe la aplicación de estos criterios únicamente a las sanciones previstas en el artículo 20-U, es decir, únicamente a las infracciones muy graves. Sin embargo, el propio régimen sancionador previsto en el proyecto de ley establece rangos de sanción no solo para infracciones muy graves, sino también para infracciones graves y leves, conforme se desprende de los artículos 20-S y 20-T.

17.2. En efecto, la existencia de rangos para el establecimiento de una sanción presupone necesariamente la posibilidad de graduar la sanción dentro de dichos márgenes, ya que limitar la aplicación de los criterios de graduación únicamente a las infracciones de mayor gravedad genera una inconsistencia dentro del propio sistema sancionador contemplado en el proyecto de ley.

17.3. El principio de proporcionalidad constituye no solo un pilar fundamental del derecho administrativo sancionador, sino también una garantía del debido proceso[4], pues implica que los poderes públicos titulares de la potestad sancionadora han de observar en el momento de aplicación de la

[4] Constitución de la República del Ecuador. Artículo 76, numeral 6.

ley, una reacción causa-efecto[5]. En particular, el proyecto de ley exige a la autoridad administrativa valorar, en cada caso concreto, circunstancias relevantes como:

a) La gravedad del daño causado o del riesgo generado;
b) El grado de culpabilidad;
c) La conducta previa del infractor;
d) La cooperación con la autoridad; y,
e) La capacidad económica del sujeto sancionado.

Estos elementos permiten que la sanción sea adecuada, necesaria y proporcional al comportamiento infractor.

17.4. En consecuencia, los criterios previstos en el artículo 20-X no constituyen parámetros exclusivos de las infracciones muy graves, sino que deberían ser observados para determinar las sanciones aplicables a todas las infracciones previstas en el proyecto de ley.

18. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

Artículo 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.

[5] Obando, F.J. (2008). El Derecho Administrativo Sancionador y su Proyección en el Ordenamiento Jurídico Costarricense. Asociación Internacional de Derecho Administrativo. Pág. 19.

II
OBJECIÓN AL ARTÍCULO 13

19. El artículo 13 del proyecto de ley señala:

Artículo 13.- Realícense las siguientes reformas:

1. Sustitúyase el artículo 108 por el siguiente:

Artículo 108.- Regulación y control. - El uso del espectro radioeléctrico asociado a redes satelitales, así como la prestación de servicios realizada a través de tales redes serán administrados, regulados y controlados por el Estado.

Las concesiones de frecuencias para la provisión del servicio de acceso a internet satelital fijo y móvil de órbita baja (LEO) que operen a través de Estaciones Terrenas en Movimiento (ESIM), seguirán un régimen diferenciado dispuesto por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). La fórmula para el cálculo de las tarifas por el uso y explotación de las frecuencias asignadas del espectro radioeléctrico no tomará como variables a las Estaciones Terrenas en Movimiento, los Equipos Terminales de Telecomunicaciones o los usuarios finales registrados para evitar una distorsión anticompetitiva en contra de las nuevas tecnologías.

El Título Habilitante "Registro de Servicio de Provisión de Acceso a Internet Satelital de Órbita Baja" no requerirá para su concesión del Título Habilitante de Registro de Servicio de Segmento Espacial u otro título complementario como condición previa para la prestación del servicio de acceso a internet al consumidor final.

El presente régimen será aplicable a las tecnologías de acceso a internet satelital, fijo y móvil de órbita baja (LEO), que operen mediante Estaciones Terrenas en Movimiento (ESIM), con el objetivo de promover la inclusión digital, la equidad territorial, el desarrollo productivo y la soberanía tecnológica del país.

Estas tecnologías serán reconocidas como parte de la infraestructura crítica digital del Estado, por su rol estratégico en la continuidad operativa de los servicios esenciales ante contingencias que afecten las redes terrestres.

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ejercerá el control técnico, económico y operativo sobre los servicios de acceso a internet satelital regulados por esta Ley, pudiendo realizar auditorías, verificaciones de cobertura y evaluaciones de desempeño de los operadores autorizados.

> Para el cumplimiento de estas funciones, podrá coordinar acciones con el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) y el Ministerio de Defensa Nacional, para proteger el espectro radioeléctrico como recurso estratégico de soberanía nacional.
>
> Los operadores que implementen programas de alfabetización digital, conectividad comunitaria, defensa, o inclusión tecnológica, en coordinación con el MINTEL, podrán acceder a beneficios que serán determinado por las agencias de control correspondientes.
>
> Estas acciones formarán parte de la política pública de soberanía digital del Ecuador, orientada a garantizar la autonomía tecnológica, la defensa del espectro radioeléctrico y la presencia efectiva del Estado en todo el territorio nacional.

20. El artículo 13 del proyecto de ley sustituye el artículo 108 de la Ley Orgánica de Telecomunicaciones, estableciendo, entre otros aspectos: un régimen específico para la provisión del servicio de acceso a internet satelital de órbita baja (LEO) que opere mediante Estaciones Terrenas en Movimiento (ESIM); la definición de una fórmula tarifaria específica para el uso del espectro radioeléctrico, así como la creación de un título habilitante específico para la provisión del servicio de acceso a internet satelital de órbita baja que no requeriría títulos habilitantes adicionales previos.

20.1. Sobre lo anterior, el 03 de marzo de 2026, el Ministerio de Telecomunicaciones y de la Sociedad de la Información informó a la Secretaría General Jurídica de la Presidencia de la República que, en el ámbito de sus competencias, solicitó a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) la emisión del respectivo criterio técnico institucional.

20.2. En tal virtud, la Agencia de Regulación y Control de las Telecomunicaciones elaboró el Informe Técnico Nro. IT-CREG-CCON-2026-0001 de 26 de febrero de 2026, en el cual, luego del análisis efectuado al proyecto de ley aprobado por la Asamblea Nacional, concluyó:

> […] • El mantenimiento del régimen general de títulos habilitantes, contribuciones sectoriales, régimen de usuarios y control técnico es indispensable para garantizar la sostenibilidad del modelo institucional y del servicio universal.

> • El régimen diferenciado es técnicamente viable únicamente si se circunscribe de forma expresa al cálculo de tarifas por el uso del espectro del segmento espacial satelital.
> • La propuesta de ASETEL mejora la coherencia sistémica de la norma sin afectar los objetivos de inclusión digital ni el desarrollo de las redes LEO.
> • Es completamente factible ajustar el texto para crear la categoría general de "Servicio de Acceso a Internet Satelital", asegurando el cumplimiento de las obligaciones regulatorias generales (como la obtención de títulos habilitantes) y restringiendo los beneficios a descuentos tarifarios focalizados en derechos de espectro a cambio de programas de conectividad. [...]

20.3. En este sentido, la mencionada agencia recomendó: "[...] valor[ar] el respaldo a la objeción parcial al texto aprobado del artículo 13 del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, sobre la base de los fundamentos técnicos, regulatorios y de coherencia con el marco constitucional y legal del sector de telecomunicaciones expuestos en este documento; [...]".

20.4. De conformidad con el análisis técnico efectuado por ARCOTEL, el restringir normativamente un beneficio o un régimen legal exclusivamente a sistemas de "órbita baja (LEO)", excluyendo a satélites geosetacionarios (GEO) o de órbita media (MEO), genera una asimetría regulatoria que vulnera el principio de igualdad en la prestación de servicios.

20.5. Se colige entonces, que el régimen regulatorio diferenciado exclusivo para redes de órbita baja (LEO) previsto en el proyecto de ley podría generar interpretaciones según las cuales los operadores que utilicen esta tecnología quedarían sujetos a condiciones regulatorias distintas o más favorables que las aplicables a otros operadores que prestan servicios de acceso a internet mediante redes terrestres o mediante otras tecnologías satelitales, lo cual implicaría ventajas regulatorias para estos operadores y una afectación a las condiciones de competencia dentro del mercado de internet.

20.6. De acuerdo con ARCOTEL, el marco jurídico ecuatoriano de telecomunicaciones se fundamenta en el principio de neutralidad tecnológica, el cual constituye la base técnica para crear regulaciones aplicadas a la prestación de los servicios de telecomunicaciones. Conforme a este principio, la regulación del sector no debe favorecer ni discriminar tecnologías específicas.

20.7. El principio de neutralidad tecnológica se encuentra recogido a lo largo de la Ley Orgánica de Telecomunicaciones, entre cuyos objetivos se incluye "fomentar la neutralidad tecnológica y la neutralidad de red".[6]

20.8. Bajo esta perspectiva, establecer un régimen normativo específico aplicable únicamente a una tecnología orbital determinada (LEO), excluyendo otras tecnologías satelitales como las de órbita media (MEO) o geoestacionaria (GEO), podría resultar incompatible con el principio de neutralidad tecnológica que rige el sector de las telecomunicaciones.

20.9. En consecuencia, el desarrollo de nuevas tecnologías satelitales representa una oportunidad importante para ampliar la conectividad y reducir brechas digitales, especialmente en zonas rurales o de difícil acceso. No obstante, la incorporación de estas tecnologías al mercado debe realizarse dentro de un marco regulatorio coherente con los principios que rigen el sector, a fin de garantizar condiciones equitativas para todos los operadores.

20.10. Por lo tanto, con base en las consideraciones expuestas en los numerales precedentes y, acogiendo las recomendaciones técnicas, presento el siguiente texto alternativo:

Artículo 108.- Regulación y control. El uso del espectro radioeléctrico asociado a redes satelitales, así como la prestación de servicios realizada a través de tales redes serán administrados, regulados y controlados por el Estado.

Las concesiones de frecuencias para la provisión del servicio de acceso a internet satelital seguirán un régimen tarifario diferenciado exclusivamente por el uso del segmento espacial satelital. Dicho régimen tarifario, así como los requisitos y condiciones técnicas para el otorgamiento del respectivo título habilitante y prestación del servicio, serán definidos por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

La fórmula para el cálculo de las tarifas por el uso y explotación de las frecuencias asignadas del espectro radioeléctrico no tomará como variables a las Estaciones Terrenas, los Equipos Terminales de Telecomunicaciones o los usuarios finales

[6] Ley Orgánica de Telecomunicaciones, publicada en el Tercer Registro Oficial Suplemento No. 439 de 18 de febrero de 2015. Artículo 3, numeral 13.

registrados para evitar una distorsión anticompetitiva en contra de las nuevas tecnologías.

El Título Habilitante "Registro de Servicio de Provisión de Acceso a Internet Satelital" no requerirá para su concesión del Título Habilitante de Registro de Servicio de Segmento Espacial u otro título similar complementario como condición previa para la prestación del servicio de acceso a internet al consumidor final.

Las tecnologías de acceso a internet satelital serán reconocidas como parte de la infraestructura crítica digital del Estado, por su rol estratégico en la continuidad operativa de los servicios esenciales ante contingencias que afecten las redes terrestres.

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ejercerá el control técnico, sobre los servicios de acceso a internet satelital regulados por esta Ley, pudiendo realizar auditorías, verificaciones de cobertura y evaluaciones de desempeño de los operadores autorizados.

Para el cumplimiento de estas funciones, podrá coordinar acciones con el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) y el Ministerio de Defensa Nacional, para proteger el espectro radioeléctrico como recurso estratégico de soberanía nacional.

Los operadores que implementen programas de alfabetización digital, conectividad comunitaria, defensa, o inclusión tecnológica, en coordinación con el MINTEL, podrán acceder a beneficios que se aplicarán en las tarifas de los derechos de concesión de frecuencias y uso de frecuencias, los cuales serán determinados por las agencias de control correspondientes.

Estas acciones formarán parte de la política pública de soberanía digital del Ecuador, orientada a garantizar la autonomía tecnológica, la defensa del espectro radioeléctrico y la presencia efectiva del Estado en todo el territorio nacional.

III
OBJECIÓN A LA DISPOSICIÓN GENERAL PRIMERA

21. La disposición en cuestión señala:

Primera.- Las disposiciones de esta ley se aplicarán en un marco de complementariedad y coordinación interinstitucional.

La rectoría normativa, de planificación y coordinación en materia de ciberseguridad corresponde al ente rector en transformación digital, sin sustituir ni interferir en las competencias exclusivas atribuidas por la Constitución

> y la ley a otros órganos del sector público, en particular a los rectores de defensa nacional, educación superior, seguridad pública, protección de datos personales, la Contraloría General del Estado y las Superintendencias.
>
> La fiscalización y la potestad sancionadora recaerán de manera exclusiva en los órganos de control especializados dentro de sus respectivos sectores. El ente rector únicamente intervendrá en los ámbitos que no cuenten con órgano especializado, limitándose a emitir lineamientos técnicos generales, coordinar acciones preventivas y remitir informes técnicos de carácter no vinculante.
>
> Toda acción normativa, técnica o administrativa derivada de esta ley deberá coordinarse con las entidades competentes para evitar duplicidades, garantizar la seguridad jurídica y asegurar la eficacia institucional. (énfasis añadido)

22. El segundo inciso de la disposición general primera establece que la rectoría normativa, de planificación y coordinación en materia de ciberseguridad le corresponde al ente rector en transformación digital. Sin embargo, el mismo proyecto de ley identifica expresamente al ente rector en materia de ciberseguridad como la autoridad encargada de ejercer funciones de rectoría normativa, planificación y coordinación interinstitucional en esta materia.

22.1. En efecto, de conformidad con el literal b) del artículo 5, una de las atribuciones del **ente rector en ciberseguridad** es "ejercer funciones de rectoría normativa, planificación y coordinación interinstitucional en materia de ciberseguridad".

22.2. Por tanto, la referencia contenida en la Disposición General Primera al "ente rector en transformación digital" introduce una discrepancia dentro del propio cuerpo normativo que podría generar conflictos de competencia y afectar la implementación normativa.

22.3. En Derecho Público, la claridad en la asignación de competencias resulta esencial para garantizar la responsabilidad administrativa de las autoridades y la seguridad jurídica de los administrados. Bajo esta premisa, cuando una norma atribuye funciones de rectoría a dos autoridades distintas, se genera un margen de incertidumbre que puede traducirse en dificultades para el ejercicio de determinadas competencias.

22.4. En consecuencia, la coexistencia de dos referencias distintas ("ente rector en transformación digital" y "ente rector en ciberseguridad") puede generar ambigüedad respecto de cuál es la autoridad encargada de ejercer la rectoría en esta materia.

23. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

> Primera.- Las disposiciones de esta ley se aplicarán en un marco de complementariedad y coordinación interinstitucional.
>
> La rectoría normativa, de planificación y coordinación en materia de ciberseguridad corresponde al ente rector en ciberseguridad, sin sustituir ni interferir en las competencias exclusivas atribuidas por la Constitución y la ley a otros órganos del sector público, en particular a los rectores de defensa nacional, educación superior, seguridad pública, protección de datos personales, la Contraloría General del Estado y las Superintendencias.
>
> La fiscalización y la potestad sancionadora recaerán de manera exclusiva en los órganos de control especializados dentro de sus respectivos sectores. El ente rector únicamente intervendrá en los ámbitos que no cuenten con órgano especializado, limitándose a emitir lineamientos técnicos generales, coordinar acciones preventivas y remitir informes técnicos de carácter no vinculante.
>
> Toda acción normativa, técnica o administrativa derivada de esta ley deberá coordinarse con las entidades competentes para evitar duplicidades, garantizar la seguridad jurídica y asegurar la eficacia institucional.

IV
OBJECIÓN A LA DISPOSICIÓN GENERAL SEXTA

24. La disposición en cuestión señala:

> Sexta. - En el plazo máximo de doce (12) meses contados desde la entrada en vigencia de esta ley, el ente rector adoptará las medidas necesarias para la organización y funcionamiento del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), conforme al Reglamento previsto en la Disposición Transitoria Primera en coordinación con los equipos y centros de respuesta a incidentes existentes.
>
> Durante este período de transición:

> a) El EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), continuará cumpliendo sus funciones como CSIRT sectorial especializado en telecomunicaciones, integrándose al **Sistema Nacional de Ciberseguridad** bajo la coordinación del CSIRT Nacional.
>
> b) El ente rector gestionará ante los organismos internacionales la transferencia, reconocimiento o coexistencia de las membresías y acreditaciones que actualmente posee el EcuCERT, garantizando la continuidad de la representación del Ecuador en las redes globales de respuesta a incidentes.
>
> c) La Red Nacional de Confianza (RNC) se articulará como mecanismo de cooperación público - privada y de intercambio de información técnica bajo la supervisión del CSIRT Nacional, sin perjuicio de la autonomía operativa de los CSIRT sectoriales.
>
> Vencido el plazo, el ente rector expedirá la normativa técnica que regule la integración, coordinación y delimitación de competencias entre el CSIRT Nacional, el EcuCERT y los demás CSIRT sectoriales. (énfasis añadido).

25. La Disposición General Sexta establece un régimen de transición para la organización y funcionamiento del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional). En particular, el literal a) dispone que el EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), continuará cumpliendo sus funciones como CSIRT sectorial especializado en telecomunicaciones, integrándose al Sistema Nacional de Ciberseguridad bajo la coordinación del CSIRT Nacional.

25.1. Sin embargo, de la revisión del texto aprobado la Asamblea Nacional, se observa que el proyecto de ley no crea, regula ni estructura formalmente un "Sistema Nacional de Ciberseguridad".

25.2. Si bien el proyecto de ley establece varias figuras institucionales como el ente rector en materia de ciberseguridad, el CSIRT Nacional y los CSIRT sectoriales, en ninguna disposición del proyecto se define la existencia, naturaleza jurídica, estructura, integrantes o competencias de un Sistema Nacional de Ciberseguridad como entidad o esquema institucional formal.

25.3. En este sentido, la incorporación de referencias a estructuras institucionales no previstas expresamente en el ordenamiento jurídico puede afectar la claridad del marco normativo y generar incertidumbre

respecto de los mecanismos de coordinación para la gestión de incidentes de seguridad informática.

25.4. Por tanto, en una materia técnica como la ciberseguridad, en la que intervienen múltiples actores, resulta fundamental que la arquitectura institucional prevista en la ley sea clara, precisa y plenamente definida. De lo contrario, podrían surgir interpretaciones divergentes sobre el alcance de las relaciones entre el CSIRT Nacional, los CSIRT sectoriales y las autoridades competentes.

26. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

Sexta. - En el plazo máximo de doce (12) meses contados desde la entrada en vigencia de esta ley, el ente rector adoptará las medidas necesarias para la organización y funcionamiento del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), conforme al Reglamento previsto en la Disposición Transitoria Primera en coordinación con los equipos y centros de respuesta a incidentes existentes.

Durante este período de transición:

a) El EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), continuará cumpliendo sus funciones como CSIRT sectorial especializado en telecomunicaciones, bajo la coordinación del CSIRT Nacional.

b) El ente rector gestionará ante los organismos internacionales la transferencia, reconocimiento o coexistencia de las membresías y acreditaciones que actualmente posee el EcuCERT, garantizando la continuidad de la representación del Ecuador en las redes globales de respuesta a incidentes.

c) La Red Nacional de Confianza (RNC) se articulará como mecanismo de cooperación público - privada y de intercambio de información técnica bajo la supervisión del CSIRT Nacional, sin perjuicio de la autonomía operativa de los CSIRT sectoriales.

Vencido el plazo, el ente rector expedirá la normativa técnica que regule la integración, coordinación y delimitación de competencias entre el CSIRT Nacional, el EcuCERT y los demás CSIRT sectoriales.

27. En mérito de las consideraciones expuestas y en ejercicio de las atribuciones que me confieren los artículos 137 y 138 de la Constitución de la República, emito la correspondiente **OBJECIÓN PARCIAL POR INCONVENIENCIA** al proyecto de **Ley Orgánica para el Fortalecimiento de la Ciberseguridad**, decisión que queda establecida en los términos precedentes, así como en el documento correspondiente, cuyo auténtico devuelvo a su autoridad.

Atentamente,

Firmado electrónicamente por:
DANIEL ROYGILCHRIST NOBOA AZIN
Validar únicamente con FirmaEC

Daniel Noboa Azin
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

Memorando Nro. AN-ABIM-2026-0069-M

Quito, D.M., 31 de marzo de 2026

PARA: Sr. Mtr. Niels Anthonez Olsen Peet
Presidente de la Asamblea Nacional

ASUNTO: Moción de allanamiento a la objeción parcial al "Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad"

De mi consideración:

En virtud de la convocatoria a la Sesión Nro. 082-AN-2025-2029, del Pleno de la Asamblea Nacional, para el día martes 31 de marzo de 2026, que dentro del orden del día respecto a "Conocer y resolver respecto del Informe No Vinculante sobre la Objeción Parcial al Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad", de conformidad con el artículo 135 de la Ley Orgánica de la Función Legislativa, me permito presentar la siguiente moción para su aprobación:

"MOCIÓN: Allanarse a la objeción parcial por inconveniencia al Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, específicamente respecto al artículo 6 que comprende los artículos 20-A, 20-Q, 20-S, 20-T, 20-U y 20-X; así como al artículo 13 y de la Disposición General Primera del referido proyecto."

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Sra. Inés Margarita Alarcón Bueno
ASAMBLEÍSTA

Copia:
Sr. Giovanny Francisco Bravo Rodríguez
Secretario General

Firmado electrónicamente por:
INES MARGARITA ALARCON BUENO
Validar únicamente con FirmaEC

REPÚBLICA DEL ECUADOR
Asamblea Nacional

EL PLENO

CONSIDERANDO:

Que el artículo 227 de la Constitución de la República dispone que la administración pública constituye un servicio a la colectividad guiado por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación; principios cuya realización demanda garantizar la seguridad, continuidad y confiabilidad de los servicios públicos que operan mediante medios y plataformas digitales;

Que, el artículo 277 de la Constitución establece como deberes del Estado garantizar los derechos de las personas y la naturaleza, dirigir y regular el proceso de desarrollo, producir bienes y servicios, promover la ciencia y la tecnología, e impulsar actividades económicas mediante instituciones que aseguren el cumplimiento de la Constitución y la ley; deberes que, en la era digital, requieren la incorporación de la ciberseguridad como componente estructural de la acción estatal;

Que, la transformación digital del Estado ecuatoriano constituye un proceso estratégico para la modernización institucional, el fortalecimiento de la transparencia, la mejora de la prestación de servicios públicos, la innovación en la gestión administrativa y la ampliación del acceso y participación ciudadana en entornos digitales, de conformidad con la Ley Orgánica para la Transformación Digital y Audiovisual;

Que, la interconexión creciente de sistemas, redes y servicios públicos y privados, así como la dependencia del país de tecnologías digitales para la provisión de servicios esenciales, incrementan la exposición del Ecuador a riesgos y amenazas cibernéticas, tales como ciberataques, accesos indebidos, filtraciones de datos, interrupciones operativas y afectaciones a la infraestructura estratégica,

comprometiendo la continuidad del funcionamiento del Estado y la seguridad nacional;

Que, la ciberseguridad concebida como el conjunto de medidas técnicas, organizativas, normativas y de gobernanza destinadas a proteger la confidencialidad, integridad, disponibilidad, autenticidad y resiliencia de los activos digitales se ha convertido en una condición habilitante para la protección del interés público, la continuidad del funcionamiento del Estado, la confianza ciudadana y el adecuado desarrollo de la economía digital;

Que, se requiere dotar al país de un marco legal que establezca estándares nacionales de seguridad digital, defina mecanismos de gestión y notificación de incidentes, y consolide procedimientos de coordinación interinstitucional que eviten duplicidades y respeten las competencias de los órganos de regulación y control especializados, asegurando un enfoque basado en riesgos y continuidad operativa;

Que, la identificación, clasificación y priorización de servicios esenciales e infraestructura crítica digital constituye un requisito indispensable para la continuidad operativa del Estado y la protección del interés público, siendo necesario contar con un Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital, como instrumento técnico que permita ordenar las capacidades de ciberseguridad, gestionar riesgos de manera proporcional y fortalecer la resiliencia nacional;

Que, la creciente frecuencia y sofisticación de incidentes de ciberseguridad exige la adopción de mecanismos uniformes y oportunos de gestión y notificación de incidentes, que permitan activar respuestas técnicas coordinadas, mitigar efectos, prevenir la propagación de amenazas y alinear al país con estándares internacionales de referencia;

Que, la acelerada evolución de tecnologías emergentes, incluyendo la computación cuántica, genera riesgos que pueden comprometer la solidez de los mecanismos criptográficos tradicionales utilizados para la protección de información estatal, privada y de servicios esenciales, lo cual exige incorporar el principio de adaptabilidad tecnológica y adoptar estándares internacionales resilientes frente a dichas amenazas, con el fin de garantizar la seguridad, continuidad y confiabilidad del ecosistema digital nacional;

Que, la identificación temprana de vulnerabilidades y fallas en sistemas tecnológicos requiere habilitar jurídicamente actividades de hacking ético y pruebas de penetración, bajo principios de consentimiento, finalidad legítima, profesionalización y protección de datos personales, con el fin de fortalecer las capacidades de seguridad digital y prevenir riesgos que puedan comprometer servicios esenciales o infraestructura crítica;

Que, las amenazas cibernéticas tienen un carácter transnacional, distribuido y de rápida propagación, lo cual demanda fortalecer la cooperación internacional, la participación del Ecuador en redes globales de respuesta a incidentes (CSIRT, CERT, FIRST), y la armonización de los estándares nacionales con marcos internacionales de prevención, mitigación y resiliencia;

Que, la existencia de órganos de regulación y control especializados en sectores estratégicos obliga a que la potestad sancionadora en materia de ciberseguridad se ejerza conforme a los principios de especialidad, coordinación y non bis in ídem, y que su aplicación en sectores no regulados se realice de manera subsidiaria, gradual y proporcional, conforme al nivel de riesgo, la capacidad económica del sujeto obligado y la criticidad del servicio involucrado;

Que, la alfabetización digital, la formación en seguridad digital y la promoción de buenas prácticas de higiene digital son elementos esenciales para la prevención de riesgos, la mitigación de amenazas y el fortalecimiento de la resiliencia ciudadana, especialmente en el sistema educativo, lo que demanda la

incorporación de contenidos de seguridad digital en los distintos niveles de formación;

Que, es responsabilidad del Estado fortalecer el marco jurídico de la ciberseguridad mediante la incorporación de disposiciones especializadas dentro de la Ley Orgánica para la Transformación Digital y Audiovisual, sin alterar su estructura institucional ni generar nuevas entidades, optimizando capacidades existentes y garantizando la sostenibilidad fiscal establecida en el artículo 287 de la Constitución; y,

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

LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD

Capítulo I

En la LEY ORGÁNICA DE TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL, efectúense las siguientes reformas:

Artículo 1.- Agréguese al final del artículo 1 lo siguiente:

"e. 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. 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."

Artículo 2.- Agréguese como literal h) del artículo 2, lo siguiente:

"h. Ciberseguridad: 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."

Artículo 3.- Sustitúyase el primer inciso del artículo 3 por el siguiente:

"Art. 3.- Rectoría. - 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."

Artículo 4.- Agréguese al final del artículo 5 lo siguiente:

"g) Servicio esencial. - 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. - 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. - 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. - 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. - 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). - 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. - 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. - 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. - 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. - 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). - 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."

Artículo 5.- Agréguese a continuación del artículo 7 el siguiente artículo:

"Artículo 7-A.- Atribuciones del ente rector en ciberseguridad. - 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."

Artículo 6.- Agréguese a continuación del artículo 20, el siguiente título:

"Título (...)

DE LA CIBERSEGURIDAD

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 7.- Sustitúyase el artículo 32 por el siguiente:

"Artículo. 32.- 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."

Artículo 8.- Sustitúyase el primer inciso del artículo 33 por el siguiente:

"Artículo. 33.- De la transformación digital de las mallas curriculares. - 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."

CAPÍTULO II

Otras disposiciones reformatorias

A LA LEY ORGÁNICA DE EDUCACIÓN INTERCULTURAL

Artículo 9.- Realícense las siguientes reformas:

1. A continuación del literal q) del artículo 6, agréguese el siguiente:

"r. El sistema educativo fomentará la seguridad digital y la ciberseguridad, promoviendo una educación que desarrolle habilidades de prevención de riesgos digitales y respalde la integridad física, psicológica y emocional de los estudiantes en entornos digitales."

2. Sustitúyase el literal k) del artículo 13, por el siguiente:

"k. Garantizar el desarrollo de competencias digitales, incluyendo la educación en seguridad digital y buenas prácticas de higiene digital en todos los niveles educativos, así como el acceso y el uso seguro de las tecnologías de la información y comunicación. Las instituciones educativas deberán fomentar el uso responsable de la tecnología y educar en la prevención de riesgos en línea, a fin de propiciar un entorno seguro de aprendizaje."

3. A continuación del literal oo) del artículo 13, agréguese el siguiente:

"pp. Implementar programas de ciberseguridad y protección digital en todas las instituciones educativas, en coordinación con el Ministerio de Telecomunicaciones y de la Sociedad de la Información. Estos programas deberán incluir herramientas para la detección y prevención de riesgos digitales, así como medidas para asegurar la conectividad segura y la protección de la información personal de los estudiantes."

4. A continuación del artículo 13, agréguese el siguiente:

"Artículo 13.1.- Educación en Seguridad Digital y Protección contra Amenazas en el Ciberespacio. - La Autoridad Educativa Nacional incorporará en el currículo nacional contenidos sobre seguridad digital, destinados a educar a estudiantes en el uso responsable de la tecnología, identificación de riesgos en línea, y buenas prácticas de higiene digital. Estos contenidos incluirán temas como ciberacoso, grooming, sexting, privacidad de la información y desinformación, y otras formas de captación o manipulación en entornos digitales que puedan afectar la integridad, seguridad y desarrollo de niños, niñas y adolescentes.

Se implementarán programas de capacitación en seguridad digital y ciberseguridad para docentes y personal educativo, a fin de que puedan identificar y prevenir amenazas digitales, así como educar a los estudiantes en prácticas seguras en el entorno digital.

La Autoridad Educativa Nacional establecerá protocolos de prevención y respuesta ante incidentes de violencia digital en el sistema educativo. Estos protocolos incluirán medidas para:

a) La identificación temprana de ciberacoso, grooming y otros tipos de violencia digital.

b) La creación de rutas de denuncia seguras para estudiantes y personal educativo.

c) La coordinación con las autoridades competentes para la protección y atención de las víctimas."

5.- Agréguese a continuación del literal w) del artículo 14, el siguiente:

"x. Recibir educación en seguridad digital y buenas prácticas en el uso de las tecnologías de la información, que promueva un entorno seguro y responsable en el uso de redes sociales, plataformas de aprendizaje y otros espacios digitales."

A LA LEY ORGÁNICA DE COMUNICACIÓN

Artículo 10.- Sustitúyase el literal c) del artículo 74 por el siguiente:

"c) Destinar una hora diaria, no acumulable, para la transmisión de programas oficiales de tele-educación, cultura, salubridad, derechos y seguridad digital, elaborados por los Ministerios o Secretarías competentes en estas materias."

AL CÓDIGO ORGÁNICO INTEGRAL PENAL

Artículo 11.- Al final del artículo 232 añadir el siguiente inciso:

"No constituyen delito las acciones de acceso, prueba o evaluación realizadas con el consentimiento expreso del titular o responsable del sistema, siempre que se ejecuten con fines de verificación o fortalecimiento de la seguridad, conforme a los procedimientos y registros establecidos en la Ley Orgánica para el Fortalecimiento de la Ciberseguridad y su normativa técnica."

A LA LEY ORGÁNICA DE TRANSPORTE TERRESTRE, TRÁNSITO Y SEGURIDAD VIAL

Artículo 12.- Realícense las siguientes reformas:

1. Añádase el siguiente inciso en el artículo 64B:

"Si el país se encuentra en grave conmoción interna por seguridad, el Presidente de la República podrá reglamentar que será obligatorio el uso del medio tecnológico automático para el servicio de peajes para todos los vehículos a nivel nacional."

2. Añádase a continuación de la disposición transitoria Octogésima Cuarta, la siguiente:

“Octogésima Quinta.- En el plazo de ciento ochenta (180) días la entidad competente en materia de Transporte Terrestre, Tránsito y Seguridad Vial, realizará un proceso de análisis, verificación y revisión de las acreditaciones nacionales emitidas a favor de los laboratorios con competencia técnica propios o de terceros encargados de la calibración de los medios tecnológicos de detección, registro y sanción automática de infracciones, las cuales deberán cumplir por lo menos con los estándares de calidad emitidos por el Servicio de Acreditación Ecuatoriano (SAE) y Servicio Ecuatoriano de Normalización (INEN).”

A LA LEY ORGÁNICA DE TELECOMUNICACIONES

Artículo 13.- Realícense las siguientes reformas:

1. Sustitúyase el artículo 108 por el siguiente:

“Artículo 108.- Regulación y control. - El uso del espectro radioeléctrico asociado a redes satelitales, así como la prestación de servicios realizada a través de tales redes serán administrados, regulados y controlados por el Estado.

Las concesiones de frecuencias para la provisión del servicio de acceso a internet satelital seguirán un régimen tarifario diferenciado exclusivamente por el uso del segmento espacial satelital. Dicho régimen tarifario, así como los requisitos y condiciones técnicas para el otorgamiento del respectivo título habilitante y prestación del servicio, serán definidos por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

La fórmula para el cálculo de las tarifas por el uso y explotación de las frecuencias asignadas del espectro radioeléctrico no tomará como variables a las Estaciones Terrenas, los Equipos Terminales de Telecomunicaciones o los usuarios finales registrados para evitar una distorsión anticompetitiva en contra de las nuevas tecnologías.

El Título Habilitante "Registro de Servicio de Provisión de Acceso a Internet Satelital" no requerirá para su concesión del Título Habilitante de Registro de Servicio de Segmento Espacial u otro título similar complementario como condición previa para la prestación del servicio de acceso a internet al consumidor final.

Las tecnologías de acceso a internet satelital serán reconocidas como parte de la infraestructura crítica digital del Estado, por su rol estratégico en la continuidad operativa de los servicios esenciales ante contingencias que afecten las redes terrestres.

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ejercerá el control técnico, sobre los servicios de acceso a internet satelital regulados por esta Ley, pudiendo realizar auditorías, verificaciones de cobertura y evaluaciones de desempeño de los operadores autorizados.

Para el cumplimiento de estas funciones, podrá coordinar acciones con el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) y el Ministerio de Defensa Nacional, para proteger el espectro radioeléctrico como recurso estratégico de soberanía nacional.

Los operadores que implementen programas de alfabetización digital, conectividad comunitaria, defensa, o inclusión tecnológica, en coordinación con el MINTEL, podrán acceder a beneficios que se aplicarán en las tarifas de los derechos de concesión de frecuencias y uso de frecuencias, los cuales serán determinados por las agencias de control correspondientes.

Estas acciones formarán parte de la política pública de soberanía digital del Ecuador, orientada a garantizar la autonomía tecnológica, la defensa del espectro radioeléctrico y la presencia efectiva del Estado en todo el territorio nacional."

A LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

Artículo 14.- Sustitúyase el primer inciso del artículo 43, por el siguiente:

"Artículo 43.- Notificación de vulneración de seguridad.- El responsable del tratamiento deberá notificar la vulneración de la seguridad de los datos personales a la Autoridad de Protección de Datos Personales, al organismo de regulación y control competente, y, para efectos informativos y de coordinación técnica para la gestión y mitigación de incidentes, al CSIRT correspondiente, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación."

DISPOSICIONES GENERALES

Primera. - Las disposiciones de esta ley se aplicarán en un marco de complementariedad y coordinación interinstitucional.

La rectoría normativa, de planificación y coordinación en materia de ciberseguridad corresponde al ente rector en ciberseguridad, sin sustituir ni interferir en las competencias exclusivas atribuidas por la Constitución y la ley a otros órganos del sector público, en particular a los rectores de defensa nacional, educación superior,

seguridad pública, protección de datos personales, la Contraloría General del Estado y las Superintendencias.

La fiscalización y la potestad sancionadora recaerán de manera exclusiva en los órganos de control especializados dentro de sus respectivos sectores. El ente rector únicamente intervendrá en los ámbitos que no cuenten con órgano especializado, limitándose a emitir lineamientos técnicos generales, coordinar acciones preventivas y remitir informes técnicos de carácter no vinculante.

Toda acción normativa, técnica o administrativa derivada de esta ley deberá coordinarse con las entidades competentes para evitar duplicidades, garantizar la seguridad jurídica y asegurar la eficacia institucional.

Segunda. - La implementación de la política pública de ciberseguridad y transformación digital se extenderá a todos los niveles de gobierno, en el marco de sus competencias y autonomía garantizadas por la Constitución. Los gobiernos autónomos descentralizados, en coordinación con el ente rector, adoptarán medidas técnicas y organizativas en materia de ciberseguridad, conforme a los lineamientos generales emitidos por dicho ente y con pleno respeto a su capacidad normativa y de gestión.

Tercera. - El CSIRT Nacional coordinará sus funciones con los equipos técnicos de respuesta a incidentes que mantengan los órganos de regulación, supervisión o control especializados en sus respectivos sectores.

Dichos equipos actuarán como CSIRT sectoriales de referencia mientras se constituyen formalmente conforme a la normativa técnica.

Su integración se regirá por los principios de cooperación, intercambio de información y respeto a las competencias sectoriales.

DISPOSICIONES TRANSITORIAS

Primera. - En el plazo máximo de doce (12) meses contados a partir de la publicación de la presente ley en el Registro Oficial, el ente rector expedirá la normativa técnica indispensable para la aplicación de la presente ley, con la siguiente priorización:

Dentro de los primeros seis (6) meses:

a) Estándares mínimos nacionales de ciberseguridad, aplicables de inmediato a los sectores que no cuenten con regulación especializada y como referencia de equivalencia para aquellos supervisados por órganos de control especializados.

b) Reglamento de Gestión y Notificación de Incidentes de Seguridad Digital.

c) Reglamento de Clasificación y Protección de Servicios Esenciales e Infraestructura Crítica Digital.

d) Reglamento sobre evaluación de vulnerabilidades y hacking ético a que se refiere el artículo 20-L.

Dentro de los primeros doce (12) meses:

a) Elaborar y publicar la primera versión del Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital, conforme a los estándares mínimos nacionales de ciberseguridad.

b) Reglamento de Organización y Funcionamiento del CSIRT Nacional, mediante el cual se consolidará su estructura, competencias, recursos y procedimientos definitivos, en complemento a la instalación inicial dispuesta en la Disposición Transitoria Séptima.

c) Reglamento de Responsabilidades y Obligaciones de Prestadores de Servicios Digitales y del sector privado.

d) Reglamento de Fiscalización Técnica en materia de ciberseguridad.

Los reglamentos aquí previstos constituyen el marco mínimo indispensable para la implementación inicial de esta ley, sin perjuicio de que el ente rector expida otras normas técnicas complementarias en el ámbito de sus competencias.

Segunda. - Aplicación diferenciada del régimen sancionador.

a) En los sectores con órgano de control especializado y normativa previa en materia de riesgos y seguridad digital, tales como el financiero y de telecomunicaciones, el régimen administrativo sancionador previsto en el Capítulo VI de esta ley será exigible a partir de la vigencia de la presente ley.

b) En los sectores que carezcan de órgano especializado y regulación previa en materia de ciberseguridad, el régimen sancionador será exigible únicamente luego de un período de adecuación mínima de veinticuatro (24) meses contados desde la expedición de la normativa técnica básica señalada en el literal a) de la Disposición Transitoria Primera.

Durante este período, las actuaciones del ente rector tendrán carácter preventivo, orientador y de acompañamiento y mejora técnica, actuando de manera subsidiaria y en coordinación con las autoridades competentes, priorizando la adopción de estándares mínimos nacionales de ciberseguridad.

c) En todos los casos, la imposición de sanciones deberá observar los criterios de gradualidad, proporcionalidad, criticidad del servicio y capacidad económica del sujeto obligado, conforme a lo dispuesto en el artículo 20-X de esta ley.

Tercera. - Hasta que el ente rector emita la normativa técnica prevista en esta ley, las actividades de fiscalización y evaluación técnica que establece el artículo 20-M tendrán carácter preventivo, orientador y de acompañamiento técnico. No se impondrán correcciones técnicas ni sanciones durante este período, salvo en casos de incumplimientos graves o deliberados que afecten de forma directa la continuidad de servicios esenciales.

Cuarta. - El ente rector, en coordinación con el ente rector de Relaciones Exteriores, gestionará en el plazo de un año contado desde la publicación de esta ley, la incorporación activa del Ecuador en redes internacionales de ciberseguridad (CSIRT, CERT, FIRST) y promoverá el alineamiento normativo con instrumentos multilaterales relevantes.

Quinta. - Los gobiernos autónomos descentralizados, en el marco de la Disposición General Segunda y de lo dispuesto en el artículo 20-A de esta ley, contarán con un plazo de hasta veinticuatro (24) meses, contados desde la publicación de los lineamientos técnicos que emita el ente rector en materia de ciberseguridad, para adoptar progresivamente las medidas organizativas y técnicas básicas de ciberseguridad en los servicios públicos esenciales de su competencia.

Durante dicho período, las actuaciones del ente rector tendrán carácter preventivo y orientador, sin aplicación de medidas sancionadoras, salvo en casos de incumplimientos graves y deliberados que afecten de forma directa la continuidad de servicios esenciales.

Sexta. - En el plazo máximo de doce (12) meses contados desde la entrada en vigencia de esta ley, el ente rector adoptará las medidas necesarias para la organización y funcionamiento del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), conforme al Reglamento previsto en la Disposición Transitoria Primera en coordinación con los equipos y centros de respuesta a incidentes existentes.

Durante este período de transición:

a) El EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), continuará cumpliendo sus funciones como CSIRT sectorial especializado en telecomunicaciones, integrándose al Sistema Nacional de Ciberseguridad bajo la coordinación del CSIRT Nacional.

b) El ente rector gestionará ante los organismos internacionales la transferencia, reconocimiento o coexistencia de las membresías y acreditaciones que actualmente posee el EcuCERT, garantizando la continuidad de la representación del Ecuador en las redes globales de respuesta a incidentes.

c) La Red Nacional de Confianza (RNC) se articulará como mecanismo de cooperación público - privada y de intercambio de información técnica bajo la supervisión del CSIRT Nacional, sin perjuicio de la autonomía operativa de los CSIRT sectoriales.

Vencido el plazo, el ente rector expedirá la normativa técnica que regule la integración, coordinación y delimitación de competencias entre el CSIRT Nacional, el EcuCERT y los demás CSIRT sectoriales.

Séptima. - Hasta que se constituyan formalmente los CSIRT sectoriales previstos en la normativa técnica, los órganos de regulación, supervisión o control especializados ejercerán de manera provisional las funciones de coordinación, gestión y reporte de incidentes de ciberseguridad en sus respectivos sectores, en articulación con el CSIRT Nacional.

Octava. - La implementación de las obligaciones internas del ente rector previstas en esta ley se realizará mediante un proceso de fortalecimiento institucional progresivo, orientado a la consolidación de capacidades técnicas, operativas y presupuestarias.

Esta disposición no modificará los plazos, fases ni efectos establecidos en las disposiciones transitorias anteriores, ni suspenderá la exigibilidad de las obligaciones y estándares mínimos previstos en esta ley.

El proceso de fortalecimiento institucional deberá completarse dentro del plazo de veinticuatro (24) meses, conforme al cronograma de ejecución que establezca el ente rector.

DISPOSICIÓN FINAL

La presente Ley entrará en vigor a partir de la fecha de su publicación en el Registro Oficial.

Dada y suscrita en el Auditorio “Mercedes Neira de Quezada”, ubicado en la Av. 25 de junio entre Italia y 7ma Avenida, edificio del ex Diario “Opinión”, en la ciudad de Machala, provincia de El Oro, a los treinta y un días del mes de marzo del año dos mil veintiséis.

Firmado electrónicamente por:
NIELS ANTHONEZ OLSEN PEET
Validar únicamente con FirmaEC

NIELS OLSEN PEET
Presidente de la Asamblea Nacional

Firmado electrónicamente por:
GIOVANNY FRANCISCO BRAVO RODRIGUEZ
Validar únicamente con FirmaEC

GIOVANNY BRAVO RODRÍGUEZ
Secretario General

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

CERTIFICACIÓN:

En mi calidad de Prosecretario General de la Asamblea Nacional, conforme lo acredito con el acta de posesión de 14 de mayo de 2025, suscrita por el señor presidente de la Asamblea Nacional, Niels Olsen Peet, y en ejercicio de la atribución contenida en el artículo 20.1 de la Ley Orgánica de la Función Legislativa, **CERTIFICO** que el Pleno de la Asamblea Nacional no consideró la objeción parcial por inconveniencia a la Disposición General Sexta del proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, formulada por el señor Presidente de la República del Ecuador, ingeniero Daniel Noboa Azín, a través del oficio No. T.368-SGJ-26-0061, de fecha 12 de marzo de 2026, ingresado en el sistema de gestión documental de la Asamblea Nacional con número de trámite interno 478636, el día 13 de marzo de 2026.

Esta certificación se la extiende en estricto cumplimiento de las funciones de esta Secretaría General, dispuestas en el artículo 20 de la Ley Orgánica de la Función Legislativa; artículo 20 de la Codificación del Reglamento Orgánico Funcional de la Asamblea Nacional, expedido mediante Resolución Nro. CAL-NAOP-2025-2027-107 de 20 de agosto de 2025; y, en consideración de lo dispuesto en el artículo 64 de la Ley Orgánica de la Función Legislativa.

Quito, D.M., 13 de abril de 2026

Firmado electrónicamente por:
JORGE ENRIQUE LOPEZ TERAN
Validar únicamente con FirmaEC

Jorge Enrique López Terán
Prosecretario General
ASAMBLEA NACIONAL DEL ECUADOR

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

Oficio No. T.368-SGJ-26-0137

Quito, D.M., 13 de mayo de 2026

Señor Magíster
Niels Anthonez Olsen Peet
PRESIDENTE DE LA ASAMBLEA NACIONAL
En su Despacho. –

De mi consideración:

Reciba un cordial saludo de la Secretaría General Jurídica de la Presidencia de la República.

Me dirijo a usted con la finalidad de informar que, mediante Oficio No. T.368-SGJ-26-0136, de 13 de mayo de 2026, se remitió al Registro Oficial, para su respectiva publicación, la Disposición Transitoria Sexta de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad, de conformidad con lo dispuesto en el artículo 64 de la Ley Orgánica de la Función Legislativa y con la certificación emitida el 13 de abril de 2026 por el señor Jorge López Terán, Prosecretario General de la Asamblea Nacional, cuya parte pertinente señala:

> […] **el Pleno de la Asamblea Nacional no consideró la objeción parcial por inconveniencia a la Disposición General Sexta del proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad**, formulada por el señor Presidente de la República del Ecuador, ingeniero Daniel Noboa Azín, a través del oficio No. T.368-SGJ-26-0061, de fecha 12 de marzo de 2026, ingresado en el sistema de gestión documental de la Asamblea Nacional con número de trámite interno 478636, el día 13 de marzo de 2026. […] (énfasis añadido).

Particular que comunico para los fines pertinentes.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PABLO ENRIQUE HERRERIA BONNET

Enrique Herrería Bonnet
Secretario General Jurídico
PRESIDENCIA DE LA REPÚBLICA

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

Oficio No. T.368-SGJ-26-0136

Quito, D.M., 13 de mayo de 2026

Señora Magíster
Martha Jaqueline Vargas Camacho
Directora del Registro Oficial
CORTE CONSTITUCIONAL DEL ECUADOR
En su Despacho. –

De mi consideración:

El 10 de febrero de 2026, mediante Oficio No. AN-NAOP-2026-002-O, el Presidente de la Asamblea Nacional remitió al Presidente Constitucional de la República el proyecto de **Ley Orgánica para el Fortalecimiento de la Ciberseguridad,** aprobado en segundo debate en la misma fecha, a fin de que se proceda con su correspondiente sanción u objeción presidencial.

El 12 de marzo de 2026, mediante Oficio No. T.368-SGJ-26-0061, el Presidente Constitucional de la República, en ejercicio de las atribuciones conferidas por los artículos 137 y 138 de la Constitución de la República, presentó objeción parcial por inconveniencia al referido proyecto de ley.

Mediante Oficio No. AN-NAOP-2026-008-O, de 13 de abril de 2026, el Presidente de la Asamblea Nacional notificó al Presidente Constitucional de la República sobre el tratamiento de la objeción parcial por inconveniencia formulada al referido proyecto de ley.

Al referido oficio, entre otras, se adjuntó la certificación de 13 de abril de 2026, que señaló:

> […] **el Pleno de la Asamblea Nacional no consideró la objeción parcial por inconveniencia a la Disposición General Sexta del proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad**, formulada por el señor Presidente de la República del Ecuador, ingeniero Daniel Noboa Azín, a través del oficio No. T.368-SGJ-26-0061, de fecha 12 de marzo de 2026, ingresado en el sistema de gestión documental de la Asamblea Nacional con número de trámite interno 478636, el día 13 de marzo de 2026. […] (énfasis añadido).

En este sentido, al no haber emitido pronunciamiento la Asamblea Nacional respecto del contenido material de la "Disposición Transitoria Sexta", cuyo texto consta en la objeción presidencial remitida con Oficio No. T.368-SGJ-26-0061, se entiende que el órgano legislativo se allanó de manera tácita.

En virtud de lo expuesto, remito la **Disposición Transitoria Sexta de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad**, junto con el oficio del Presidente de la Asamblea Nacional, así como las certificaciones emitidas por la Secretaría General respecto del tratamiento efectuado por el Pleno de la Asamblea Nacional al proyecto de ley, para su publicación en el Registro Oficial.

Con sentimientos de alta estima.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PABLO ENRIQUE
HERRERIA BONNET

Enrique Herrería Bonnet
Secretario General Jurídico
PRESIDENCIA DE LA REPÚBLICA

DOCUMENTOS ENVIADOS POR LA PRESIDENCIA DE LA REPÚBLICA

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

Oficio No. T.368-SGJ-26-0136

Quito, D.M., 13 de mayo de 2026

Señora Magíster
Martha Jaqueline Vargas Camacho
Directora del Registro Oficial
CORTE CONSTITUCIONAL DEL ECUADOR
En su Despacho. –

De mi consideración:

El 10 de febrero de 2026, mediante Oficio No. AN-NAOP-2026-002-O, el Presidente de la Asamblea Nacional remitió al Presidente Constitucional de la República el proyecto de **Ley Orgánica para el Fortalecimiento de la Ciberseguridad,** aprobado en segundo debate en la misma fecha, a fin de que se proceda con su correspondiente sanción u objeción presidencial.

El 12 de marzo de 2026, mediante Oficio No. T.368-SGJ-26-0061, el Presidente Constitucional de la República, en ejercicio de las atribuciones conferidas por los artículos 137 y 138 de la Constitución de la República, presentó objeción parcial por inconveniencia al referido proyecto de ley.

Mediante Oficio No. AN-NAOP-2026-008-O, de 13 de abril de 2026, el Presidente de la Asamblea Nacional notificó al Presidente Constitucional de la República sobre el tratamiento de la objeción parcial por inconveniencia formulada al referido proyecto de ley.

Al referido oficio, entre otras, se adjuntó la certificación de 13 de abril de 2026, que señaló:

> […] **el Pleno de la Asamblea Nacional no consideró la objeción parcial por inconveniencia a la Disposición General Sexta del proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad**, formulada por el señor Presidente de la República del Ecuador, ingeniero Daniel Noboa Azín, a través del oficio No. T.368-SGJ-26-0061, de fecha 12 de marzo de 2026, ingresado en el sistema de gestión documental de la Asamblea Nacional con número de trámite interno 478636, el día 13 de marzo de 2026. […] (énfasis añadido).

En este sentido, al no haber emitido pronunciamiento la Asamblea Nacional respecto del contenido material de la "Disposición Transitoria Sexta", cuyo texto consta en la objeción presidencial remitida con Oficio No. T.368-SGJ-26-0061, se entiende que el órgano legislativo se allanó de manera tácita.

En virtud de lo expuesto, remito la **Disposición Transitoria Sexta de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad**, junto con el oficio del Presidente de la Asamblea Nacional, así como las certificaciones emitidas por la Secretaría General respecto del tratamiento efectuado por el Pleno de la Asamblea Nacional al proyecto de ley, para su publicación en el Registro Oficial.

Con sentimientos de alta estima.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PABLO ENRIQUE HERRERIA BONNET

Enrique Herrería Bonnet
Secretario General Jurídico
PRESIDENCIA DE LA REPÚBLICA

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

Oficio No. AN-NAOP-2026-008-O

Quito, D.M., 13 de abril de 2026

Señor
Daniel Noboa Azín
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA DEL ECUADOR
En su despacho. -

De mi consideración:

El Pleno de la Asamblea Nacional, de conformidad con lo previsto en los artículos 120 numeral 6 de la Constitución de la República del Ecuador y 9 numeral 6 de la Ley Orgánica de la Función Legislativa, trató el proyecto de "**LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD**" de acuerdo con el siguiente detalle:

1. Primer debate: 5 de agosto de 2025 (Sesión Nro. 024-AN-2025-2029);
2. Segundo debate: 10 de febrero de 2026 (Sesión Nro. 069-AN-2025-2029);
3. Fecha de aprobación: 10 de febrero de 2026 (Sesión Nro. 069-AN-2025-2029).
4. Fecha de objeción presidencial: 13 de marzo de 2026;
5. Fecha de tratamiento y aprobación de la enmienda del proyecto: 31 de marzo de 2026 (Sesión Nro. 082-AN-2025-2029).

En la sesión Nro. 082-AN-2025-2029 de 31 de marzo de 2026, el Pleno de la Asamblea Nacional conoció y resolvió respecto del Informe No Vinculante a la Objeción Parcial por Inconveniencia al Proyecto de "Ley Orgánica para el Fortalecimiento de la Ciberseguridad", en virtud de lo cual aprobó la siguiente moción:

"Allanarse a la objeción parcial por inconveniencia al Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, específicamente respecto al artículo 6 que comprende los artículos 20-A, 20-Q, 20-S, 20-T, 20-U y 20-X; así como al artículo 13 y de la Disposición General Primera del referido proyecto."

Por consiguiente, y en atención al artículo 64 Ley Orgánica de la Función Legislativa, se remite para que su autoridad proceda conforme lo dispone la norma: (i) texto auténtico del proyecto de "Ley Orgánica para el Fortalecimiento de la Ciberseguridad"; y, (ii) las certificaciones de la Secretaría General, respecto de las fechas en las que el Pleno de la Asamblea Nacional realizó el tratamiento del proyecto de ley.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
NIELS ANTHONEZ OLSEN PEET

NIELS OLSEN PEET
Presidente de la Asamblea Nacional

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

CERTIFICACIÓN

En mi calidad de Secretario General de la Asamblea Nacional, **CERTIFICO** que, el proyecto de "**LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD**", fue tratado por el Pleno de la Asamblea Nacional, de acuerdo con el siguiente detalle:

1. Primer debate: 5 de agosto de 2025 (Sesión Nro. 024-AN-2025-2029);
2. Segundo debate: 10 de febrero de 2026 (Sesión Nro. 069-AN-2025-2029);
3. Fecha de aprobación: 10 de febrero de 2026 (Sesión Nro. 069-AN-2025-2029).
4. Fecha de objeción presidencial: 13 de marzo de 2026;
5. Fecha de tratamiento y aprobación de la enmienda del proyecto: 31 de marzo de 2026 (Sesión Nro. 082-AN-2025-2029).

Quito, 1 de abril de 2026.

Firmado electrónicamente por:
GIOVANNY FRANCISCO BRAVO RODRIGUEZ
Validar únicamente con FirmaEC

GIOVANNY FRANCISCO BRAVO RODRÍGUEZ
Secretario General

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

CERTIFICACIÓN:

En mi calidad de Prosecretario General de la Asamblea Nacional, conforme lo acredito con el acta de posesión de 14 de mayo de 2025, suscrita por el señor presidente de la Asamblea Nacional, Niels Olsen Peet, y en ejercicio de la atribución contenida en el artículo 20.1 de la Ley Orgánica de la Función Legislativa, **CERTIFICO** que el Pleno de la Asamblea Nacional no consideró la objeción parcial por inconveniencia a la Disposición General Sexta del proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, formulada por el señor Presidente de la República del Ecuador, ingeniero Daniel Noboa Azín, a través del oficio No. T.368-SGJ-26-0061, de fecha 12 de marzo de 2026, ingresado en el sistema de gestión documental de la Asamblea Nacional con número de trámite interno 478636, el día 13 de marzo de 2026.

Esta certificación se la extiende en estricto cumplimiento de las funciones de esta Secretaría General, dispuestas en el artículo 20 de la Ley Orgánica de la Función Legislativa; artículo 20 de la Codificación del Reglamento Orgánico Funcional de la Asamblea Nacional, expedido mediante Resolución Nro. CAL-NAOP-2025-2027-107 de 20 de agosto de 2025; y, en consideración de lo dispuesto en el artículo 64 de la Ley Orgánica de la Función Legislativa.

Quito, D.M., 13 de abril de 2026

Firmado electrónicamente por:
JORGE ENRIQUE LOPEZ TERAN
Validar únicamente con FirmaEC

Jorge Enrique López Terán
Prosecretario General
ASAMBLEA NACIONAL DEL ECUADOR

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

Oficio No. T.368-SGJ-26-0061

Guayaquil, 12 marzo de 2026

Señor Magíster
Niels Anthonez Olsen Peet
PRESIDENTE DE LA ASAMBLEA NACIONAL
En su Despacho. –

De mi consideración:

Mediante Oficio Nro. AN-SG-2026-0095-O de 11 de febrero de 2026, la Asamblea Nacional remitió a la Presidencia de la República el proyecto de **"LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD"**, discutido y aprobado en segundo debate de 10 de febrero de 2026, para la correspondiente sanción u objeción presidencial.

En ejercicio de las potestades conferidas por los artículos 137 y 138 de la Constitución de la República, notifico a usted y, por su intermedio, a la Asamblea Nacional con la siguiente **OBJECIÓN PARCIAL POR INCONVENIENCIA** al referido proyecto de ley, en los siguientes términos:

I
OBJECIÓN AL ARTÍCULO 6

(i) Artículo 20-A

1. El artículo 20-A, contenido en el artículo 6 del proyecto de ley, señala lo siguiente:

> Artículo 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-J**; 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). (énfasis añadido)

2. A continuación, se expone el argumento que fundamenta la objeción parcial por inconveniencia:

2.1. La disposición analizada establece que las normas del título denominado "DE LA CIBERSEGURIDAD", les serán aplicables a 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-J**.

2.2. Es decir, define el ámbito de aplicación del régimen de ciberseguridad respecto de los prestadores de servicios digitales, condicionando su alcance al principio de responsabilidad compartida.

2.3. Sin embargo, el artículo 20-A hace remisión al artículo 20-J, el cual establece la obligación de coordinación que tienen las entidades públicas y los operadores de infraestructura crítica digital con la autoridad competente, en tanto establece:

Artículo 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.

2.4. Por el contrario, el **artículo 20-I** efectivamente hace alusión a las responsabilidades que tienen los prestadores de servicios digitales a fin de garantizar el cumplimiento de la ley, de conformidad con el principio de responsabilidad compartida, estableciendo: i) medidas técnicas y organizativas; ii) evaluación y gestión de riesgos; iii) cooperación para gestión de incidentes; etc.

2.5. En consecuencia, la remisión al artículo 20-J resulta técnicamente incorrecta por cuanto no guarda relación con el alcance de las obligaciones derivadas del principio de responsabilidad compartida.

3. En tal virtud, y con el propósito de optimizar la claridad y técnica normativa del texto, propongo la siguiente alternativa:

> Artículo 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).

(ii) Artículo 20-Q

4. El artículo 20-Q, contenido en el artículo 6 del proyecto de ley, señala:

> Artículo 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-J** 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." (énfasis añadido)

5. Al tratarse de materia sancionadora, la norma debe prever de manera clara y expresa no solo las conductas que configuran una infracción administrativa o los sujetos responsables por dichas conductas —aspectos que efectivamente se encuentran determinados en el proyecto de ley— sino también el alcance de esta responsabilidad administrativa.

5.1. La disposición bajo análisis establece la responsabilidad administrativa que se origina como producto del incumplimiento de las disposiciones contenidas en el referido Título. Esta disposición es una norma estructural del régimen administrativo sancionador en virtud de que delimita aspectos como: sujetos responsables y el alcance material de su responsabilidad.

5.2. En este sentido, el literal b) dispone que los prestadores de servicios digitales serán responsables administrativamente, exclusivamente en lo relativo a los elementos bajo su esfera de control, conforme al **artículo 20-J** y al principio de responsabilidad compartida.

5.3. No obstante, la remisión al artículo 20-J resulta incorrecta, de acuerdo con lo expuesto en el artículo 20-A.

5.4. En consecuencia, esta inconsistencia constituye un defecto técnico que podría comprometer la correcta aplicación del régimen sancionador y generar inseguridad jurídica.[1]

6. Con el objeto de optimizar la redacción y precisión del texto normativo, se propone lo que sigue:

> Artículo 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.

(iii) Artículo 20-S

7. El artículo 20-S, contenido en el artículo 6 del proyecto de ley, señala:

> Artículo 20-S.- Sanciones por infracciones leves. - **El ente rector de ciberseguridad** impondrá las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción leve, según las siguientes reglas:
>
> 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

[1] Constitución de la República del Ecuador, Registro Oficial No. 449 de 20 de octubre de 2008, artículo 82.

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.

El ente rector de ciberseguridad establecerá la multa aplicable en función del principio de proporcionalidad." (énfasis añadido)

8. El artículo bajo análisis establece las sanciones administrativas que impondrá el ente rector de ciberseguridad en caso de verificarse el cometimiento de una infracción leve.

8.1. No obstante, el artículo 20-Y del proyecto de ley establece expresamente que "[l]a potestad sancionadora en materia de ciberseguridad será ejercida por los órganos de regulación, supervisión o control especializados dentro de su ámbito de competencia [y que] El ente rector ejercerá esta potestad únicamente en los sectores que carezcan de órgano especializado […]".

8.2. De igual forma, los incisos segundo y tercero del artículo 20-Z del proyecto de ley establecen que:

> 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 sus 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. (énfasis añadido)

8.3. Como se observa, el texto aprobado genera una contradicción interna respecto de la titularidad de la potestad sancionadora, a saber: por un lado, el artículo 20-S atribuye de manera directa y general la potestad sancionadora al ente rector; y, por otro, los artículos 20-Y y 20-Z establecen que dicha potestad corresponde primariamente a los órganos de control especializados, quedando el ente rector como autoridad subsidiaria.

8.4. El ordenamiento jurídico determina que las instituciones del Estado y sus servidores ejercerán únicamente las atribuciones expresamente conferidas por la Constitución y la Ley[2]. Asimismo, el principio de lealtad institucional prevé que las administraciones públicas respetarán, entre si, el ejercicio legítimo de las competencias y ponderarán los intereses públicos implicados[3].

8.5. El artículo 20-Y del proyecto de ley reconoce esta lógica, empero, al atribuir en el artículo 20-S la potestad sancionadora de manera directa al ente rector, se produce una desalineación normativa que podría provocar conflictos de competencia y dar lugar a procedimientos paralelos en varias instituciones.

8.6. En consecuencia, la coexistencia de disposiciones contradictorias sobre la titularidad de la potestad sancionadora podría generar incertidumbre respecto de la autoridad competente para imponer sanciones administrativas, lo que se traduce en inseguridad jurídica, así como en una afectación al principio de competencia previsto en la Constitución de la República.

9. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

> Artículo 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] Constitución de la República del Ecuador, Registro Oficial No. 449 de 20 de octubre de 2008, artículo 226.
[3] Código Orgánico Administrativo, Registro Oficial Suplemento No. 31 de 07 de julio de 2017, artículo 25.

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.

(iv) Artículo 20-T

10. El artículo 20-T, contenido en el artículo 6 del proyecto de ley, señala:

Artículo 20-T.- Sanciones por infracciones graves. - **El ente rector de ciberseguridad** impondrá las siguientes sanciones administrativas, en el 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. El ente rector de ciberseguridad establecerá la multa aplicable en función del principio de proporcionalidad. (énfasis añadido)

11. La disposición bajo análisis, al igual que en el caso del artículo 20-S, establece las sanciones administrativas que impondrá el ente rector de ciberseguridad en caso de verificarse el cometimiento de una infracción grave.

11.1. No obstante, la coexistencia de disposiciones contradictorias sobre la titularidad de la potestad sancionadora podría ocasionar inseguridad jurídica, así como una afectación al principio de competencia previsto en la Constitución de la República, de acuerdo con lo expuesto respecto del artículo 20-S.

12. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

Artículo 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.

(v) Artículo 20-U

13. El artículo 20-U, contenido en el artículo 6 del proyecto de ley, señala:

Artículo 20-U.- Infracciones muy graves. - **El ente rector de ciberseguridad** impondrá las siguientes sanciones administrativas, en el 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. El ente rector de ciberseguridad establecerá la multa aplicable en función del principio de proporcionalidad.

14. El artículo 20-U se titula “Infracciones muy graves”; no obstante, esta disposición busca regular las sanciones aplicables frente al presunto cometimiento de infracciones muy graves, no las infracciones *per se*. Esta duplicación en el título del artículo podría generar confusión interpretativa

debido a que en el artículo 20-R ya se encuentran definidas las infracciones muy graves en materia de ciberseguridad.

14.1. Lo correcto, entonces, sería que el artículo bajo análisis se denomine "Sanciones por infracciones muy graves", a efectos de guardar uniformidad con los artículos 20-S y 20-T, que contemplan las sanciones por el cometimiento de infracciones leves y graves, respectivamente.

14.2. Por otro lado, de la misma forma que en los artículos 20-S y 20-T, el artículo determina las sanciones administrativas que impondrá el ente rector de ciberseguridad en caso de verificarse el cometimiento de una infracción muy grave.

15. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo la siguiente alternativa:

> Artículo 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.

(vi) Artículo 20-X

16. El artículo 20-X, contenido en el artículo 6 del proyecto de ley, señala:

> Artículo 20-X.- Criterios de graduación. - Para determinar la sanción dentro de los rangos del **artículo 20-U**, se considerarán, entre otros:
>
> 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, la sanción deberá ser proporcional al daño potencial o efectivo causado. (énfasis añadido)

17. La disposición bajo análisis establece los criterios que se deben observar para determinar la sanción aplicable por el cometimiento de infracciones muy graves, conforme los rangos previstos en el artículo 20-U.

17.1. La redacción actual del artículo 20-X circunscribe la aplicación de estos criterios únicamente a las sanciones previstas en el artículo 20-U, es decir, únicamente a las infracciones muy graves. Sin embargo, el propio régimen sancionador previsto en el proyecto de ley establece rangos de sanción no solo para infracciones muy graves, sino también para infracciones graves y leves, conforme se desprende de los artículos 20-S y 20-T.

17.2. En efecto, la existencia de rangos para el establecimiento de una sanción presupone necesariamente la posibilidad de graduar la sanción dentro de dichos márgenes, ya que limitar la aplicación de los criterios de graduación únicamente a las infracciones de mayor gravedad genera una inconsistencia dentro del propio sistema sancionador contemplado en el proyecto de ley.

17.3. El principio de proporcionalidad constituye no solo un pilar fundamental del derecho administrativo sancionador, sino también una garantía del debido proceso[4], pues implica que los poderes públicos titulares de la potestad sancionadora han de observar en el momento de aplicación de la

[4] Constitución de la República del Ecuador. Artículo 76, numeral 6.

ley, una reacción causa-efecto[5]. En particular, el proyecto de ley exige a la autoridad administrativa valorar, en cada caso concreto, circunstancias relevantes como:

a) La gravedad del daño causado o del riesgo generado;
b) El grado de culpabilidad;
c) La conducta previa del infractor;
d) La cooperación con la autoridad; y,
e) La capacidad económica del sujeto sancionado.

Estos elementos permiten que la sanción sea adecuada, necesaria y proporcional al comportamiento infractor.

17.4. En consecuencia, los criterios previstos en el artículo 20-X no constituyen parámetros exclusivos de las infracciones muy graves, sino que deberían ser observados para determinar las sanciones aplicables a todas las infracciones previstas en el proyecto de ley.

18. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

Artículo 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.

[5] Obando, F.J. (2008). El Derecho Administrativo Sancionador y su Proyección en el Ordenamiento Jurídico Costarricense. Asociación Internacional de Derecho Administrativo. Pág. 19.

II
OBJECIÓN AL ARTÍCULO 13

19. El artículo 13 del proyecto de ley señala:

Artículo 13.- Realícense las siguientes reformas:

1. Sustitúyase el artículo 108 por el siguiente:

Artículo 108.- Regulación y control. - El uso del espectro radioeléctrico asociado a redes satelitales, así como la prestación de servicios realizada a través de tales redes serán administrados, regulados y controlados por el Estado.

Las concesiones de frecuencias para la provisión del servicio de acceso a internet satelital fijo y móvil de órbita baja (LEO) que operen a través de Estaciones Terrenas en Movimiento (ESIM), seguirán un régimen diferenciado dispuesto por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). La fórmula para el cálculo de las tarifas por el uso y explotación de las frecuencias asignadas del espectro radioeléctrico no tomará como variables a las Estaciones Terrenas en Movimiento, los Equipos Terminales de Telecomunicaciones o los usuarios finales registrados para evitar una distorsión anticompetitiva en contra de las nuevas tecnologías.

El Título Habilitante "Registro de Servicio de Provisión de Acceso a Internet Satelital de Órbita Baja" no requerirá para su concesión del Título Habilitante de Registro de Servicio de Segmento Espacial u otro título complementario como condición previa para la prestación del servicio de acceso a internet al consumidor final.

El presente régimen será aplicable a las tecnologías de acceso a internet satelital, fijo y móvil de órbita baja (LEO), que operen mediante Estaciones Terrenas en Movimiento (ESIM), con el objetivo de promover la inclusión digital, la equidad territorial, el desarrollo productivo y la soberanía tecnológica del país.

Estas tecnologías serán reconocidas como parte de la infraestructura crítica digital del Estado, por su rol estratégico en la continuidad operativa de los servicios esenciales ante contingencias que afecten las redes terrestres.

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ejercerá el control técnico, económico y operativo sobre los servicios de acceso a internet satelital regulados por esta Ley, pudiendo realizar auditorías, verificaciones de cobertura y evaluaciones de desempeño de los operadores autorizados.

> Para el cumplimiento de estas funciones, podrá coordinar acciones con el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) y el Ministerio de Defensa Nacional, para proteger el espectro radioeléctrico como recurso estratégico de soberanía nacional.
>
> Los operadores que implementen programas de alfabetización digital, conectividad comunitaria, defensa, o inclusión tecnológica, en coordinación con el MINTEL, podrán acceder a beneficios que serán determinado por las agencias de control correspondientes.
>
> Estas acciones formarán parte de la política pública de soberanía digital del Ecuador, orientada a garantizar la autonomía tecnológica, la defensa del espectro radioeléctrico y la presencia efectiva del Estado en todo el territorio nacional.

20. El artículo 13 del proyecto de ley sustituye el artículo 108 de la Ley Orgánica de Telecomunicaciones, estableciendo, entre otros aspectos: un régimen específico para la provisión del servicio de acceso a internet satelital de órbita baja (LEO) que opere mediante Estaciones Terrenas en Movimiento (ESIM); la definición de una fórmula tarifaria específica para el uso del espectro radioeléctrico, así como la creación de un título habilitante específico para la provisión del servicio de acceso a internet satelital de órbita baja que no requeriría títulos habilitantes adicionales previos.

20.1. Sobre lo anterior, el 03 de marzo de 2026, el Ministerio de Telecomunicaciones y de la Sociedad de la Información informó a la Secretaría General Jurídica de la Presidencia de la República que, en el ámbito de sus competencias, solicitó a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) la emisión del respectivo criterio técnico institucional.

20.2. En tal virtud, la Agencia de Regulación y Control de las Telecomunicaciones elaboró el Informe Técnico Nro. IT-CREG-CCON-2026-0001 de 26 de febrero de 2026, en el cual, luego del análisis efectuado al proyecto de ley aprobado por la Asamblea Nacional, concluyó:

> […] • El mantenimiento del régimen general de títulos habilitantes, contribuciones sectoriales, régimen de usuarios y control técnico es indispensable para garantizar la sostenibilidad del modelo institucional y del servicio universal.

> • El régimen diferenciado es técnicamente viable únicamente si se circunscribe de forma expresa al cálculo de tarifas por el uso del espectro del segmento espacial satelital.
> • La propuesta de ASETEL mejora la coherencia sistémica de la norma sin afectar los objetivos de inclusión digital ni el desarrollo de las redes LEO.
> • Es completamente factible ajustar el texto para crear la categoría general de "Servicio de Acceso a Internet Satelital", asegurando el cumplimiento de las obligaciones regulatorias generales (como la obtención de títulos habilitantes) y restringiendo los beneficios a descuentos tarifarios focalizados en derechos de espectro a cambio de programas de conectividad. [...]

20.3. En este sentido, la mencionada agencia recomendó: "[...] valor[ar] el respaldo a la objeción parcial al texto aprobado del artículo 13 del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, sobre la base de los fundamentos técnicos, regulatorios y de coherencia con el marco constitucional y legal del sector de telecomunicaciones expuestos en este documento; [...]".

20.4. De conformidad con el análisis técnico efectuado por ARCOTEL, el restringir normativamente un beneficio o un régimen legal exclusivamente a sistemas de "órbita baja (LEO)", excluyendo a satélites geosetacionarios (GEO) o de órbita media (MEO), genera una asimetría regulatoria que vulnera el principio de igualdad en la prestación de servicios.

20.5. Se colige entonces, que el régimen regulatorio diferenciado exclusivo para redes de órbita baja (LEO) previsto en el proyecto de ley podría generar interpretaciones según las cuales los operadores que utilicen esta tecnología quedarían sujetos a condiciones regulatorias distintas o más favorables que las aplicables a otros operadores que prestan servicios de acceso a internet mediante redes terrestres o mediante otras tecnologías satelitales, lo cual implicaría ventajas regulatorias para estos operadores y una afectación a las condiciones de competencia dentro del mercado de internet.

20.6. De acuerdo con ARCOTEL, el marco jurídico ecuatoriano de telecomunicaciones se fundamenta en el principio de neutralidad tecnológica, el cual constituye la base técnica para crear regulaciones aplicadas a la prestación de los servicios de telecomunicaciones. Conforme a este principio, la regulación del sector no debe favorecer ni discriminar tecnologías específicas.

20.7. El principio de neutralidad tecnológica se encuentra recogido a lo largo de la Ley Orgánica de Telecomunicaciones, entre cuyos objetivos se incluye "fomentar la neutralidad tecnológica y la neutralidad de red".[6]

20.8. Bajo esta perspectiva, establecer un régimen normativo específico aplicable únicamente a una tecnología orbital determinada (LEO), excluyendo otras tecnologías satelitales como las de órbita media (MEO) o geoestacionaria (GEO), podría resultar incompatible con el principio de neutralidad tecnológica que rige el sector de las telecomunicaciones.

20.9. En consecuencia, el desarrollo de nuevas tecnologías satelitales representa una oportunidad importante para ampliar la conectividad y reducir brechas digitales, especialmente en zonas rurales o de difícil acceso. No obstante, la incorporación de estas tecnologías al mercado debe realizarse dentro de un marco regulatorio coherente con los principios que rigen el sector, a fin de garantizar condiciones equitativas para todos los operadores.

20.10. Por lo tanto, con base en las consideraciones expuestas en los numerales precedentes y, acogiendo las recomendaciones técnicas, presento el siguiente texto alternativo:

Artículo 108.- Regulación y control. El uso del espectro radioeléctrico asociado a redes satelitales, así como la prestación de servicios realizada a través de tales redes serán administrados, regulados y controlados por el Estado.

Las concesiones de frecuencias para la provisión del servicio de acceso a internet satelital seguirán un régimen tarifario diferenciado exclusivamente por el uso del segmento espacial satelital. Dicho régimen tarifario, así como los requisitos y condiciones técnicas para el otorgamiento del respectivo título habilitante y prestación del servicio, serán definidos por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

La fórmula para el cálculo de las tarifas por el uso y explotación de las frecuencias asignadas del espectro radioeléctrico no tomará como variables a las Estaciones Terrenas, los Equipos Terminales de Telecomunicaciones o los usuarios finales

[6] Ley Orgánica de Telecomunicaciones, publicada en el Tercer Registro Oficial Suplemento No. 439 de 18 de febrero de 2015. Artículo 3, numeral 13.

registrados para evitar una distorsión anticompetitiva en contra de las nuevas tecnologías.

El Título Habilitante "Registro de Servicio de Provisión de Acceso a Internet Satelital" no requerirá para su concesión del Título Habilitante de Registro de Servicio de Segmento Espacial u otro título similar complementario como condición previa para la prestación del servicio de acceso a internet al consumidor final.

Las tecnologías de acceso a internet satelital serán reconocidas como parte de la infraestructura crítica digital del Estado, por su rol estratégico en la continuidad operativa de los servicios esenciales ante contingencias que afecten las redes terrestres.

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ejercerá el control técnico, sobre los servicios de acceso a internet satelital regulados por esta Ley, pudiendo realizar auditorías, verificaciones de cobertura y evaluaciones de desempeño de los operadores autorizados.

Para el cumplimiento de estas funciones, podrá coordinar acciones con el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) y el Ministerio de Defensa Nacional, para proteger el espectro radioeléctrico como recurso estratégico de soberanía nacional.

Los operadores que implementen programas de alfabetización digital, conectividad comunitaria, defensa, o inclusión tecnológica, en coordinación con el MINTEL, podrán acceder a beneficios que se aplicarán en las tarifas de los derechos de concesión de frecuencias y uso de frecuencias, los cuales serán determinados por las agencias de control correspondientes.

Estas acciones formarán parte de la política pública de soberanía digital del Ecuador, orientada a garantizar la autonomía tecnológica, la defensa del espectro radioeléctrico y la presencia efectiva del Estado en todo el territorio nacional.

III
OBJECIÓN A LA DISPOSICIÓN GENERAL PRIMERA

21. La disposición en cuestión señala:

Primera.- Las disposiciones de esta ley se aplicarán en un marco de complementariedad y coordinación interinstitucional.

La rectoría normativa, de planificación y coordinación en materia de ciberseguridad corresponde al ente rector en transformación digital, sin sustituir ni interferir en las competencias exclusivas atribuidas por la Constitución

> y la ley a otros órganos del sector público, en particular a los rectores de defensa nacional, educación superior, seguridad pública, protección de datos personales, la Contraloría General del Estado y las Superintendencias.
>
> La fiscalización y la potestad sancionadora recaerán de manera exclusiva en los órganos de control especializados dentro de sus respectivos sectores. El ente rector únicamente intervendrá en los ámbitos que no cuenten con órgano especializado, limitándose a emitir lineamientos técnicos generales, coordinar acciones preventivas y remitir informes técnicos de carácter no vinculante.
>
> Toda acción normativa, técnica o administrativa derivada de esta ley deberá coordinarse con las entidades competentes para evitar duplicidades, garantizar la seguridad jurídica y asegurar la eficacia institucional. (énfasis añadido)

22. El segundo inciso de la disposición general primera establece que la rectoría normativa, de planificación y coordinación en materia de ciberseguridad le corresponde al ente rector en transformación digital. Sin embargo, el mismo proyecto de ley identifica expresamente al ente rector en materia de ciberseguridad como la autoridad encargada de ejercer funciones de rectoría normativa, planificación y coordinación interinstitucional en esta materia.

22.1. En efecto, de conformidad con el literal b) del artículo 5, una de las atribuciones del **ente rector en ciberseguridad** es "ejercer funciones de rectoría normativa, planificación y coordinación interinstitucional en materia de ciberseguridad".

22.2. Por tanto, la referencia contenida en la Disposición General Primera al "ente rector en transformación digital" introduce una discrepancia dentro del propio cuerpo normativo que podría generar conflictos de competencia y afectar la implementación normativa.

22.3. En Derecho Público, la claridad en la asignación de competencias resulta esencial para garantizar la responsabilidad administrativa de las autoridades y la seguridad jurídica de los administrados. Bajo esta premisa, cuando una norma atribuye funciones de rectoría a dos autoridades distintas, se genera un margen de incertidumbre que puede traducirse en dificultades para el ejercicio de determinadas competencias.

22.4. En consecuencia, la coexistencia de dos referencias distintas ("ente rector en transformación digital" y "ente rector en ciberseguridad") puede generar ambigüedad respecto de cuál es la autoridad encargada de ejercer la rectoría en esta materia.

23. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

> Primera.- Las disposiciones de esta ley se aplicarán en un marco de complementariedad y coordinación interinstitucional.
>
> La rectoría normativa, de planificación y coordinación en materia de ciberseguridad corresponde al ente rector en ciberseguridad, sin sustituir ni interferir en las competencias exclusivas atribuidas por la Constitución y la ley a otros órganos del sector público, en particular a los rectores de defensa nacional, educación superior, seguridad pública, protección de datos personales, la Contraloría General del Estado y las Superintendencias.
>
> La fiscalización y la potestad sancionadora recaerán de manera exclusiva en los órganos de control especializados dentro de sus respectivos sectores. El ente rector únicamente intervendrá en los ámbitos que no cuenten con órgano especializado, limitándose a emitir lineamientos técnicos generales, coordinar acciones preventivas y remitir informes técnicos de carácter no vinculante.
>
> Toda acción normativa, técnica o administrativa derivada de esta ley deberá coordinarse con las entidades competentes para evitar duplicidades, garantizar la seguridad jurídica y asegurar la eficacia institucional.

IV
OBJECIÓN A LA DISPOSICIÓN GENERAL SEXTA

24. La disposición en cuestión señala:

> Sexta. - En el plazo máximo de doce (12) meses contados desde la entrada en vigencia de esta ley, el ente rector adoptará las medidas necesarias para la organización y funcionamiento del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), conforme al Reglamento previsto en la Disposición Transitoria Primera en coordinación con los equipos y centros de respuesta a incidentes existentes.
>
> Durante este período de transición:

> a) El EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), continuará cumpliendo sus funciones como CSIRT sectorial especializado en telecomunicaciones, integrándose al **Sistema Nacional de Ciberseguridad** bajo la coordinación del CSIRT Nacional.
>
> b) El ente rector gestionará ante los organismos internacionales la transferencia, reconocimiento o coexistencia de las membresías y acreditaciones que actualmente posee el EcuCERT, garantizando la continuidad de la representación del Ecuador en las redes globales de respuesta a incidentes.
>
> c) La Red Nacional de Confianza (RNC) se articulará como mecanismo de cooperación público - privada y de intercambio de información técnica bajo la supervisión del CSIRT Nacional, sin perjuicio de la autonomía operativa de los CSIRT sectoriales.
>
> Vencido el plazo, el ente rector expedirá la normativa técnica que regule la integración, coordinación y delimitación de competencias entre el CSIRT Nacional, el EcuCERT y los demás CSIRT sectoriales. (énfasis añadido).

25. La Disposición General Sexta establece un régimen de transición para la organización y funcionamiento del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional). En particular, el literal a) dispone que el EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), continuará cumpliendo sus funciones como CSIRT sectorial especializado en telecomunicaciones, integrándose al Sistema Nacional de Ciberseguridad bajo la coordinación del CSIRT Nacional.

25.1. Sin embargo, de la revisión del texto aprobado la Asamblea Nacional, se observa que el proyecto de ley no crea, regula ni estructura formalmente un "Sistema Nacional de Ciberseguridad".

25.2. Si bien el proyecto de ley establece varias figuras institucionales como el ente rector en materia de ciberseguridad, el CSIRT Nacional y los CSIRT sectoriales, en ninguna disposición del proyecto se define la existencia, naturaleza jurídica, estructura, integrantes o competencias de un Sistema Nacional de Ciberseguridad como entidad o esquema institucional formal.

25.3. En este sentido, la incorporación de referencias a estructuras institucionales no previstas expresamente en el ordenamiento jurídico puede afectar la claridad del marco normativo y generar incertidumbre

respecto de los mecanismos de coordinación para la gestión de incidentes de seguridad informática.

25.4. Por tanto, en una materia técnica como la ciberseguridad, en la que intervienen múltiples actores, resulta fundamental que la arquitectura institucional prevista en la ley sea clara, precisa y plenamente definida. De lo contrario, podrían surgir interpretaciones divergentes sobre el alcance de las relaciones entre el CSIRT Nacional, los CSIRT sectoriales y las autoridades competentes.

26. En tal virtud, con la finalidad de mejorar la redacción del texto normativo, propongo el siguiente texto alternativo:

Sexta. - En el plazo máximo de doce (12) meses contados desde la entrada en vigencia de esta ley, el ente rector adoptará las medidas necesarias para la organización y funcionamiento del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), conforme al Reglamento previsto en la Disposición Transitoria Primera en coordinación con los equipos y centros de respuesta a incidentes existentes.

Durante este período de transición:

a) El EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), continuará cumpliendo sus funciones como CSIRT sectorial especializado en telecomunicaciones, bajo la coordinación del CSIRT Nacional.

b) El ente rector gestionará ante los organismos internacionales la transferencia, reconocimiento o coexistencia de las membresías y acreditaciones que actualmente posee el EcuCERT, garantizando la continuidad de la representación del Ecuador en las redes globales de respuesta a incidentes.

c) La Red Nacional de Confianza (RNC) se articulará como mecanismo de cooperación público - privada y de intercambio de información técnica bajo la supervisión del CSIRT Nacional, sin perjuicio de la autonomía operativa de los CSIRT sectoriales.

Vencido el plazo, el ente rector expedirá la normativa técnica que regule la integración, coordinación y delimitación de competencias entre el CSIRT Nacional, el EcuCERT y los demás CSIRT sectoriales.

27. En mérito de las consideraciones expuestas y en ejercicio de las atribuciones que me confieren los artículos 137 y 138 de la Constitución de la República, emito la correspondiente **OBJECIÓN PARCIAL POR INCONVENIENCIA** al proyecto de **Ley Orgánica para el Fortalecimiento de la Ciberseguridad**, decisión que queda establecida en los términos precedentes, así como en el documento correspondiente, cuyo auténtico devuelvo a su autoridad.

Atentamente,

Firmado electrónicamente por:
DANIEL ROYGILCHRIST NOBOA AZIN
Validar únicamente con FirmaEC

Daniel Noboa Azin
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

EL PLENO

CONSIDERANDO:

Que, el artículo 227 de la Constitución de la República dispone que la administración pública constituye un servicio a la colectividad guiado por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación; principios cuya realización demanda garantizar la seguridad, continuidad y confiabilidad de los servicios públicos que operan mediante medios y plataformas digitales;

Que, el artículo 277 de la Constitución establece como deberes del Estado garantizar los derechos de las personas y la naturaleza, dirigir y regular el proceso de desarrollo, producir bienes y servicios, promover la ciencia y la tecnología, e impulsar actividades económicas mediante instituciones que aseguren el cumplimiento de la Constitución y la ley; deberes que, en la era digital, requieren la incorporación de la ciberseguridad como componente estructural de la acción estatal;

Que, la transformación digital del Estado ecuatoriano constituye un proceso estratégico para la modernización institucional, el fortalecimiento de la transparencia, la mejora de la prestación de servicios públicos, la innovación en la gestión administrativa y la ampliación del acceso y participación ciudadana en entornos digitales, de conformidad con la Ley Orgánica para la Transformación Digital y Audiovisual;

Que, la interconexión creciente de sistemas, redes y servicios públicos y privados, así como la dependencia del país de tecnologías digitales para la provisión de servicios esenciales, incrementan la exposición del Ecuador a riesgos y amenazas cibernéticas, tales como ciberataques, accesos indebidos, filtraciones de datos, interrupciones operativas y afectaciones a la infraestructura estratégica, comprometiendo la continuidad del funcionamiento del Estado y la seguridad nacional;

Que, la ciberseguridad concebida como el conjunto de medidas técnicas, organizativas, normativas y de gobernanza destinadas a proteger la confidencialidad, integridad, disponibilidad, autenticidad y resiliencia de los activos digitales se ha convertido en una condición habilitante para la protección del interés público, la continuidad del funcionamiento del Estado, la confianza ciudadana y el adecuado desarrollo de la economía digital;

Que, se requiere dotar al país de un marco legal que establezca estándares nacionales de seguridad digital, defina mecanismos de gestión y notificación de incidentes, y consolide procedimientos de coordinación interinstitucional que eviten duplicidades y respeten las competencias de los órganos de regulación y control especializados, asegurando un enfoque basado en riesgos y continuidad operativa;

Que, la identificación, clasificación y priorización de servicios esenciales e infraestructura crítica digital constituye un requisito indispensable para la continuidad operativa del Estado y la protección del interés público, siendo necesario contar con un Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital, como instrumento técnico que permita ordenar las capacidades de ciberseguridad, gestionar riesgos de manera proporcional y fortalecer la resiliencia nacional;

Que, la creciente frecuencia y sofisticación de incidentes de ciberseguridad exige la adopción de mecanismos uniformes y oportunos de gestión y notificación de incidentes, que permitan activar respuestas técnicas coordinadas, mitigar efectos, prevenir la propagación de amenazas y alinear al país con estándares internacionales de referencia;

Que, la acelerada evolución de tecnologías emergentes, incluyendo la computación cuántica, genera riesgos que pueden comprometer la solidez de los mecanismos criptográficos tradicionales utilizados para la protección de información estatal, privada y de servicios esenciales, lo cual exige incorporar el principio de adaptabilidad tecnológica y adoptar estándares internacionales resilientes frente a dichas amenazas, con el fin de garantizar la seguridad, continuidad y confiabilidad del ecosistema digital nacional;

Que, la identificación temprana de vulnerabilidades y fallas en sistemas tecnológicos requiere habilitar jurídicamente actividades de hacking ético y pruebas de penetración, bajo principios de consentimiento, finalidad legítima, profesionalización y protección de datos personales, con el fin de fortalecer las capacidades de seguridad digital y prevenir riesgos que puedan comprometer servicios esenciales o infraestructura crítica;

Que, las amenazas cibernéticas tienen un carácter transnacional, distribuido y de rápida propagación, lo cual demanda fortalecer la cooperación internacional, la participación del Ecuador en redes globales de respuesta a incidentes (CSIRT, CERT, FIRST), y la

armonización de los estándares nacionales con marcos internacionales de prevención, mitigación y resiliencia;

Que, la existencia de órganos de regulación y control especializados en sectores estratégicos obliga a que la potestad sancionadora en materia de ciberseguridad se ejerza conforme a los principios de especialidad, coordinación y non bis in ídem, y que su aplicación en sectores no regulados se realice de manera subsidiaria, gradual y proporcional, conforme al nivel de riesgo, la capacidad económica del sujeto obligado y la criticidad del servicio involucrado;

Que, la alfabetización digital, la formación en seguridad digital y la promoción de buenas prácticas de higiene digital son elementos esenciales para la prevención de riesgos, la mitigación de amenazas y el fortalecimiento de la resiliencia ciudadana, especialmente en el sistema educativo, lo que demanda la incorporación de contenidos de seguridad digital en los distintos niveles de formación;

Que, es responsabilidad del Estado fortalecer el marco jurídico de la ciberseguridad mediante la incorporación de disposiciones especializadas dentro de la Ley Orgánica para la Transformación Digital y Audiovisual, sin alterar su estructura institucional ni generar nuevas entidades, optimizando capacidades existentes y garantizando la sostenibilidad fiscal establecida en el artículo 287 de la Constitución; y,

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

LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD

DISPOSICIONES TRANSITORIAS

Sexta. - En el plazo máximo de doce (12) meses contados desde la entrada en vigencia de esta ley, el ente rector adoptará las medidas necesarias para la organización y funcionamiento del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), conforme al Reglamento previsto en la Disposición Transitoria Primera en coordinación con los equipos y centros de respuesta a incidentes existentes.

Durante este período de transición:

a) El EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), continuará cumpliendo sus funciones como CSIRT sectorial especializado en telecomunicaciones, bajo la coordinación del CSIRT Nacional.

b) El ente rector gestionará ante los organismos internacionales la transferencia, reconocimiento o coexistencia de las membresías y acreditaciones que actualmente posee el EcuCERT, garantizando la continuidad de la representación del Ecuador en las redes globales de respuesta a incidentes.

c) La Red Nacional de Confianza (RNC) se articulará como mecanismo de cooperación público - privada y de intercambio de información técnica bajo la supervisión del CSIRT Nacional, sin perjuicio de la autonomía operativa de los CSIRT sectoriales.

Vencido el plazo, el ente rector expedirá la normativa técnica que regule la integración, coordinación y delimitación de competencias entre el CSIRT Nacional, el EcuCERT y los demás CSIRT sectoriales.

Mgs. Jaqueline Vargas Camacho
DIRECTORA (E)

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Atención ciudadana
Telf.: 3941-800
Ext.: 3134

www.registroficial.gob.ec

IM/PC

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

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